PRO32

Endpoint Security

ADVANCED

Руководство администратора

Оглавление

1. Введение 4
2. Обзор функций 4
3. Установка сервера администрирования PRO32 Endpoint Security 6
4. Подключение СУБД SQL при установке сервера администрирования 11
5. Консоль администратора (панель управления) 17
6. Активация лицензии 18
7. Установка клиентов PRO32 Endpoint Security 20
8. Подготовка к удаленной установке клиентских приложений 21
9. Обнаружение устройств в Active Directory 22
10. Удаленная установка PRO32 Endpoint Security 25
11. Статус удаленной установки 27
12. Установка PRO32 Endpoint Security на Linux 29
13. Политики 32
14. Политика по умолчанию 32
15. Создание новой политики 33
15.1 Вкладка «Антивирусная защита и защита от шпионского ПО» 33
15.1.1 Раздел «AMSI защита» 34
15.1.2 Раздел «Сканирование» 34
15.1.3 Раздел «Исключения». 35
15.1.4 Раздел «Защита почты». 35
15.2. Вкладка «Поведенческая защита» 36
15.3. Вкладка «Брандмауэр». 36
15.4. Вкладка «Обнаружение вторжений». 37
15.5. Вкладка «Веб-фильтрация». 38
15.6. Вкладка «Управление устройствами». 39
15.7. Вкладка «Обновление» 39
15.8. Вкладка «Привилегии» 40
16. Редактирование политики 41
17. Удаление политики 41
18. Копирование существующей политики для создания новой 41
19. Группы 42
19.1 Создание группы 42
19.2 Редактирование группы 42
19.3 Удаление группы 43
19.4 Изменение группы по умолчанию 43
20. Управление клиентами 44
21. Просмотр событий изменения статуса антивируса и брандмауэра 47
22. Добавление дополнительных полей на страницу «Управление клиентами» 48

23. Смена группы 49
24. Управление задачами 49
24.1 Создание новой задачи 50
24.2 Статусы задач 51
24.3 Удаление задачи 52
24.4 Обновление статусов задач 52
25. Переопределяющая политика 52
26. Карантин 55
27. Управление приложениями 57
27.1 Просмотр списка приложений 57
28. Блокировка приложений 58
28.1 Правило блокировки приложений 59
29. Настройки 59
29.1 Уведомления 60
29.1.1 Настройка уведомлений о событиях по e-mail 61
29.1.2 Уведомления о не зарегистрированных устройствах 62
29.2 Обнаружение местоположения 63
29.3 Настройки прокси 63
29.4 Обновления 64
29.5 Управление данными 64
29.6 Добавление настраиваемых полей 65
29.7 Изменение логотипа 66
29.8 Лицензии 66
29.9 Настройки Active Directory 67
29.10 Переадресатор событий (Интеграция с SIEM) 68
30. Администрирование 69
30.1 Роли администраторов 69
30.2 Пользователи 70
30.3 Настройки сеанса 71
30.4 Настройка параметров пароля для входа в консоль 72
31. Отчеты 73
31.1 Краткий отчёт 73
31.2 Подробный отчет 74
31.3 Экспорт полного отчета по аппаратным средствам в различных форматах 76
32. Миграция на PRO32 Endpoint Security с ESET (средствами консоли ESET Protect) 76
33. Миграция на PRO32 Endpoint Security с Kaspersky Endpoint Security 85

1. Введение

Вас приветствует команда PRO32!

Защита от вирусных атак и угроз – обязательная составляющая современного бизнеса. Компания, которая эффективно пресекает работу вредоносного ПО, сохраняет данные сотрудников и клиентов, не только выполняет требования действующего законодательства, но и заботится о своей репутации. PRO32 предлагает антивирус для предприятий и корпоративных сетей. Программа своевременно обнаруживает и блокирует различные угрозы. Обеспечивает стабильную работу техники и защищает информацию.

PRO32 Endpoint Security – это мощное и простое в использовании комплексное решение для обеспечения безопасности, гарантирующее защиту от новых видов угроз. Это решение с централизованным управлением, которое состоит из тесно взаимосвязанных модулей защиты от вирусов, защиты от шпионских программ, защиты от спама, защиты личных данных и брандмауэра.

В продукте реализована методика многоуровневой защиты и механизм оптимизации сигнатур. Поддерживается настройка безопасности сетей, разведка угроз, функция обнаружения вирусов по эвристической методике. Программа эффективно защищает от вредоносного ПО, приложений-вымогателей, фишинга, APT-атак и т.д. Работает на минимальных требованиях, что позволяет избежать обновления старой техники и продлить период ее эксплуатации.

Антивирус для малого, среднего и крупного бизнеса обновляется ежедневно, что гарантирует защиту от новейших угроз. В программе предусмотрен брандмауэр с HIDS, который пресекает вторжения и проверяет всю информацию, поступающую или исходящую из корпоративных сетей. Можно применять комплексный контроль приложений и блокировать подозрительные сайты с помощью функции веб-фильтрации.

2. Обзор функций

Консоль администрирования

Консоль администрирования – это веб-консоль централизованного управления. Веб-консоль доступна через любой современный веб-браузер с любого компьютера в сети. Она позволяет управлять всеми настройками безопасности, включая установку продукта на клиентских компьютерах, управление группами, политиками, задачами, обновлениями, антивирусом, брандмауэром, контролем приложений, веб-фильтрацией, уведомлениями и т. д.

Защита от вирусов, шпионского ПО и фишинговых атак

Обнаружение всех видов вредоносного ПО. Собранные данные телеметрии находятся в защищенном облачном хранилище и обрабатываются для формирования определений вирусов. PRO32 способен распознавать известные вредоносные программы, новые варианты известных семейств вирусов и даже незнакомые и ранее неизвестные угрозы. В антивирусе для офиса реализована методика многоуровневой защиты и механизм оптимизации сигнатур. Поддерживается настройка безопасности сетей, разведка угроз, функция обнаружения вирусов по эвристической методике. Программа эффективно защищает от вредоносного ПО, приложений-вымогателей, фишинга, APT-атак и т.д. Работает на минимальных требованиях, что позволяет избежать обновления старой техники и продлить период ее эксплуатации

Защита от руткитов и программ-вымогателей

Система защиты от программ-вымогателей на основе мониторинга поведения блокирует распространение и шифрование файлов программой-вымогателем.

Защита доступа в интернет

Интеллектуальный брандмауэр - Автоматическая настройка правил доступа в Интернет из офиса/за пределами офиса. Безопасность Wi-Fi подключений. Автоматическое обнаружение и блокировка сетевых атак. Отслеживание вирусов и троянов, проникающих через браузеры и компоненты ActiveX.

Защита электронной почты

Сканер электронной почты проверяет входящие и исходящие электронные письма, чтобы не допустить попадания зараженных писем в ваш почтовый ящик. Если электронное письмо содержит вирус, сканер электронной почты удаляет зараженные вложения или помещает их в карантин.

Интеллектуальный брандмауэр со встроенными функциями HIDS/HIPS

HIPS (хостовая система предотвращения вторжений) блокирует конкретное вредоносное поведение, например создание известных вредоносных объектов на сетевом уровне, в файловой системе или реестре.

Enhanced HIPS за счет анализа содержимого и активности файлов во время выполнения обнаруживает и блокирует потенциально вредоносные процессы, создающие подозрительные объекты в нестандартных местах или инициирующие исходящие соединения с подозрительными URL-адресами или с внешними IP-адресами.

Защита устройств

Позволяет настроить парольную защиту в системе, в которой установлен продукт, перед доступом к определенному типу устройства. Вакцинация USB-накопителя не позволит вирусным программам автоматически заражать любые ПК, к которым его подключают, с использованием механизма автоматического выполнения.

Защита файловых серверов

Продукт имеет ряд функций для защиты файловых серверов: поиск руткитов, интеграция со службами Active Directory, запуск подозрительных приложений, защита от подозрительного шифрования данных (вирусы-шифровальщики). AMSI (Anti-Malware Scan Interface) – защита.

Интеграция с SIEM

Если вы используете системы мониторинга, то PRO32 Endpoint Security сможет передавать в неё события по протоколу Syslog. Доступны такие события как: Обнаружение угрозы, Нарушение доступа, Попытка перехода на заблокированные сайты, блокировка приложений.

Контроль приложений

Настроив управление доступом к приложениям, вы можете контролировать, каким программам на вашем компьютере разрешен доступ в Интернет. По умолчанию брандмауэр PRO32 автоматически добавляет в список программы, которые считает безопасными. Когда программа, которой нет в списке, попытается получить доступ к Интернету, вы получите уведомление. Вы можете разрешить или заблокировать доступ в Интернет для соответствующей программы.

*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

Контроль устройств

С ростом числа вредоносных программ, способных заражать вашу систему через такие устройства, как USB, важно обеспечить защиту доступа к этим устройствам. Функция доступа к устройствам позволяет контролировать доступ к USB-накопителям, CD-, DVD-дискам и дисководам гибких дисков. Вы можете управлять возможностью копирования файлов на диск или с диска, а также возможностью их исполнения.

*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

Веб-фильтры (блокировка сайтов/фильтрация по категориям)

Функция веб фильтрации позволяет блокировать веб-сайты и приложения/игры, а также защищать пользователей от доступа к нежелательной информации. Эта функция позволяет фильтровать веб-сайты, использующие протокол http и https. Вы также можете блокировать доступ сторонних браузеров к Интернету.

*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

3. Установка сервера администрирования PRO32 Endpoint Security

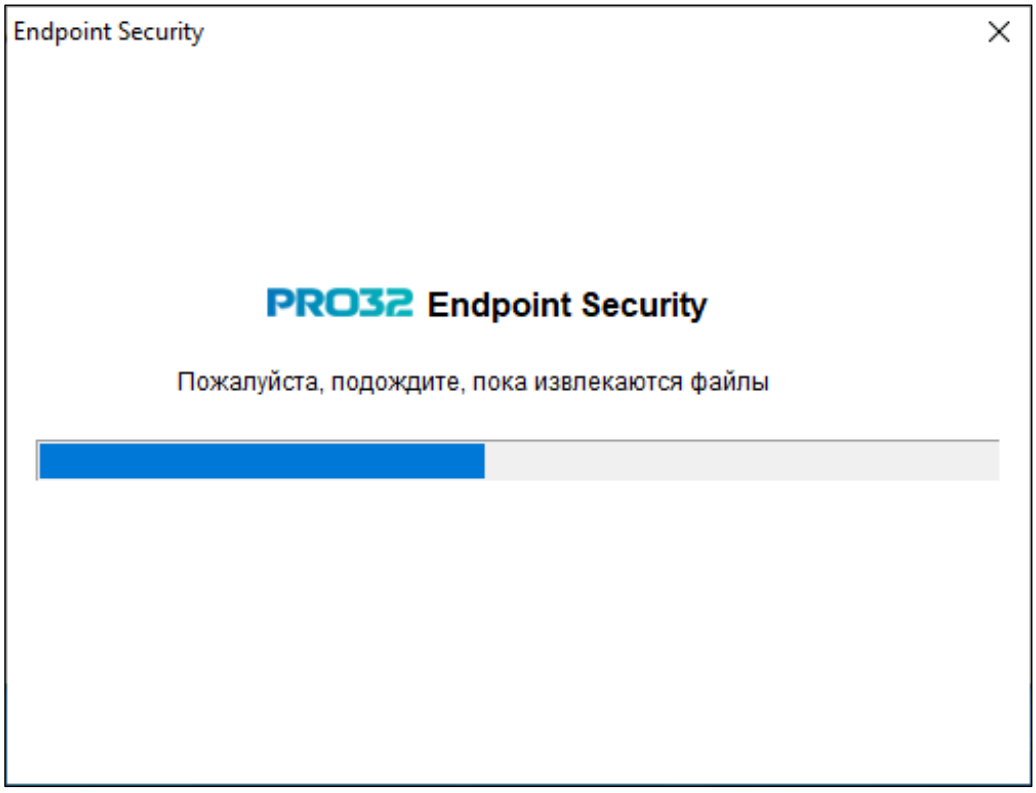
Этапы установки

1. Загрузите установочный файл:

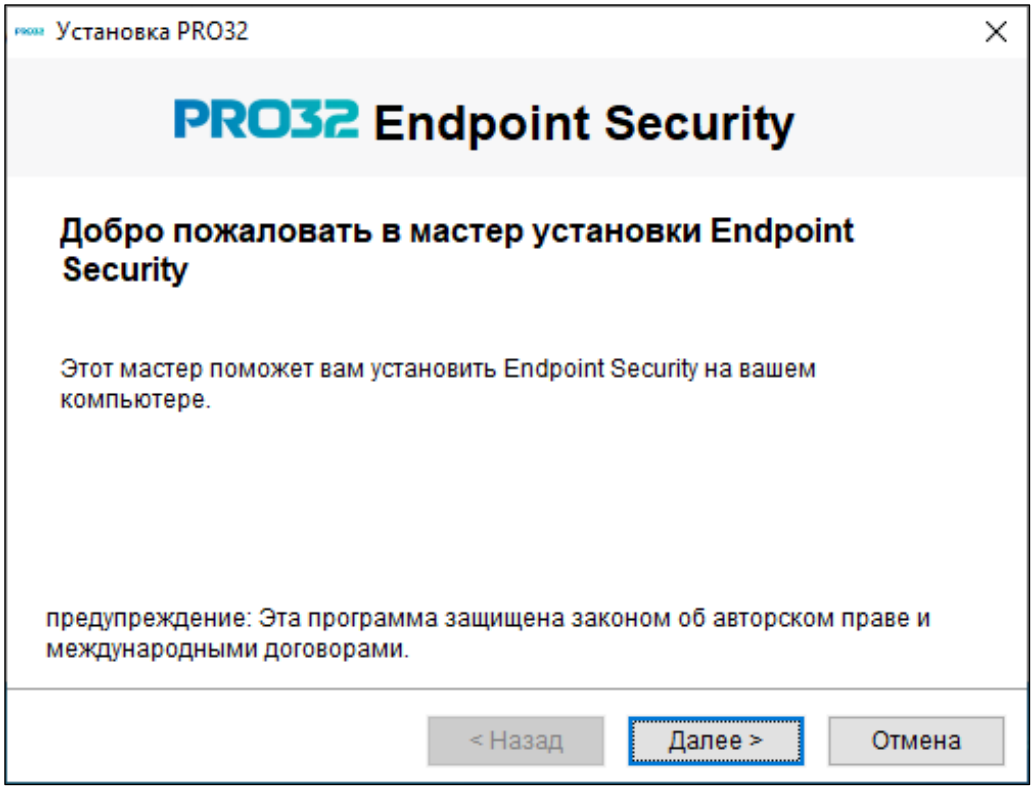
https://static.pro32.com/download/installer/PRO32EndpointSecuritySetup.exe

2. Дважды щелкните файл установщика, чтобы начать установку.

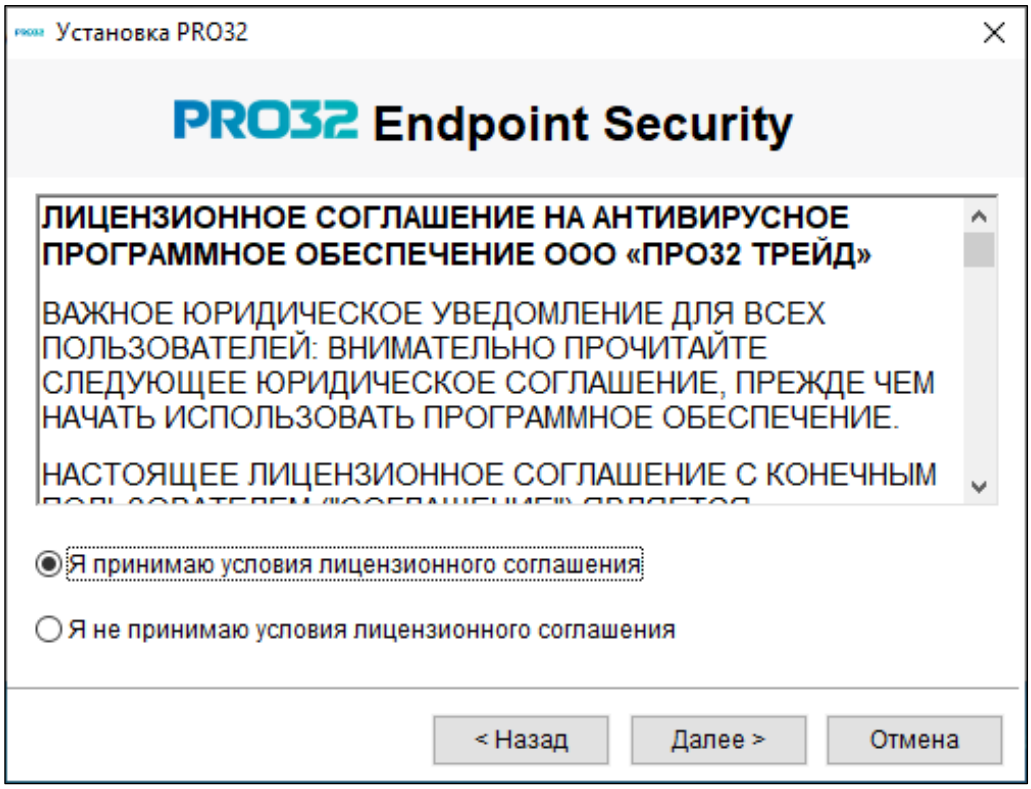
3. Извлечение файлов. Если дважды щелкнуть файл PRO32EndpointSecuritySetup.exe, будут извлечены установочные файлы.



4. После извлечения файлов автоматически запустится мастер установки, который поможет администратору выполнить установку.

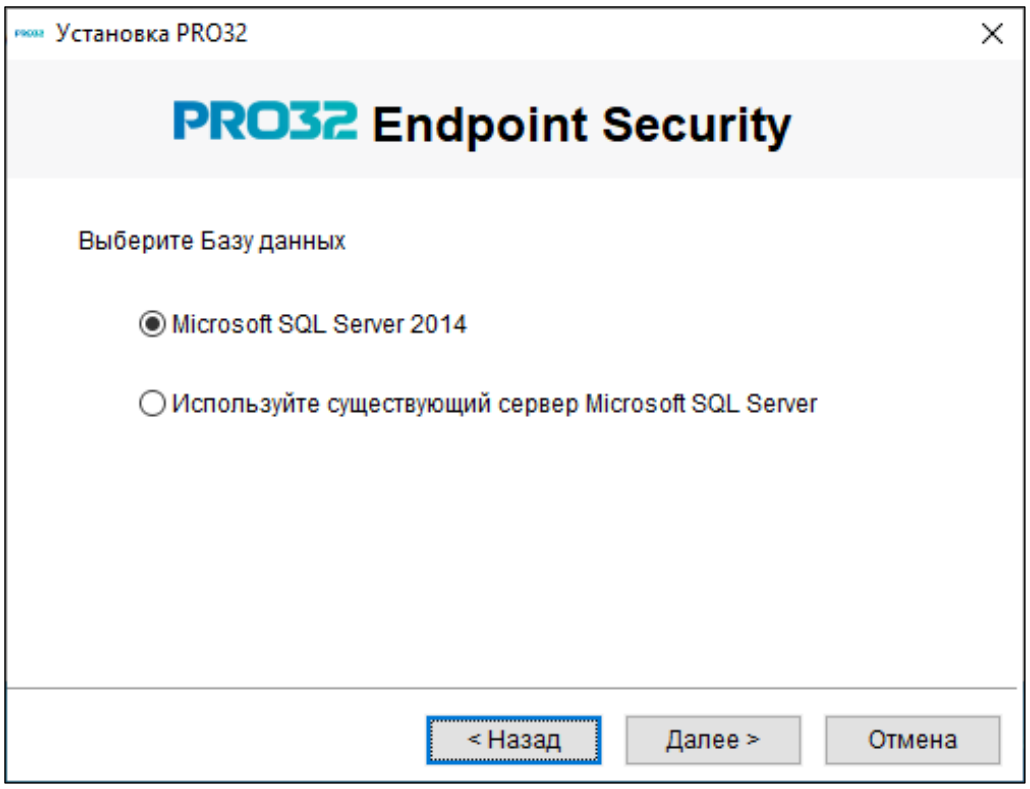


5. **Лицензионное соглашение:** прочтите лицензионное соглашение и выберите вариант «Я принимаю условия лицензионного соглашения перед установкой». При выборе опции «Я не принимаю условия лицензионного соглашения», продукт не будет установлен, а мастер установки будет закрыт.

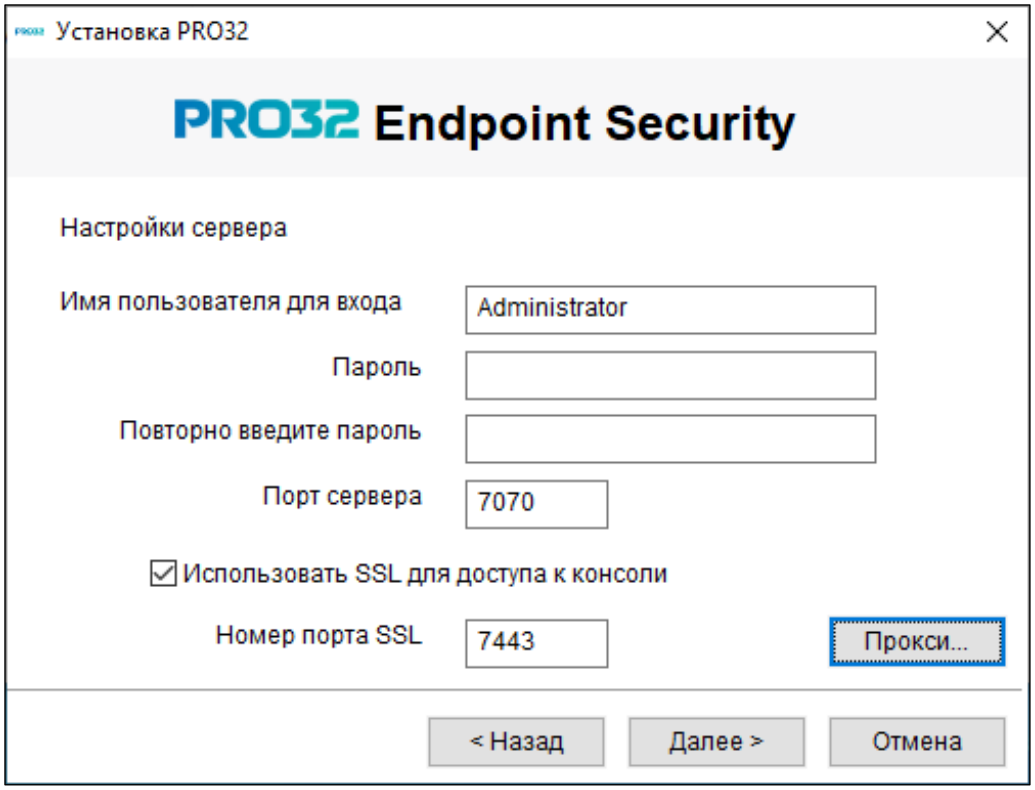


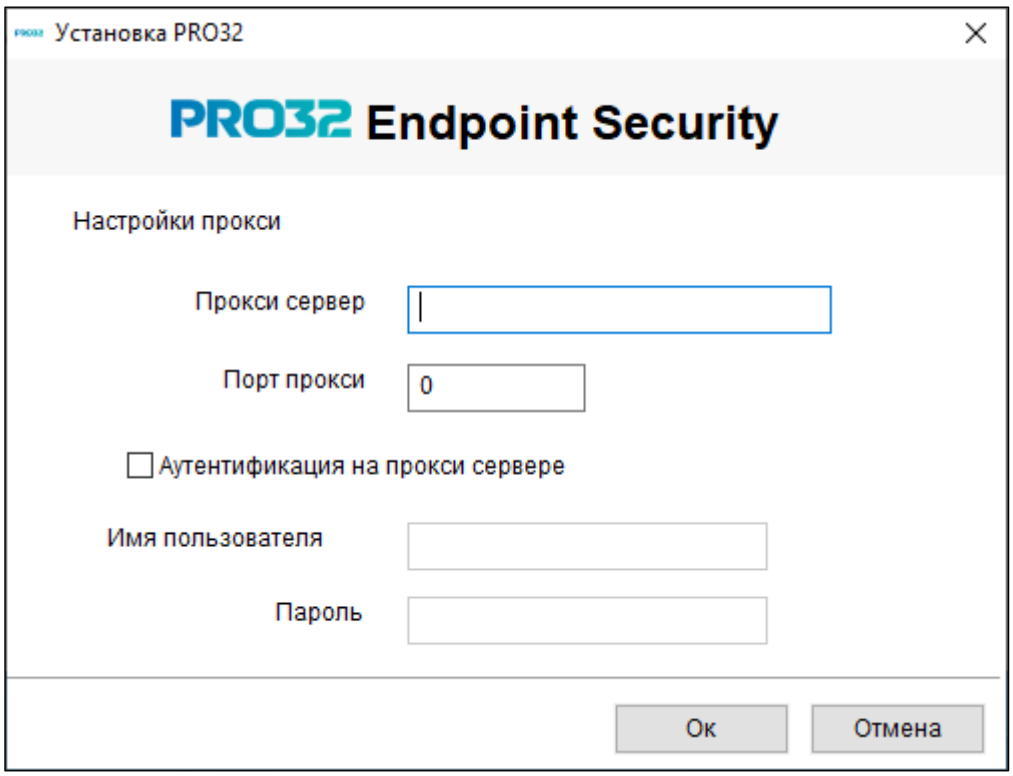
Для работы Антивируса требуется система управления базами данных (далее – СУБД). В базе данных хранятся настройки антивируса, правила, события и прочая пользовательская информация. PRO32 Endpoint Security использует СУБД Microsoft SQL Server 2014 и выше. Дистрибутив идёт в комплекте. Так же можно использовать уже установленную СУБД.

6. После принятия соглашения необходимо выбрать какую СУБД использовать, новую или существующую.

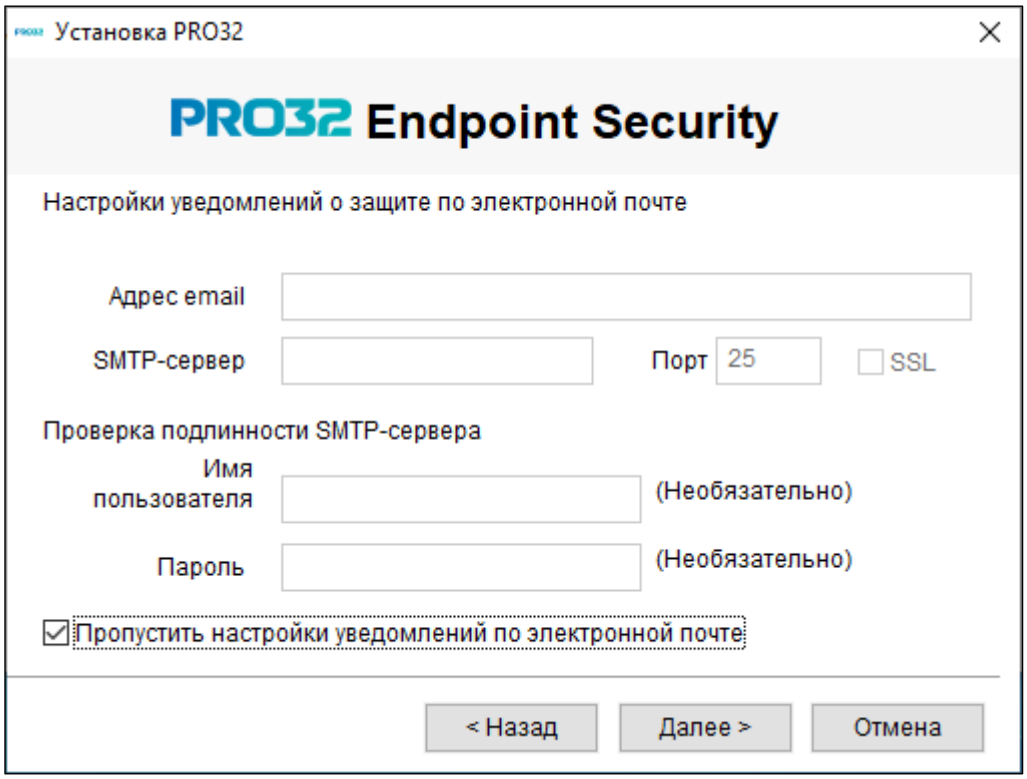


7. На следующем экране необходимо ввести учетные данные для входа в консоль администратора. Также вы можете настроить параметры проксировния, нажав соответствующую кнопку.

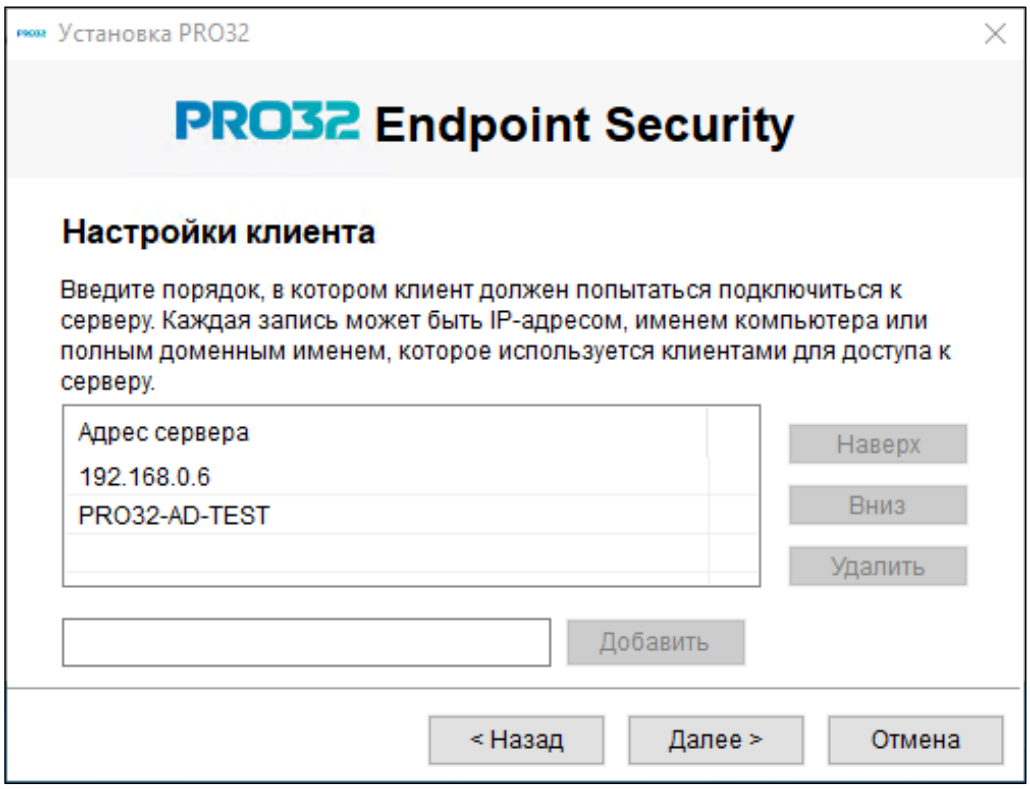


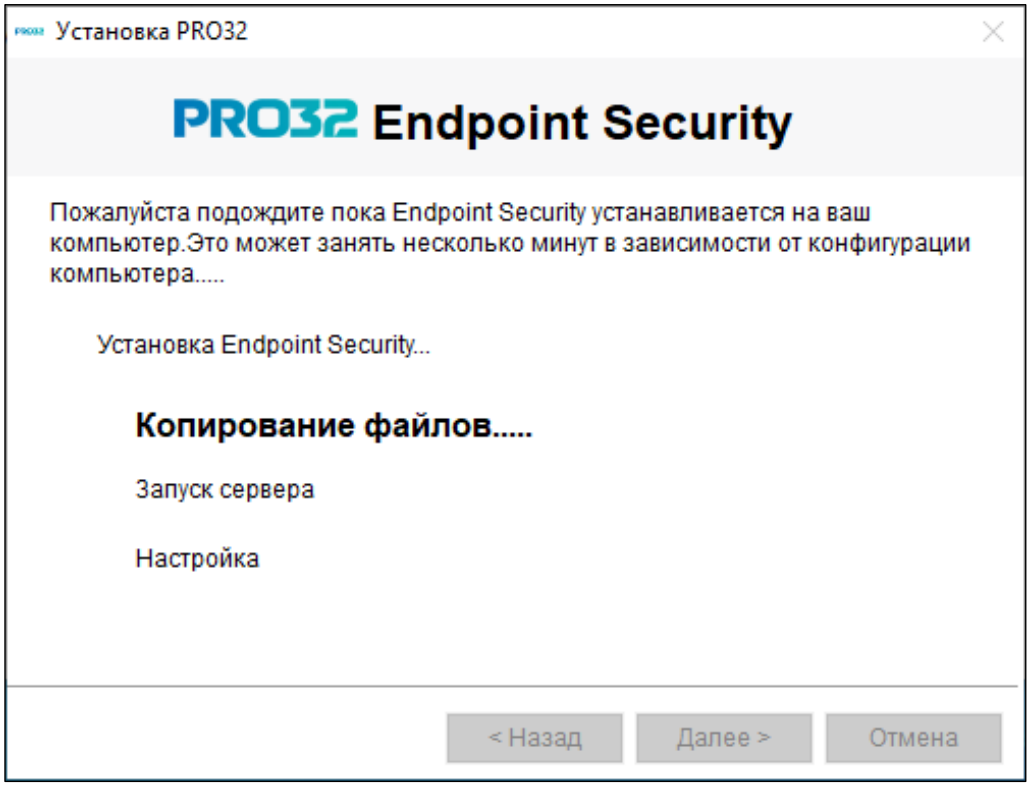


8. Задайте параметры почтового сервера (для получения уведомлений о событиях антивируса), при необходимости, либо пропустите этот шаг.



9. Укажите порядок подключения к серверу. При нажатии “Далее” PRO32 Endpoint Security будет установлен.





10. После успешной установки вы можете нажать воспользуйтесь кнопкой «Завершить», чтобы запустить консоль администратора.

4. Подключение СУБД SQL при установке сервера администрирования

1. Скачайте дистрибутив MS SQL Server 2014 или новее (по ссылке версия 2022):

   https://www.microsoft.com/en-us/download/details.aspx?id=104781

   Если СУБД уже установлена, этот шаг можно пропустить

2. Скачайте SQL Server Management Studio

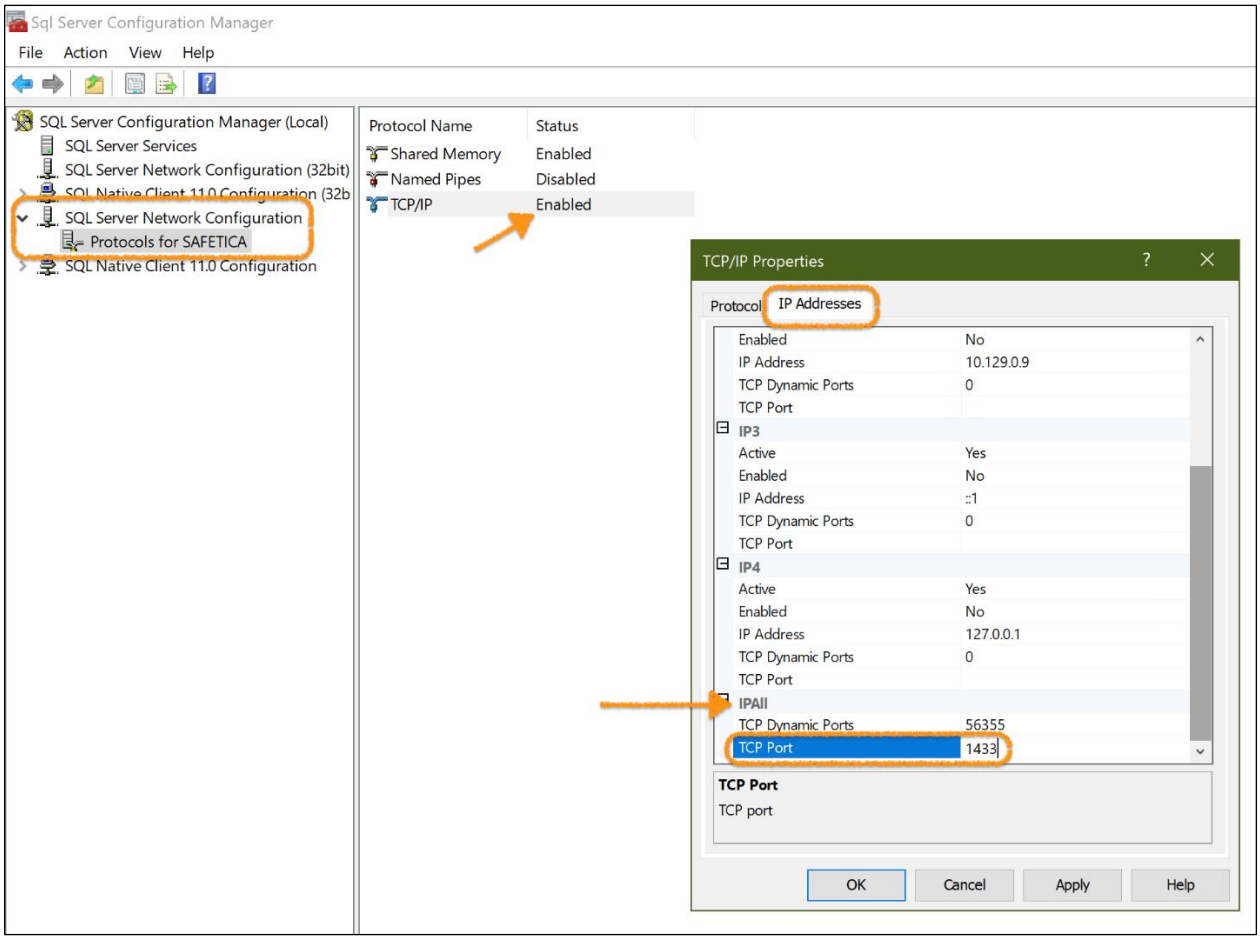
   https://learn.microsoft.com/ru-ru/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16

3. Скачайте дистрибутив PRO32 Endpoint Security
   https://static.pro32.com/download/installer/PRO32EndpointSecuritySetup.exe

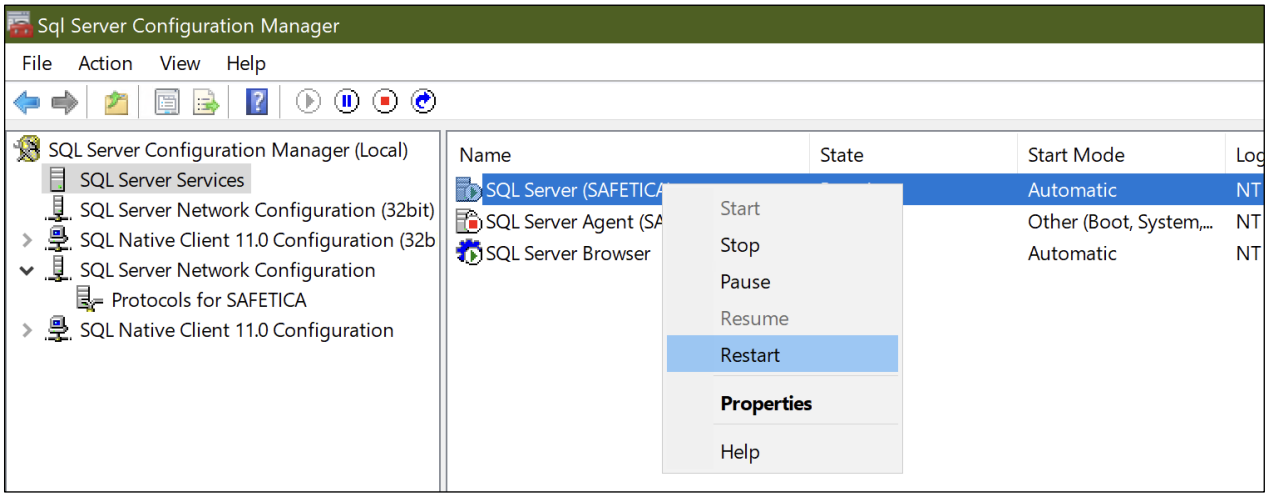
4. Установите СУБД (если не установлена). Нажмите кнопку «Пуск» и перейдите в SQL Server Configuration Manager,

5. В разделе Network Configuration включите TCP\IP

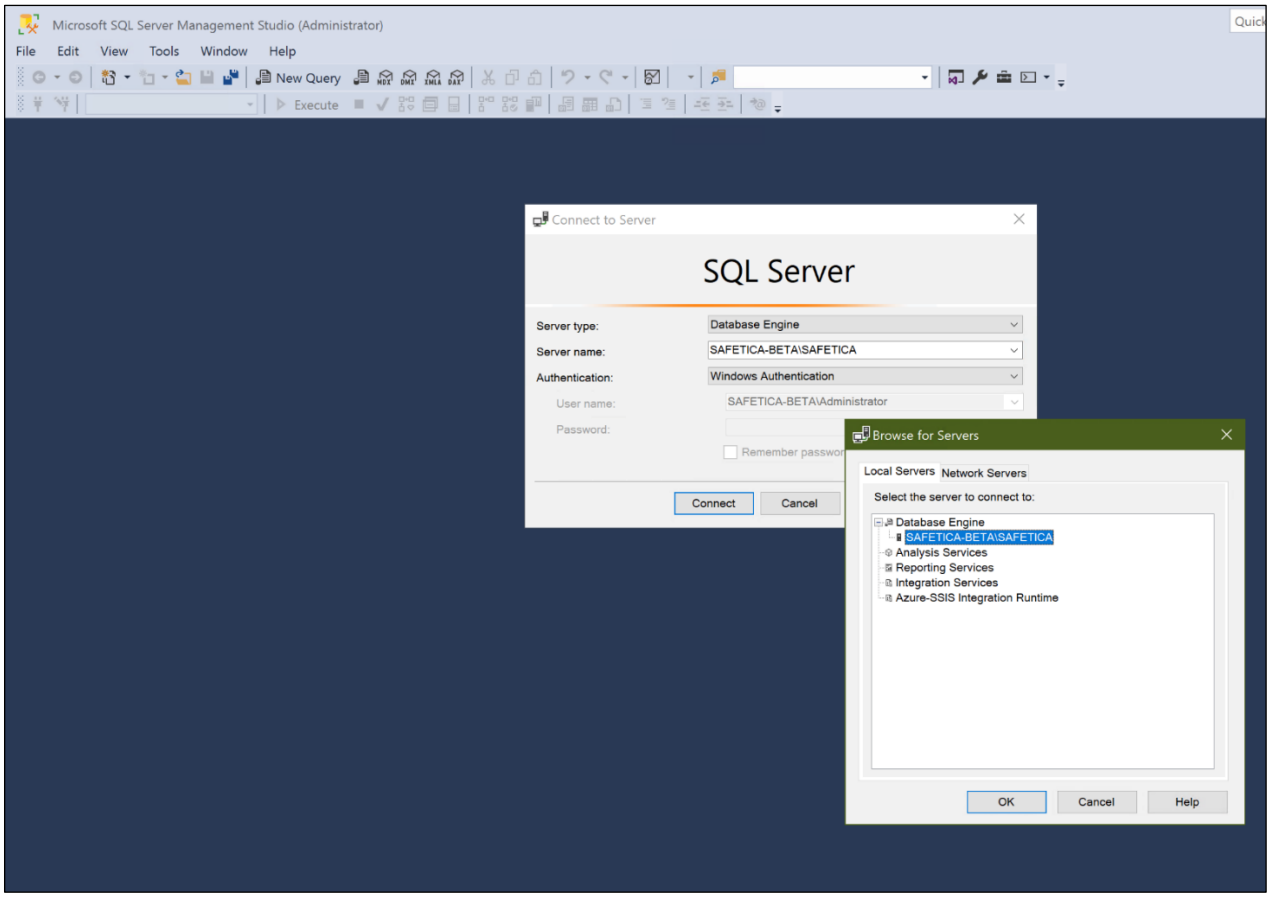
6. В параметрах TCP\IP, во вкладке IP Adresses \ IP All включите порт 1433.



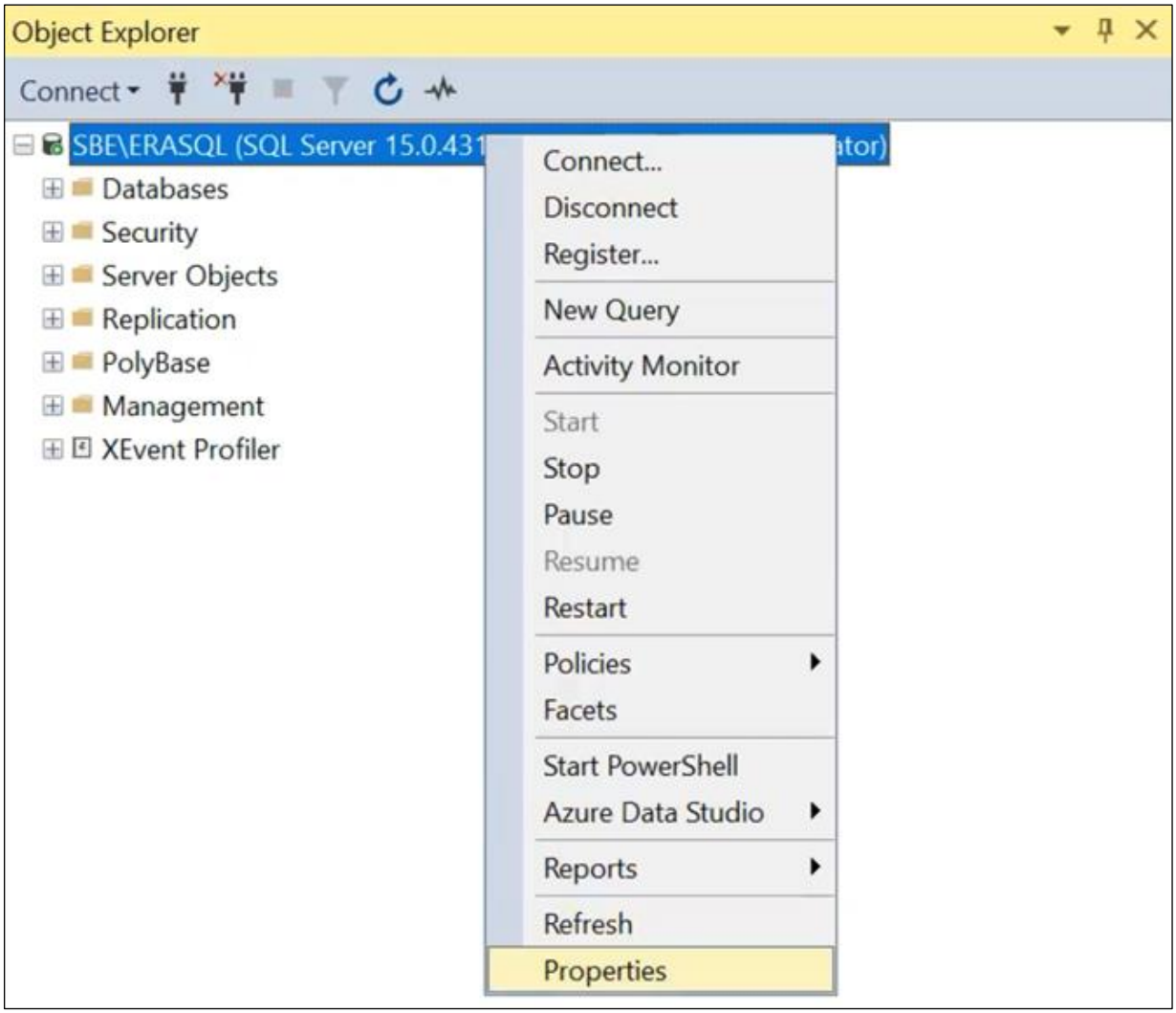
7. Перезагрузите службу СУБД для применения изменений настроек

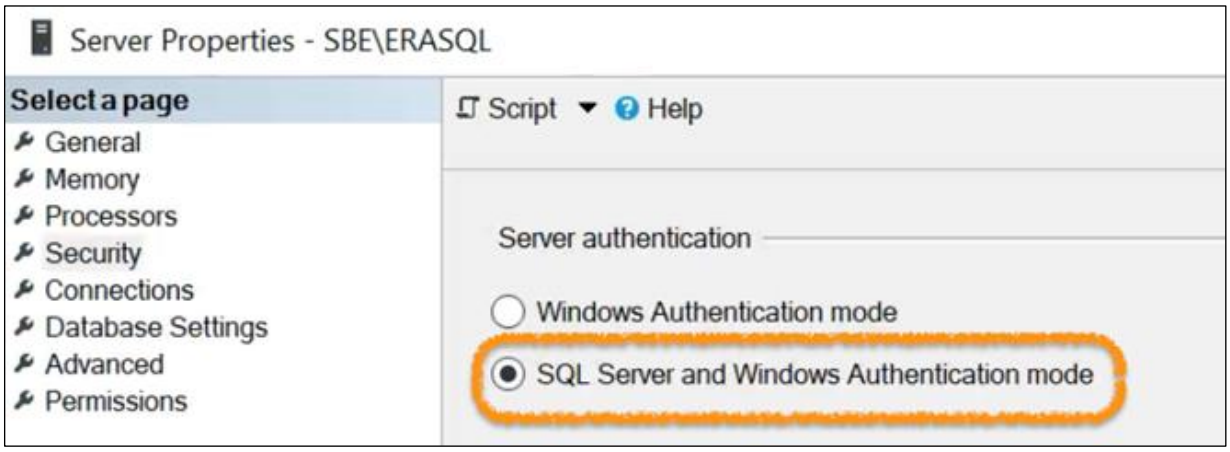


8. Установите и запустите SQL Server Management Studio. Выберите в обзоре СУБД установленную базу данных и нажмите кнопку «Connect» (ниже изображение ранее установленной СУБД, для примера, название может отличаться).

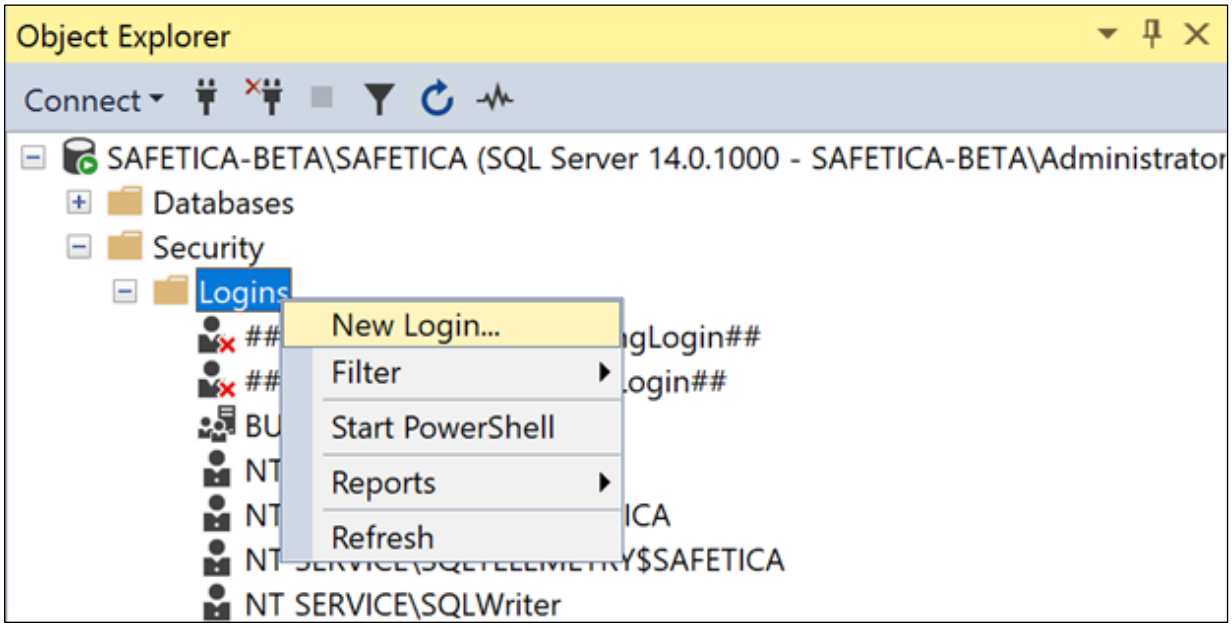


9. Включите смешанный режим аутентификации на СУБД

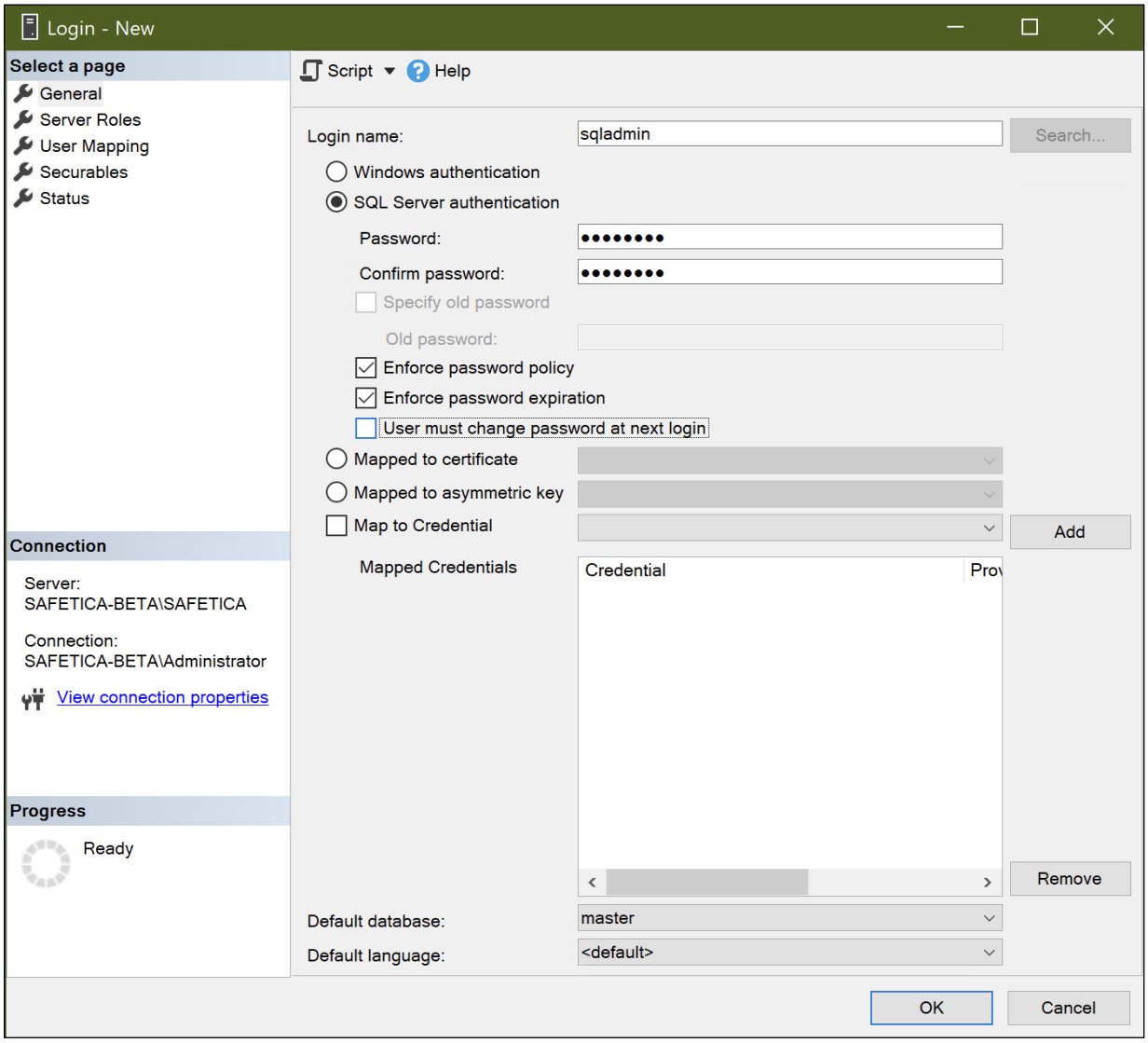




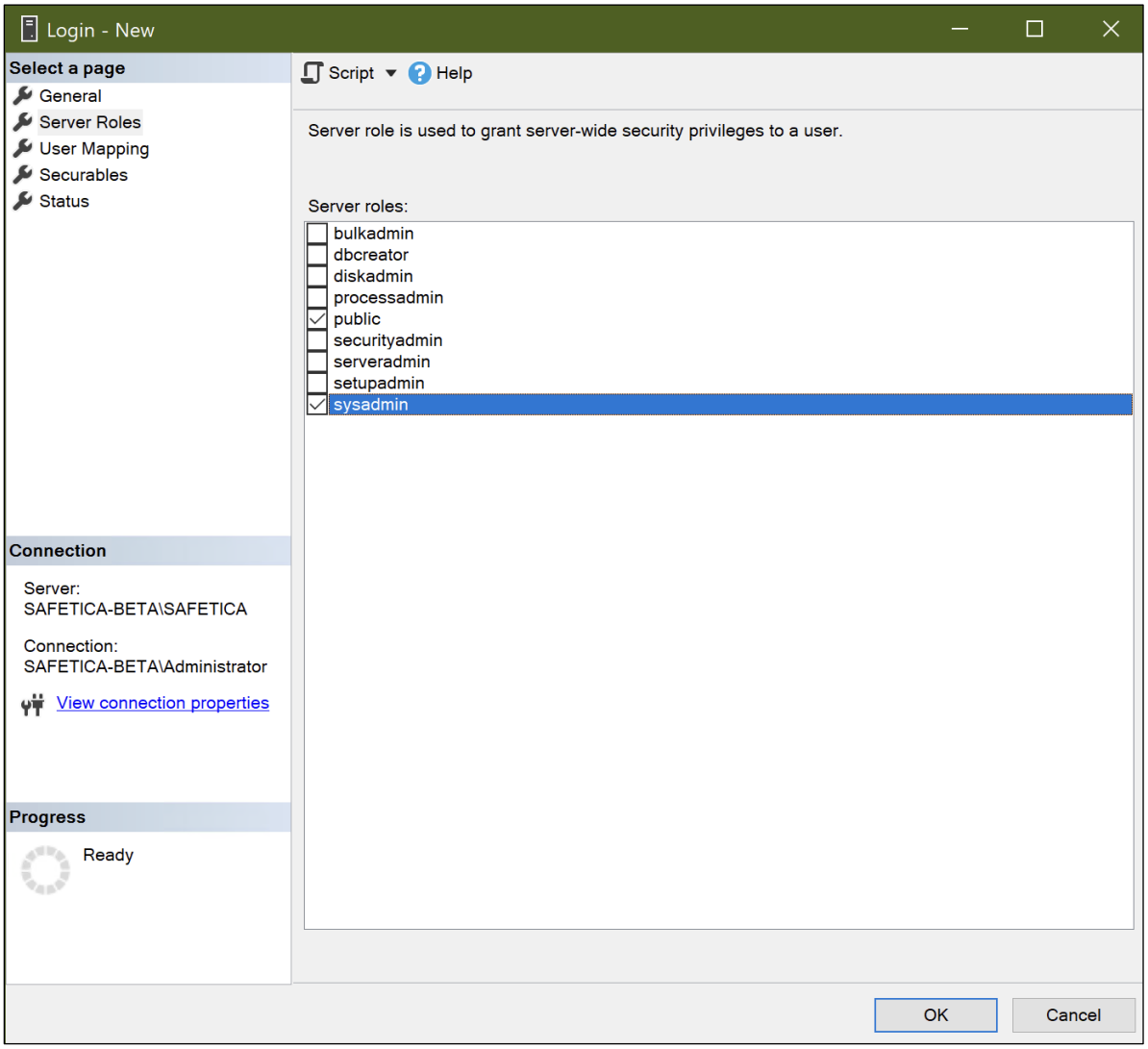
10. Создайте учетную запись, которая будет использована только для первичного подключения к СУБД.



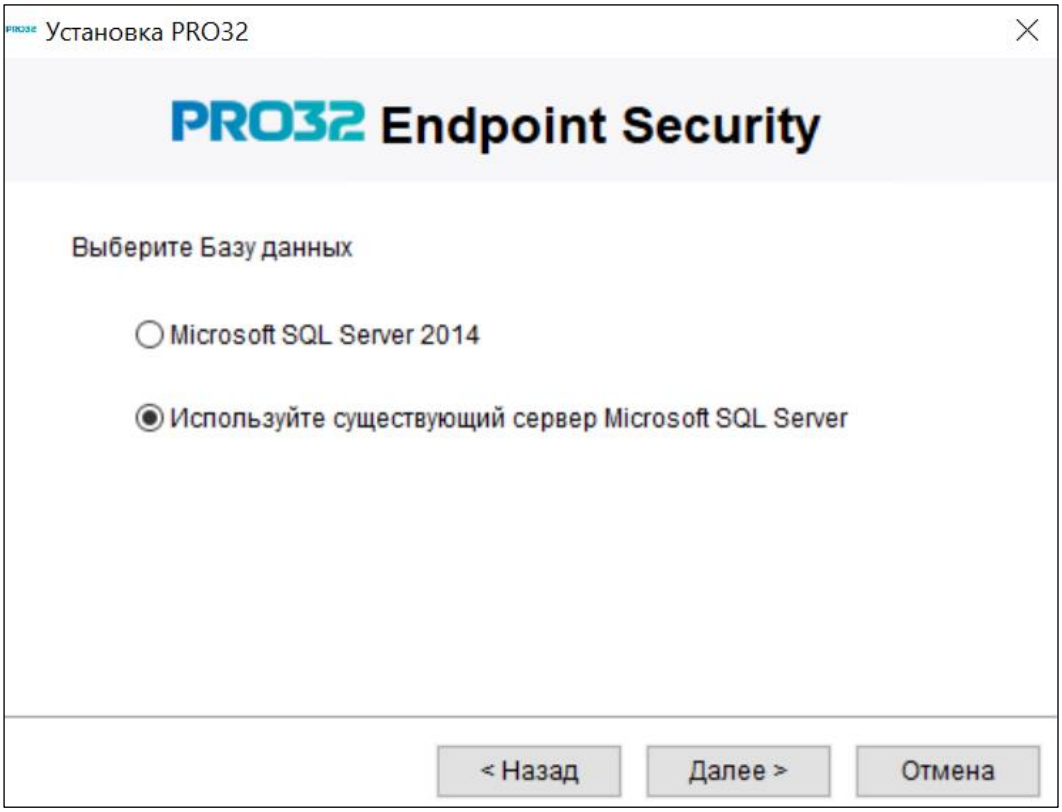
11. Выключите требование смены пароля, задаем имя и пароль для учетной записи.



12. В разделе Server Roles добавьте права Sysadmin (максимальные права на сервере).



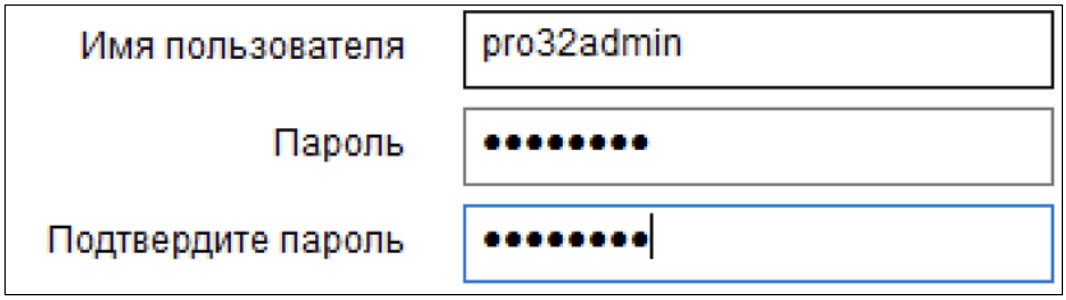
13. Запустите установочный файл PRO32 Endpoint Security. На экране выбора СУБД, выберите опцию «Использовать существующий Microsoft SQL Server».



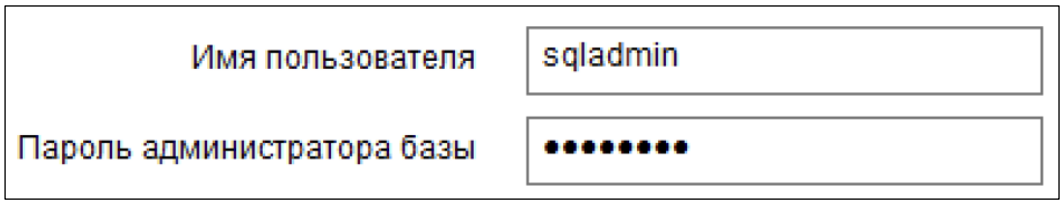
14. В параметрах необходимо задать:

Имя сервера = fqdn или IP адрес сервера MS SQL

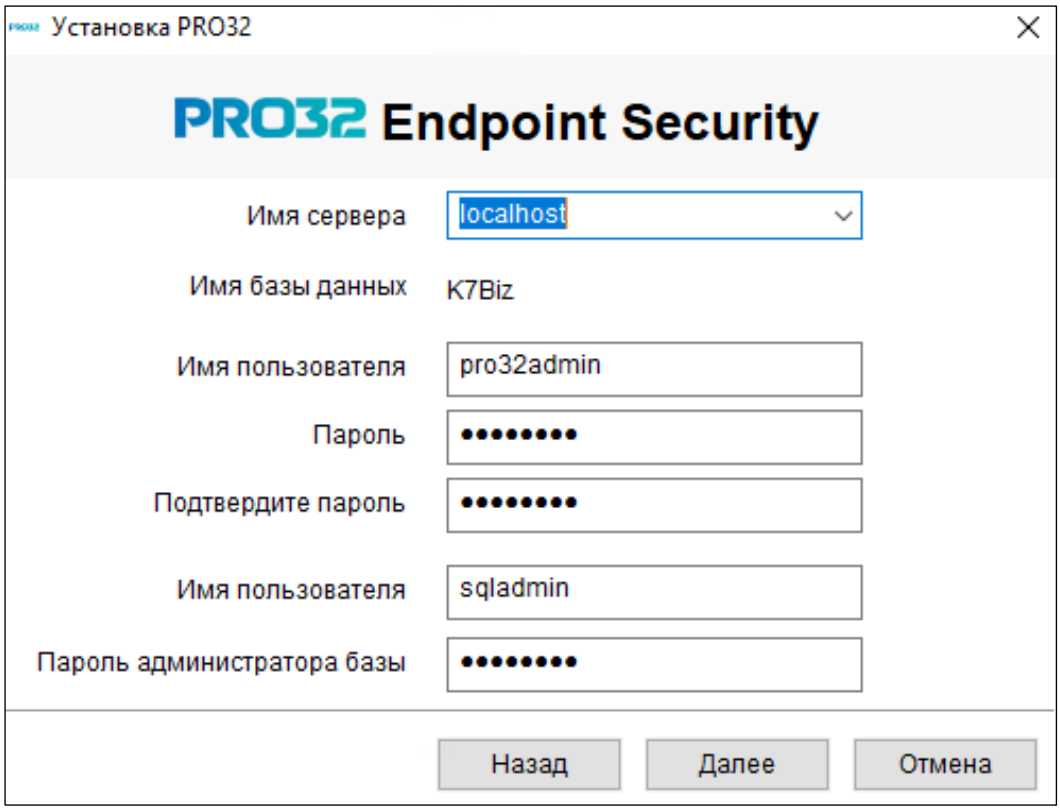
Укажите логин и пароль выделенной учетной записи в MS SQL, она будет создана для использования консолью при работе с базой данных.



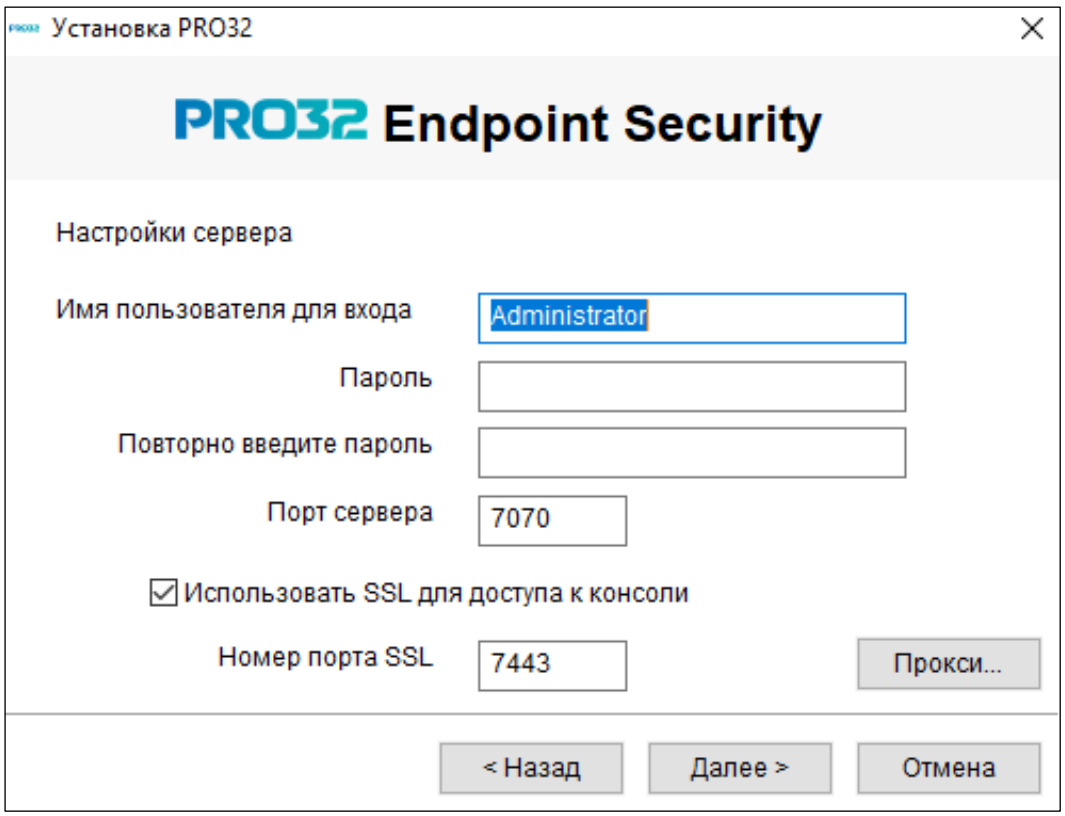
Укажите данные текущей учетной записи в MS SQL (созданной на шаге 8), она будет использована только при первичном подключении к СУБД.



В результате у вас должен получиться следующий набор настроек. Пример:

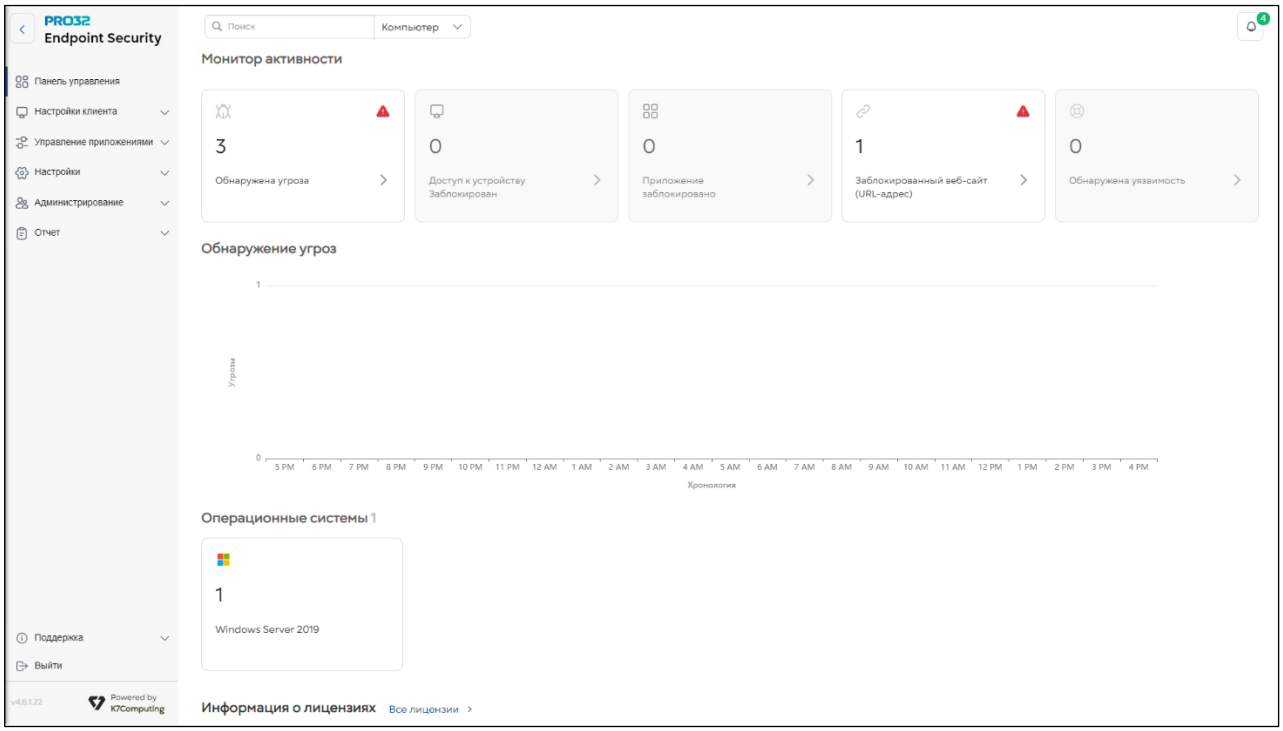


13. На следующем шаге задайте логин и пароль администратора веб консоли.



5. Консоль администратора (панель управления)

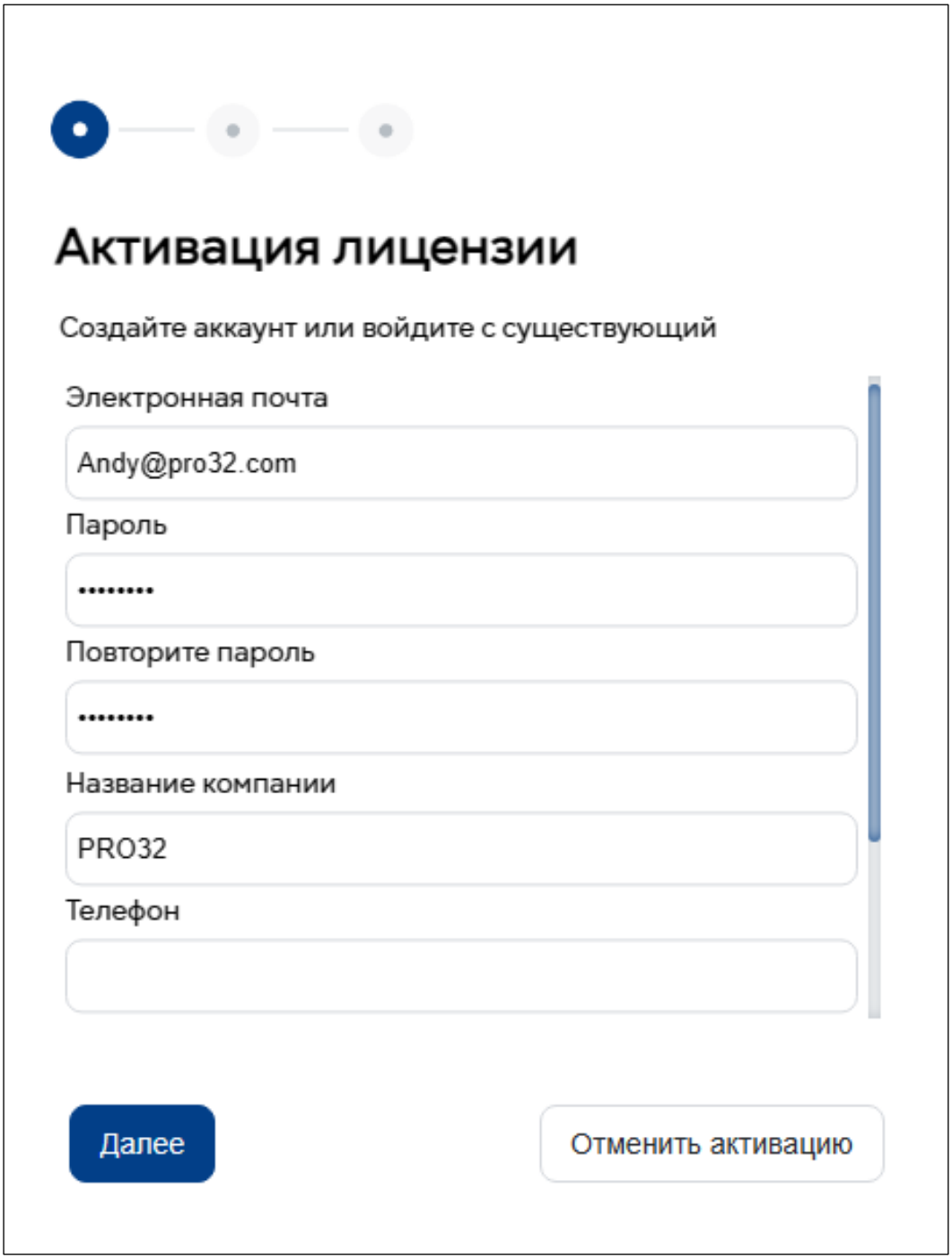
Панель управления – это главный раздел консоли, на которой администратор может легко и быстро просмотреть данные о защите клиентских компьютеров: обнаружены ли угрозы, статус обновления, статус выполнения задачи сканирования, статус установки/удаления клиентского ПО, статус защиты у антивируса и брандмауэра, сведения о нарушении правил доступа к устройствам, заблокированные приложения и веб-сайты, обнаруженные уязвимости, сведения о подписке и т. д. Если инструментальная панель выглядит необычно, администратор может быстро перейти к проблеме, щелкнув соответствующую ссылку на проблему в виджете, и просмотреть подробный отчет.



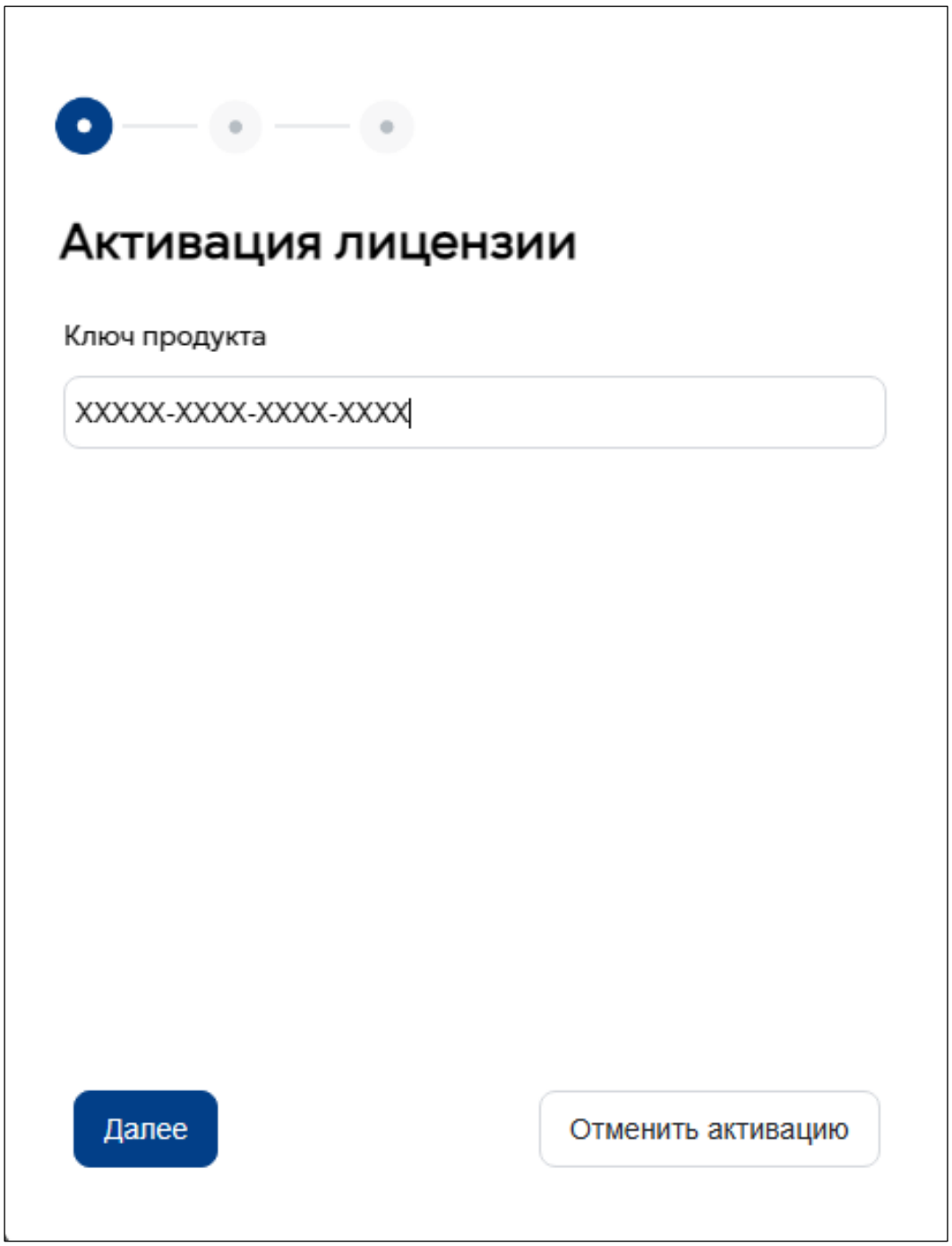
6. Активация лицензии

После завершения установки необходимо зарегистрировать и активировать продукт для регулярного получения определений вирусов и обновлений, что обеспечит безопасность системы. При первом запуске консоли администратора запустится процесс активации.

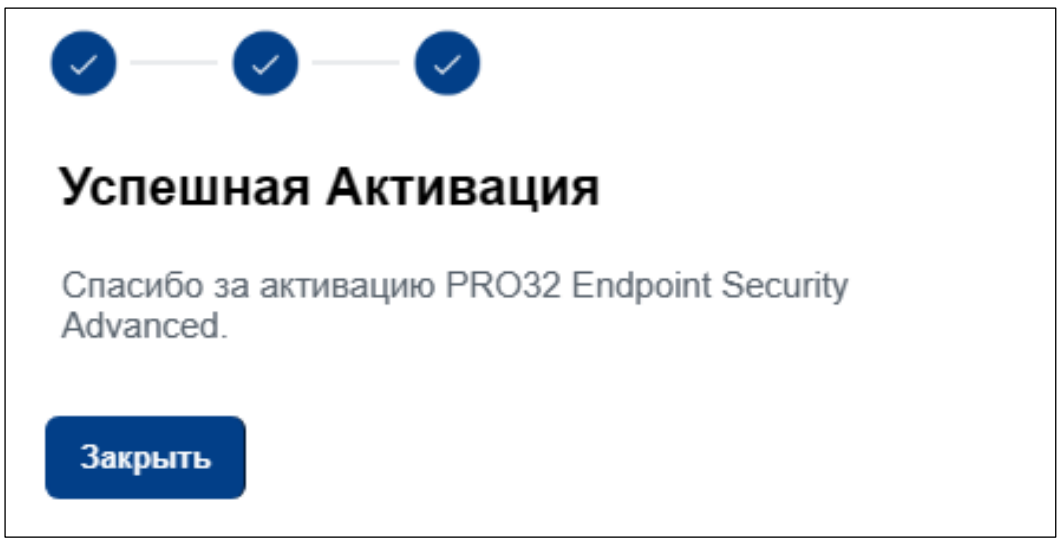
Укажите данные главного системного администратора и пароль. Нажмите кнопку **«Далее».**



Введите лицензионный ключ в формате XXXXX-XXXX-XXXX-XXXX, Нажмите кнопку **«Далее».**



Для успешной активации требуется подключение сервера активации к сети Интернет. После успешной активации нажмите кнопку **«Закрыть».**



7. Установка клиентов PRO32 Endpoint Security

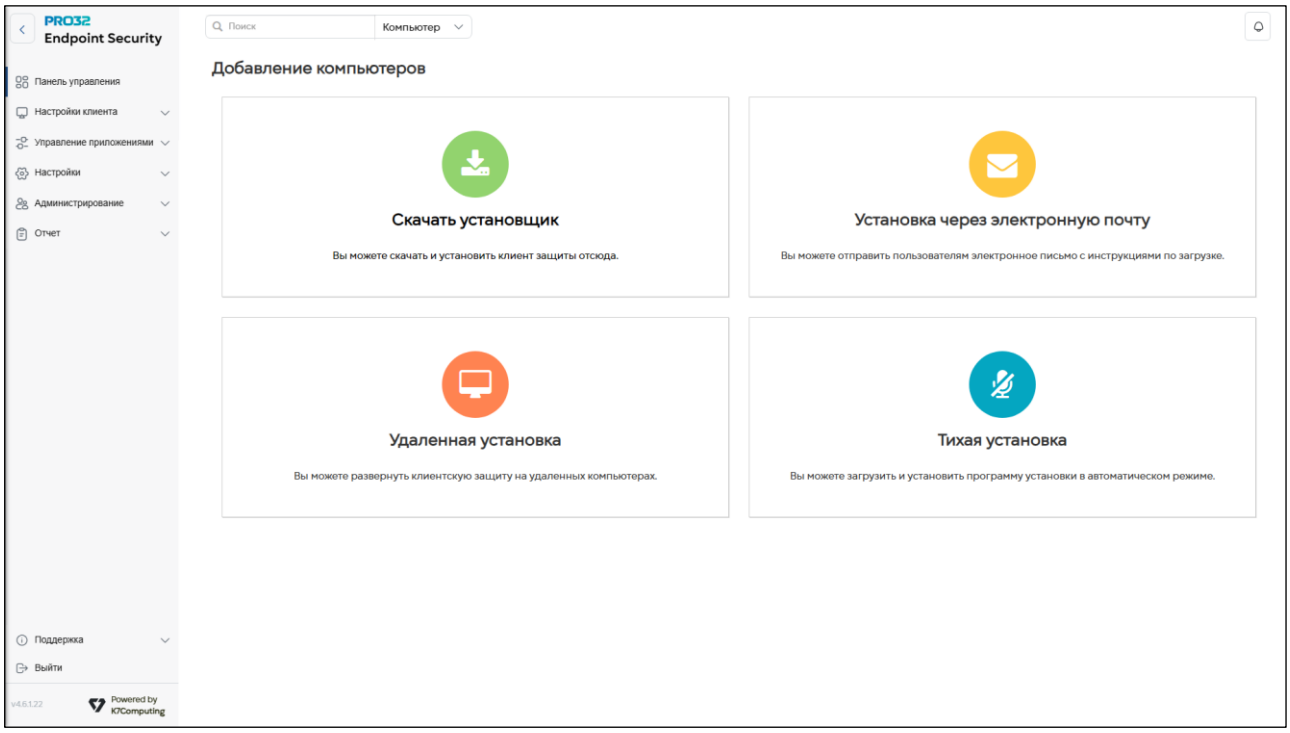
После установки и активации серверного компонента вы можете установить программу PRO32 Endpoint Client на клиентские компьютеры одним из следующих способов.

1. **Установка по URL-адресу** – развернуть PRO32 Endpoint Client на клиентских компьютерах, передав конечным пользователям с консоли администрирования ссылку на установочный файл.

2. **Уведомление по электронной почте** – отправить URL-адрес установочного файла по электронной почте всем пользователям, на чьи компьютеры требуется установить программу PRO32 Endpoint Client.

3. **Удаленная установка клиента** – установка с консоли администрирования программы PRO32 Endpoint Client на несколько компьютеров одновременно. Установка будет выполнена без пользовательского интерфейса.

4. **Тихая установка** – установка в автоматическом режиме.



8. Подготовка к удаленной установке клиентских приложений

Развертывание PRO32 Endpoint Client на клиентских компьютерах – несложный процесс благодаря мастеру удаленной установки. Для удаленной установки PRO32 Endpoint Client у вас должны права администратора на целевом компьютере. Кроме того, вам также может потребоваться изменить параметры брандмауэра Windows и параметры общего доступа к файлам, как описано ниже.

Windows XP и Windows 2003 Server

1. Отключите простой общий доступ к файлам.

Для этого выполните следующие действия:

i. Перейдите по пути **Мой компьютер → Сервис** → **Свойства папки** и откройте вкладку **Вид**.

ii. В разделе «**Дополнительные параметры»** снимите флажок «**Использовать простой общий доступ к файлам»** и нажмите «**ОК»**.

2. Если брандмауэр Windows включен, разрешите общий доступ к файлам и принтерам.

Для этого выполните следующие действия:

i. Откройте вкладку **Брандмауэр Windows** → **Исключения**.

ii. Установите флажок «**Общий доступ к файлам и принтерам»** и нажмите **«ОК».**

Windows Vista и Windows 2008 Server

1. Если брандмауэр Windows включен, разрешите общий доступ к файлам.

Для этого выполните следующие действия:

i. Перейдите по пути **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом**.

ii. В разделе «**Общий доступ и сетевое обнаружение»** включите «**Общий доступ к файлам»** и нажмите «**Сохранить изменения»**.

Windows 7 и Windows 2008 R2

1. Если брандмауэр Windows включен, разрешите общий доступ к файлам и принтерам.

Для этого выполните следующие действия:

i. Перейдите по пути **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа**.

ii. В разделе «**Общий доступ к файлам и принтерам»** включите «**Общий доступ к файлам»** и нажмите «**Сохранить изменения»**.

Если вы не входите во встроенную группу администраторов домена (Built-in/Domain Administrator), необходимо изменить настройку удаленных ограничений UAC на целевом компьютере. (Этого не требуется в XP.)

Чтобы отключить удаленные ограничения UAC, выполните следующие действия:

1. Откройте редактор реестра Windows и найдите следующий подраздел: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**

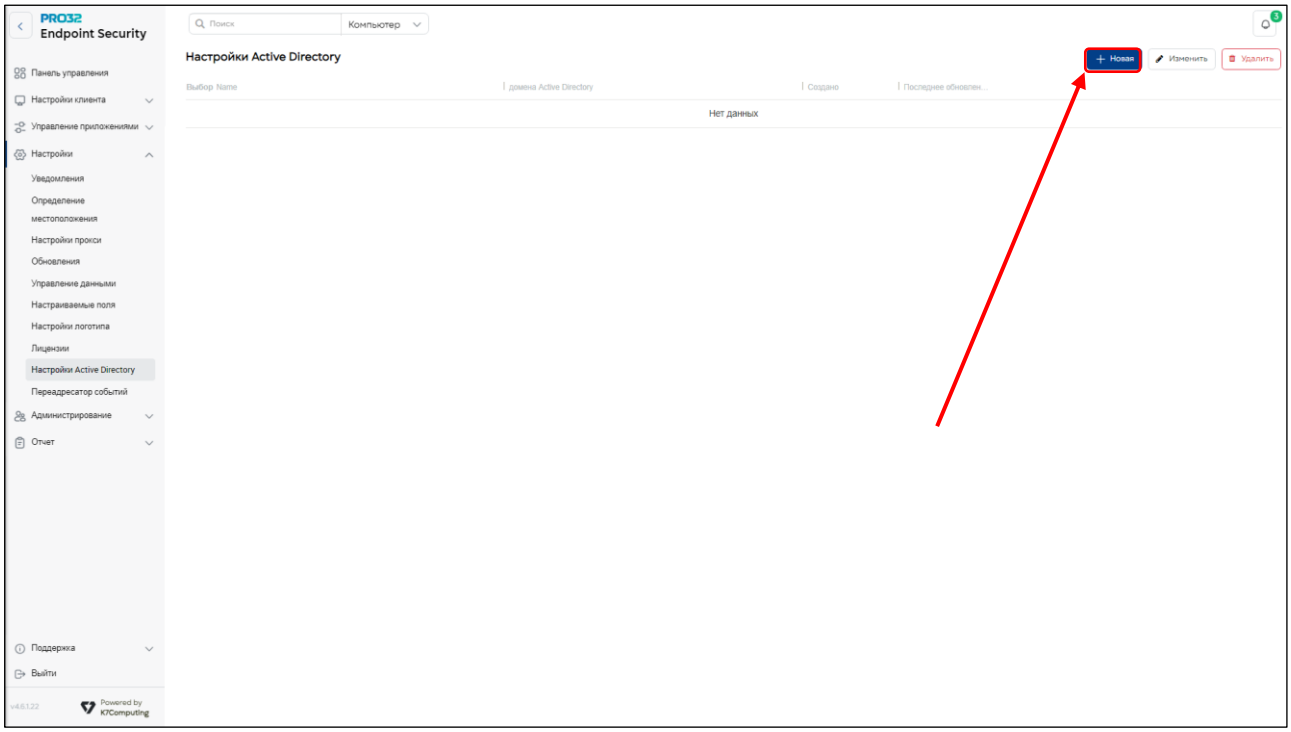
2. Если в правой части экрана нет элемента LocalAccountTokenFilterPolicy, создайте параметр **DWORD** с именем **LocalAccountTokenFilterPolicy** и в качестве **Значения** укажите **1**.

Важно, чтобы у вас был доступ к административному общему ресурсу на клиентском компьютере. Это можно проверить, выполнив команду **\\ИмяСетевогоКомпьютера\C$** из командной строки.

9. Обнаружение устройств в Active Directory

Раздел обнаружение устройств позволяет запустить процесс поиска необходимых устройств в структуре Active Directory. Первоначально необходимо добавить информацию о домене в консоль администрирования в разделе настройки Active Directory. После успешного добавление информации о домене необходимо запустить Поиск неуправляемых устройств для этого необходимо выполнить следующие шаги:

1. Для добавления параметров домена необходимо перейти по пути **Настройки → Настройки Active Directory.** Затем нажмите кнопку «Новая» в правом верхнем углу.



2. Задайте параметры домена Active Directory. Вы можете проверить состояние соединения, нажав кнопку «Тестовое соединение». Сохраните настройки.

Домен

Полное доменное имя должно быть введено в формате Distinguished Name (DN). Например,

Каноническое имя	Выдающееся имя
mydomain.com	DC=mydomain,DC=com
division.mydomain.com	DC=division,DC=mydomain,DC=com
sales.division.mydomain.com	DC=sales,DC=division,DC=mydomain,DC=com

Примечание: Если у вас есть OU, домен должен быть введен в формате OU=Staff,DC=mydomain,DC=com

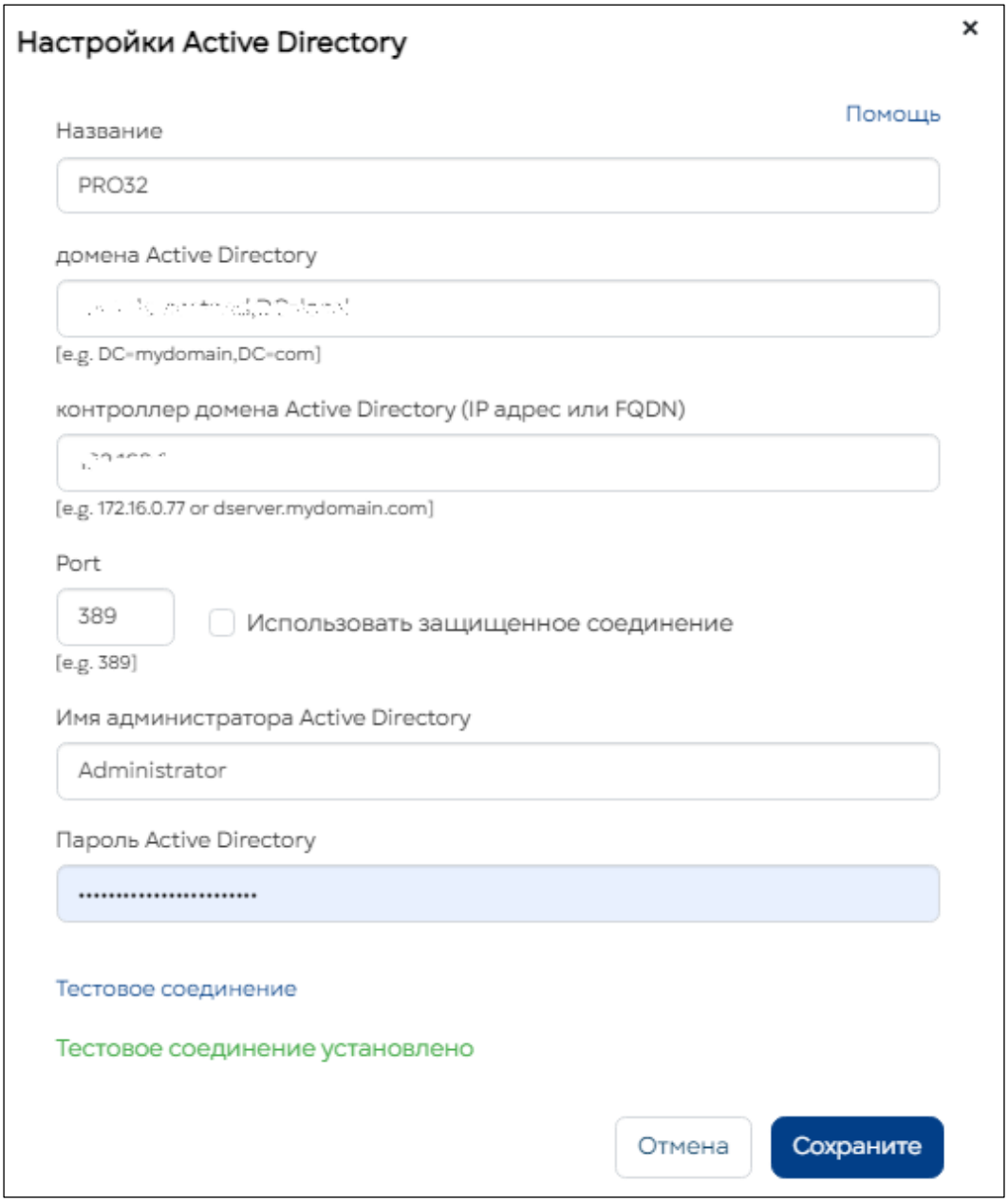
Контроллер домена

Необходимо ввести имя сервера контроллера домена. Имя компьютера не должно включать доменное имя.

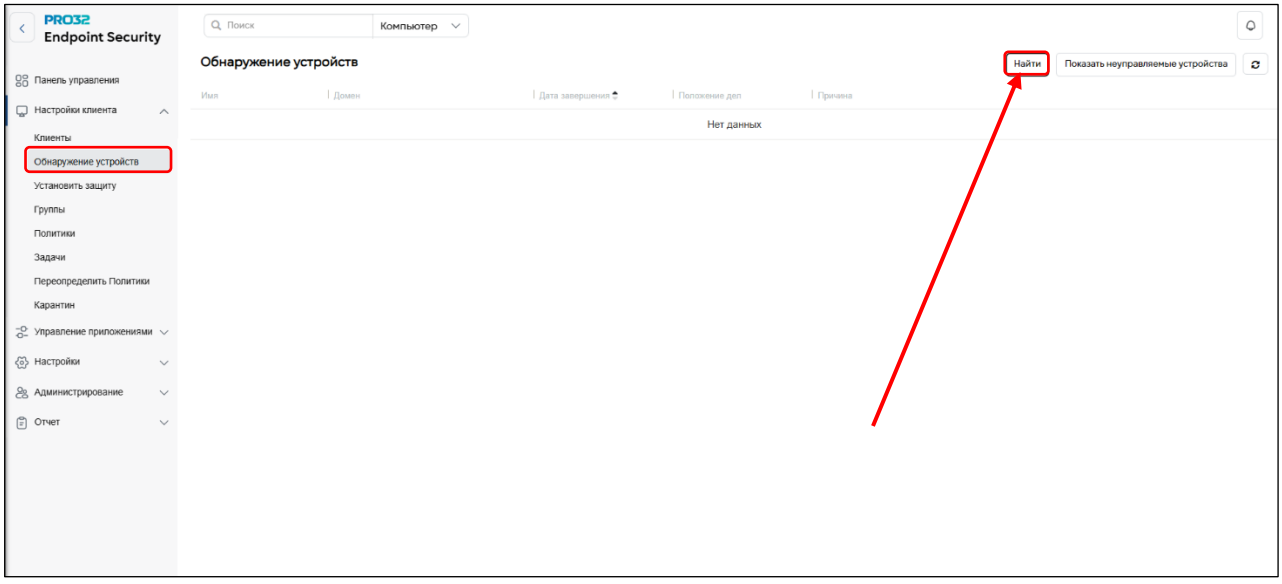
Например, если имя компьютера контроллера домена **dserver.mydomain.com**, Только **dserver** необходимо ввести.

Domain Administrator Credentials

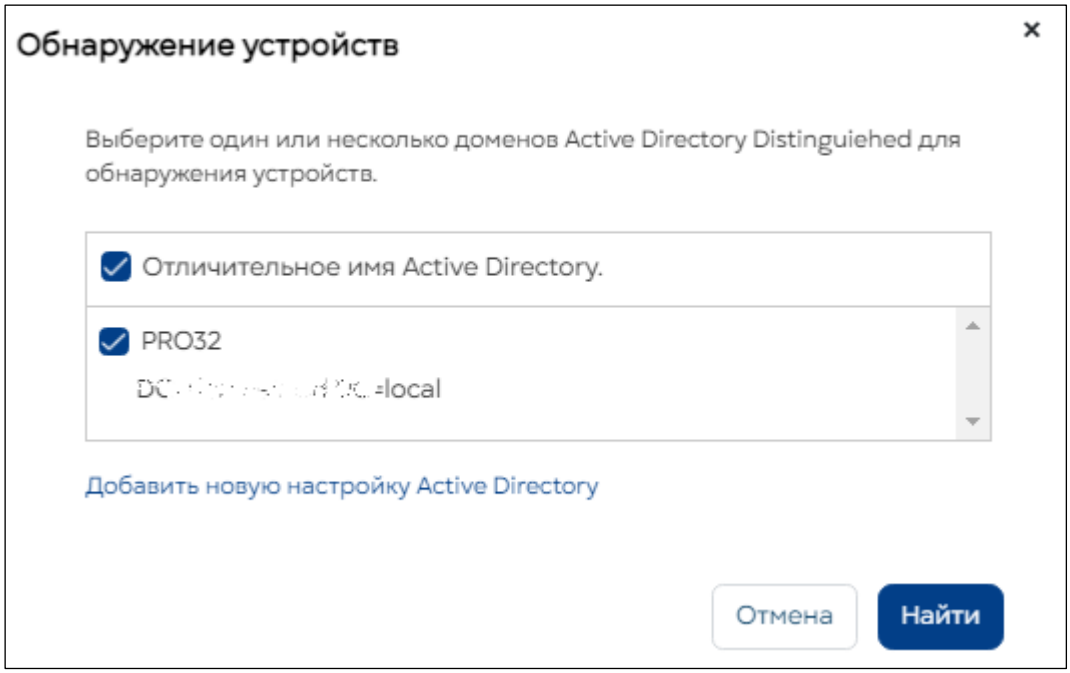
Имя пользователя и пароль администратора домена необходимы для получения списка компьютеров из Active Directory.



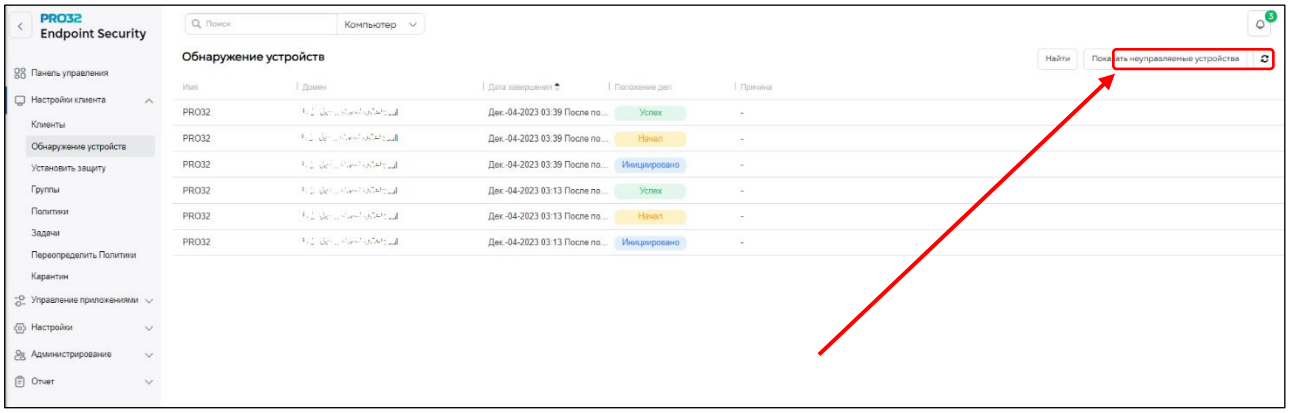
3. В панели навигации (слева), перейдите в раздел Настройки клиента – Обнаружение устройств. Нажмите кнопку **«Найти»** в правом верхнем углу.



4. Выберите один или несколько доменов Active Directory Distinguiehed для обнаружения устройств, которые вы настроили ранее.



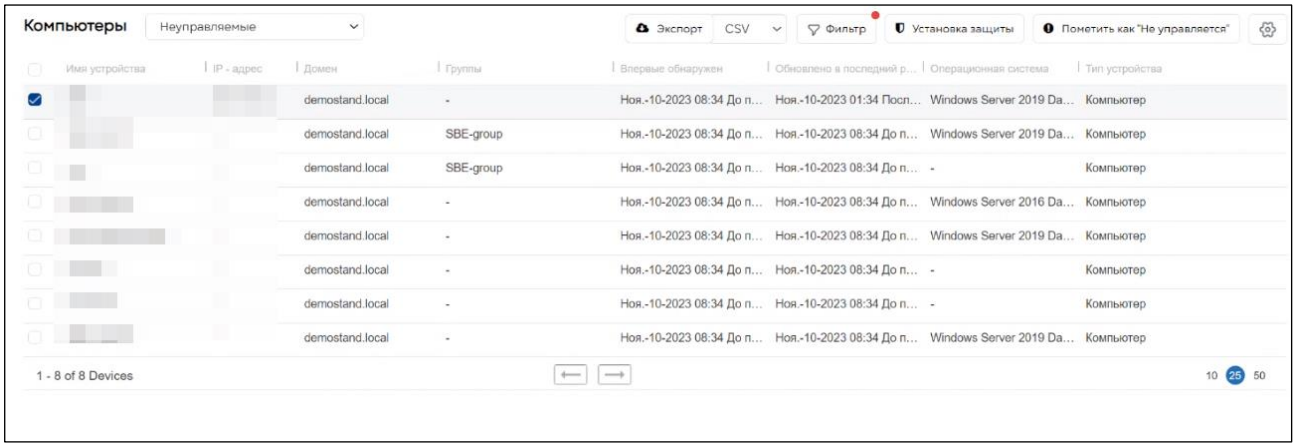
4. После успешного запуска поиска устройств в разделе неуправляемые устройств появится список:



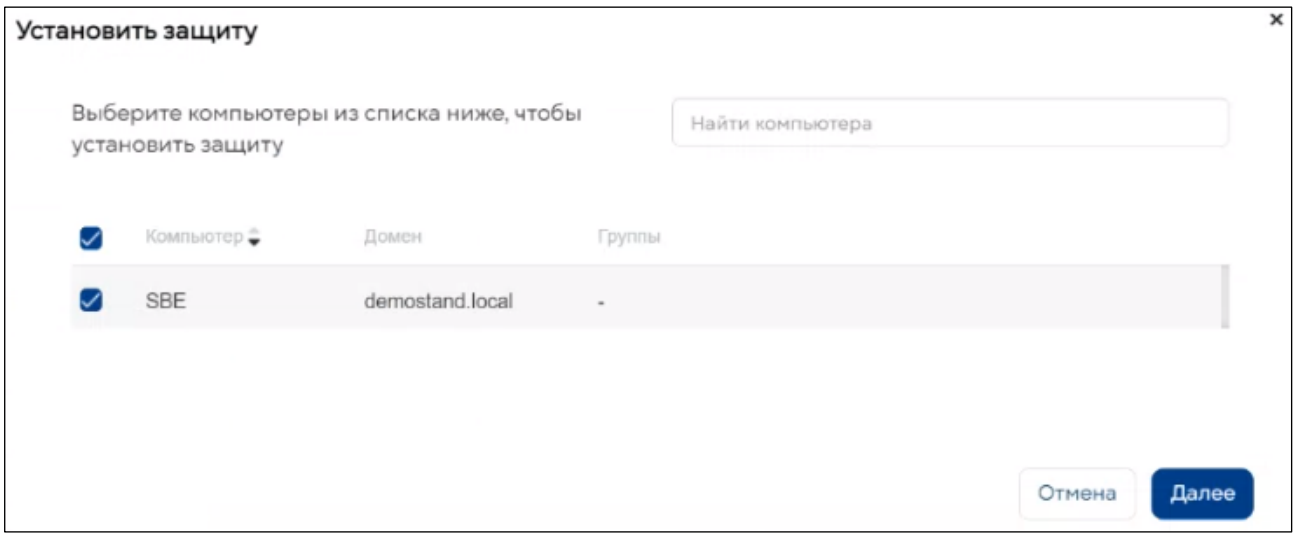
Важно!

Сканирование проводится в фоновом режиме и требует некоторого времени. Может показаться, что ничего не происходит. Воспользуйтесь кнопкой «обновить» в правом верхнем углу или нажмите комбинацию клавиш Ctrl+F5.

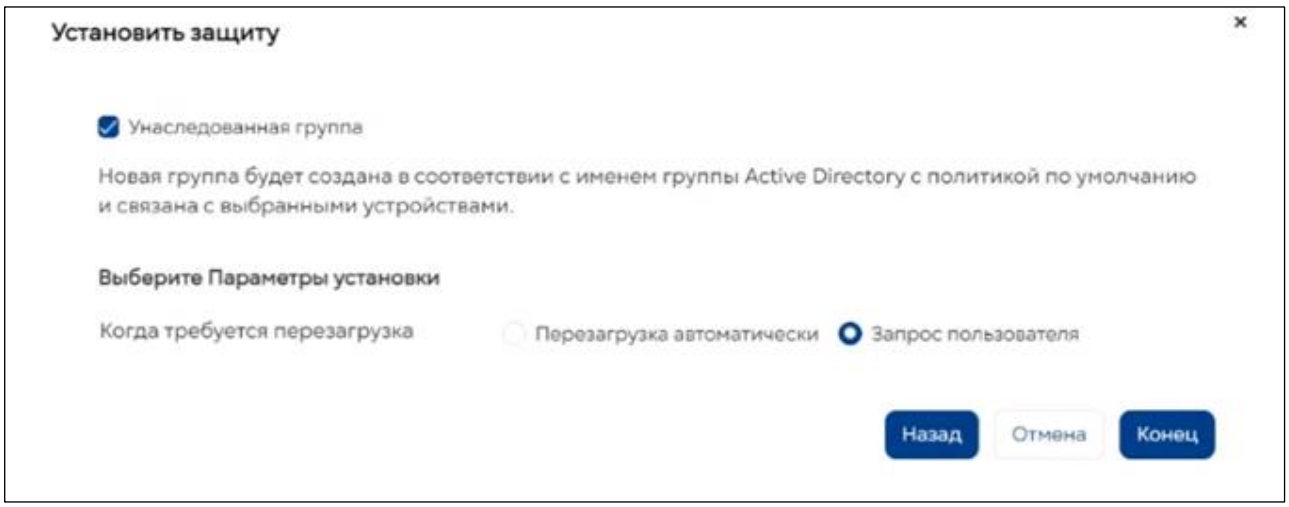
5. В списке необходимо выбрать устройства, на которых необходимо установить продукт безопасности и нажать Установка защиты.



6. Далее необходимо подтвердить выбор устройств, на которых необходимо установить клиентский дистрибутив.



7. Выберите параметры перезагрузки устройства после установки продукта безопасности и завершить установку защиты клиентского компьютера.



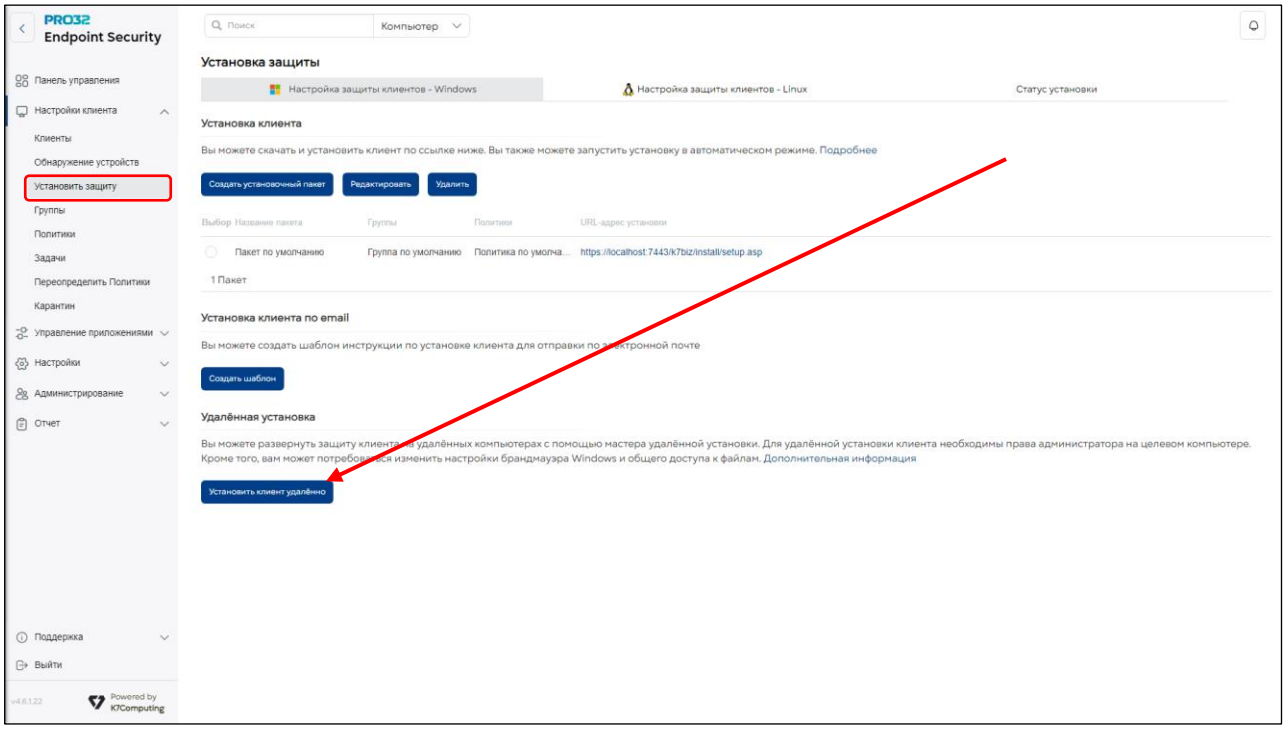
10. Удаленная установка PRO32 Endpoint Security

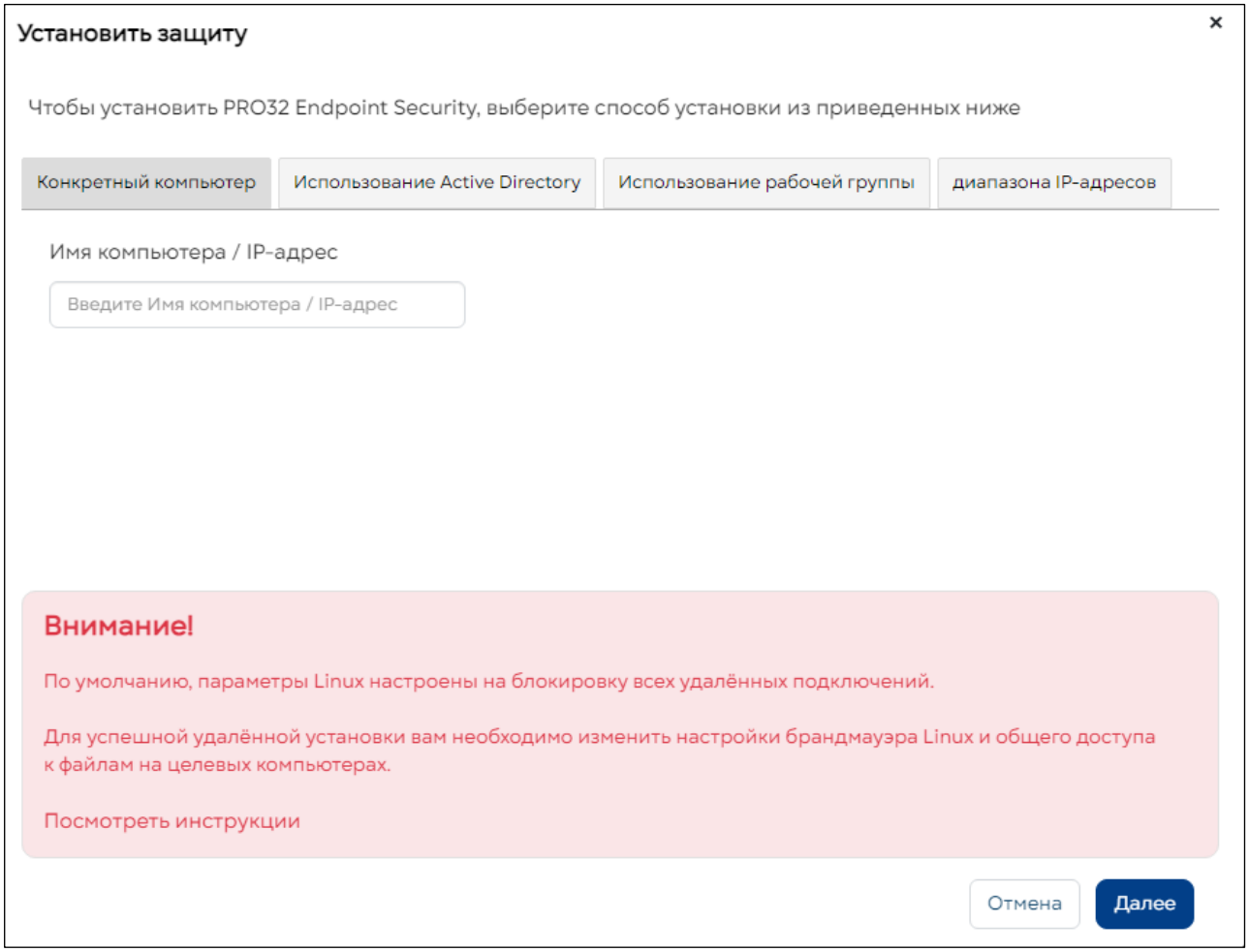
После выполнения указанных выше подготовительных шагов (9. Обнаружение устройств в Active Directory), развертывание PRO32 Endpoint на клиентских компьютерах становится простым процессом.

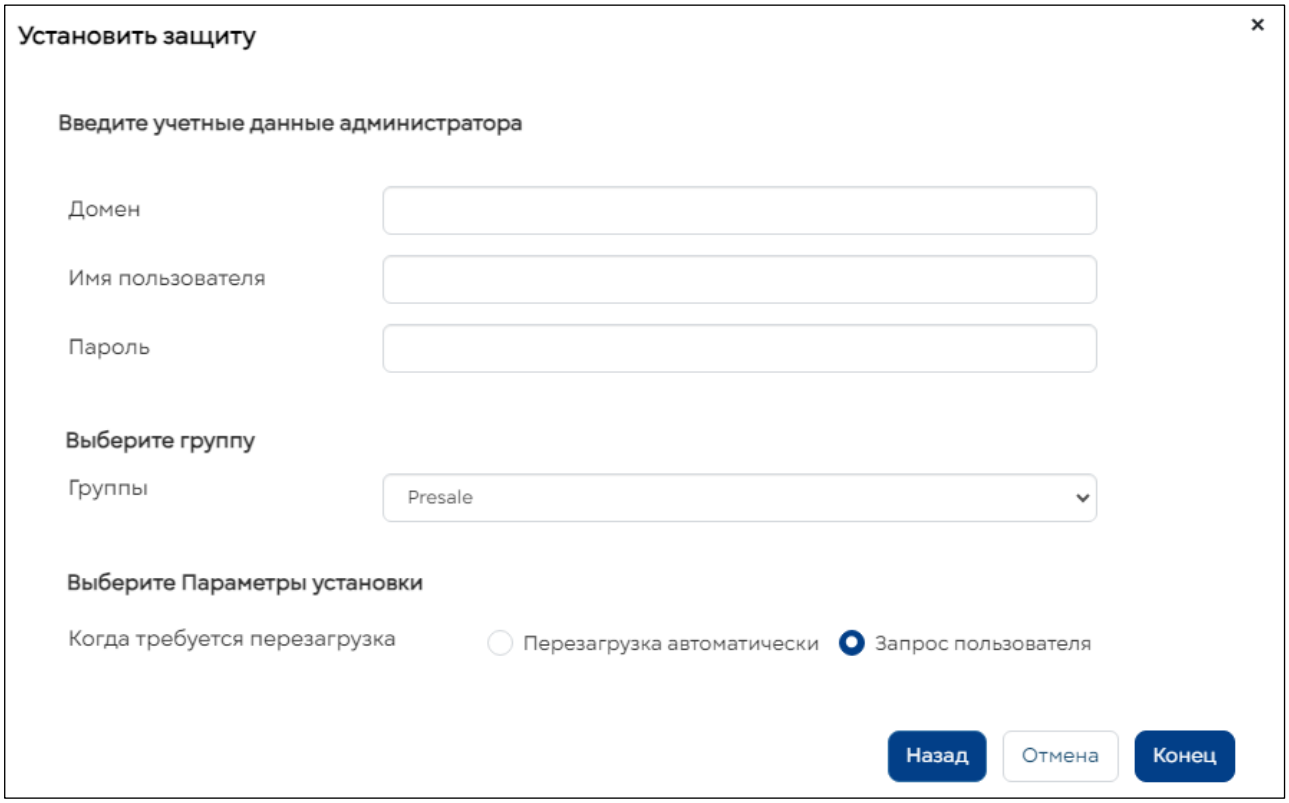
1. Откройте мастер удаленной установки. Для этого перейдите по пути **Настройки клиента → Установить защиту → Удаленная установка → Установка защиты**.

2. Укажите имя или IP-адрес клиентского компьютера, на который вы хотите установить PRO32 Endpoint Client, или воспользуйтесь **«Поиском компьютера в сети».**

3. Укажите имя пользователя рабочей группы и пароль для выбранных компьютеров.


PRO32
Endpoint Security
Панель управления
Настройки клиента
Клиенты
Обнаружение устройств
Установить защиту
Группы
Политики
Задачи
Переопределить Политики
Карантин
Управление приложениями
Настройки
Администрирование
Отчет
Поддержка
Выйти
Powered by KTComputing
Поиск
Компьютер
Установка защиты
Настройка защиты клиентов - Windows
Настройка защиты клиентов - Linux
Статус установки
Установка клиента
Вы можете скачать и установить клиент по ссылке ниже. Вы также можете запустить установку в автоматическом режиме. Подробнее
Создать установочный пакет
Редактировать
Удалить
Выбор Название пакета
Группы
Политики
URL-адрес установки
Пакет по умолчанию
Группа по умолчанию
Политика по умолча...
https://localhost:7443/k7biz/install/setup.asp
1 Пакет
Установка клиента по email
Вы можете создать шаблон инструкции по установке клиента для отправки по электронной почте
Создать шаблон
Удалённая установка
Вы можете развернуть защиту клиента на удалённых компьютерах с помощью мастера удалённой установки. Для удалённой установки клиента необходимы права администратора на целевом компьютере. Кроме того, вам может потребоваться изменить настройки брандмауэра Windows и общего доступа к файлам. Дополнительная информация
Установить клиент удалённо


Установить защиту
Чтобы установить PRO32 Endpoint Security, выберите способ установки из приведенных ниже
Конкретный компьютер
Использование Active Directory
Использование рабочей группы
диапазона IP-адресов
Имя компьютера / IP-адрес
Введите Имя компьютера / IP-адрес
Внимание!
По умолчанию, параметры Linux настроены на блокировку всех удалённых подключений.
Для успешной удалённой установки вам необходимо изменить настройки брандмауэра Linux и общего доступа к файлам на целевых компьютерах.
Посмотреть инструкции
Отмена
Далее

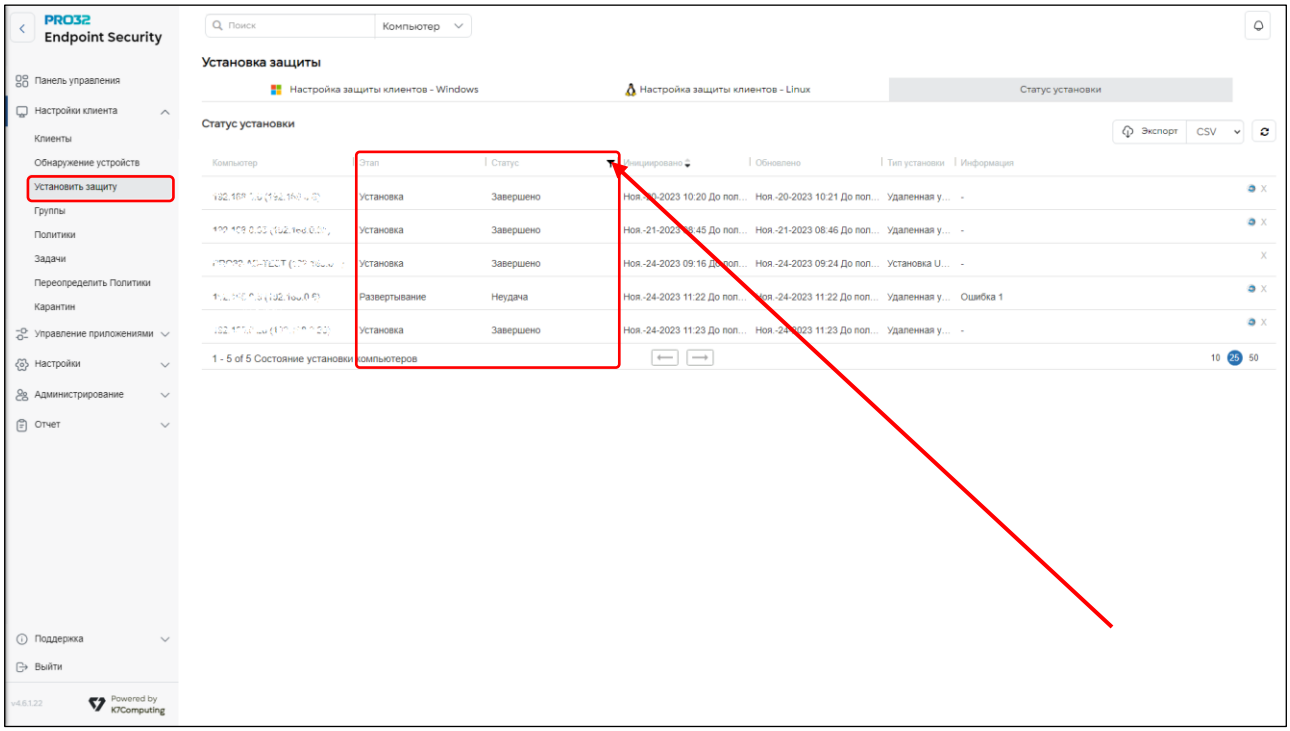


4. Укажите группу, которую вы хотите применить к выбранным компьютерам, и способ перезагрузки компьютера при установке.
5. Нажмите «Закончить».

11. Статус удаленной установки

Статус клиентских установок можно проверить по таблице **Статус удаленной установки**. В этой таблице отображается следующая информация (чтобы открыть таблицу, перейдите по пути **Управление клиентами ➔ Установка защиты ➔ Вкладка Статус защиты клиента**:

- Имя / IP-адрес компьютера
- Этап установки (удаленная push-установка, установка, удаление сторонних продуктов, уже установлено и т д.)
- Статус установки. Вы можете отфильтровать колонку по событиям: распределена, инициализирована, сбой, успешно начата, ожидание перезагрузки пользователем, успешно завершена и т. д.
- Дата и время инициализации
- Дата и время обновления
- Тип установки
- Информация о сбое

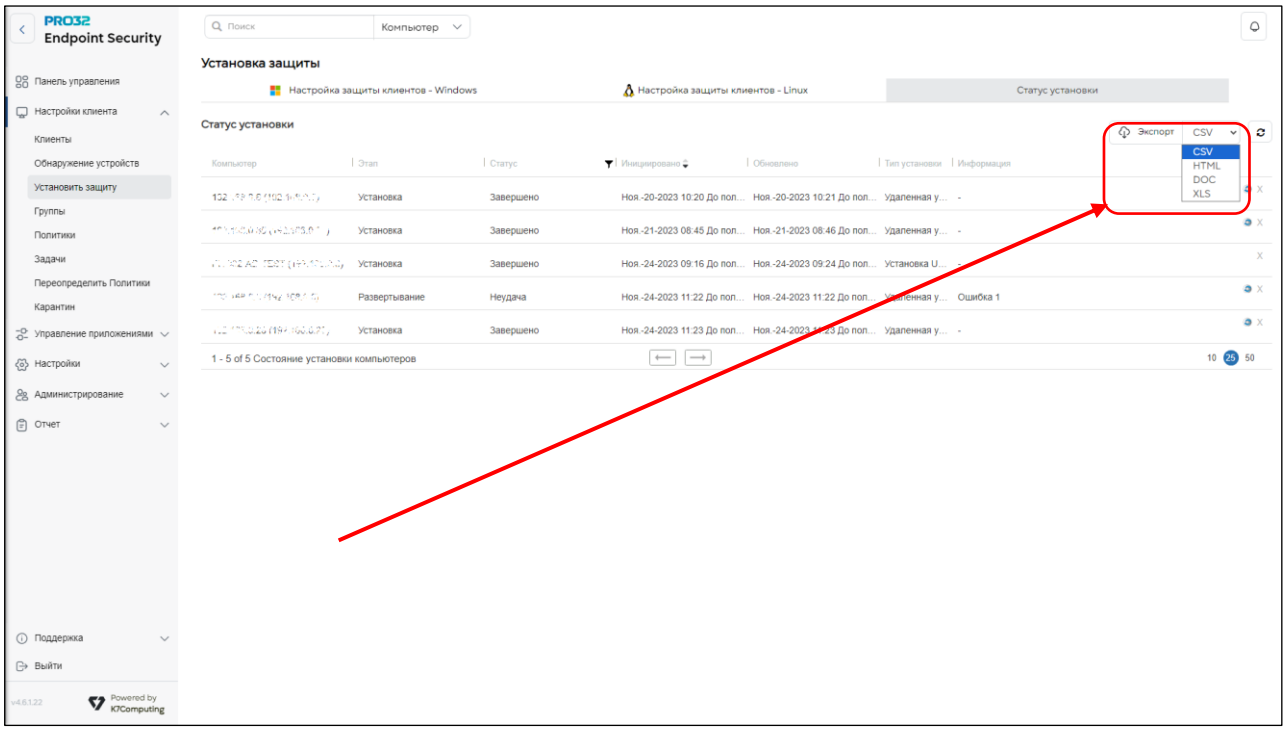


Экспорт результатов установки на клиентские компьютеры

Эта функция позволяет экспортировать информацию о статусах установки антивирусного ПО на клиентские компьютеры в различных форматах – CSV, HTML, DOC и XLS. Если в представлении установлен фильтр или сортировка, они тоже будут применены к экспортируемым данным.

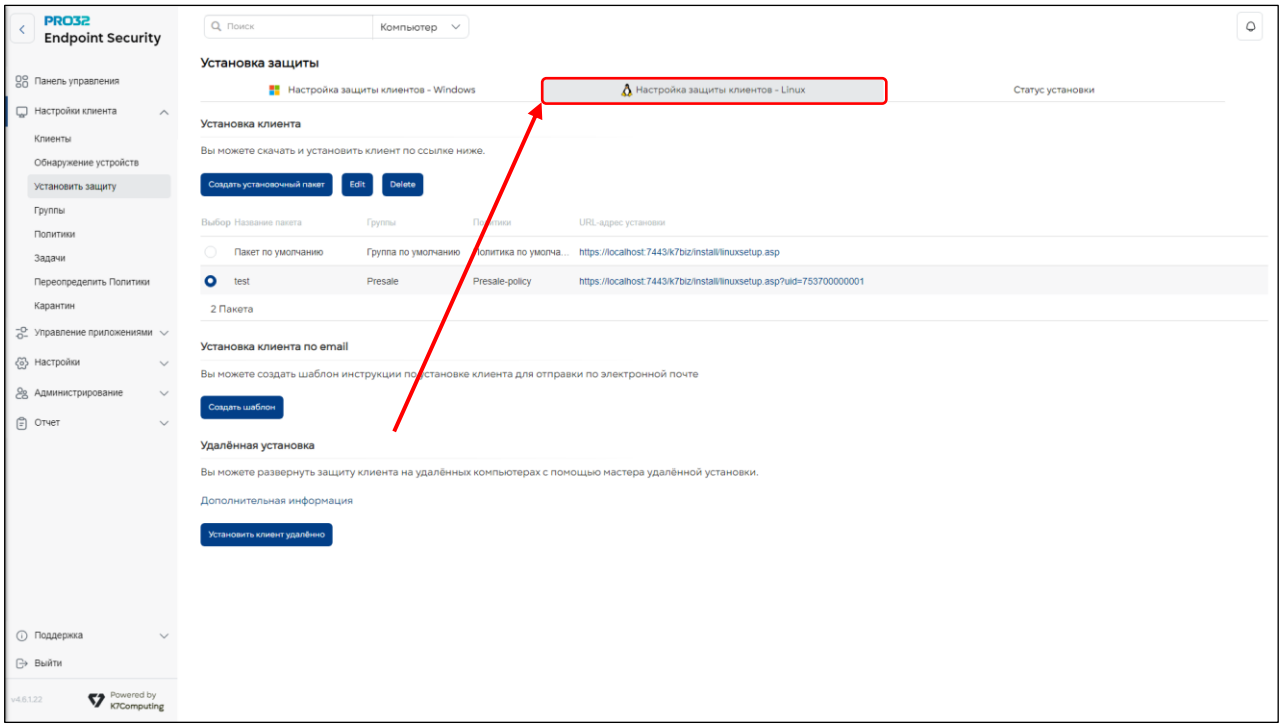
Экспорт результатов установки на клиентские компьютеры

- **Шаг 1.** Перейдите по пути Настройки клиента → Установить защиту.
- **Шаг 2.** Откройте вкладку «Статус установки клиента».
- **Шаг 3.** Выберите тип экспортируемого файла из выпадающего списка (CSV, HTML, DOC или XLS).



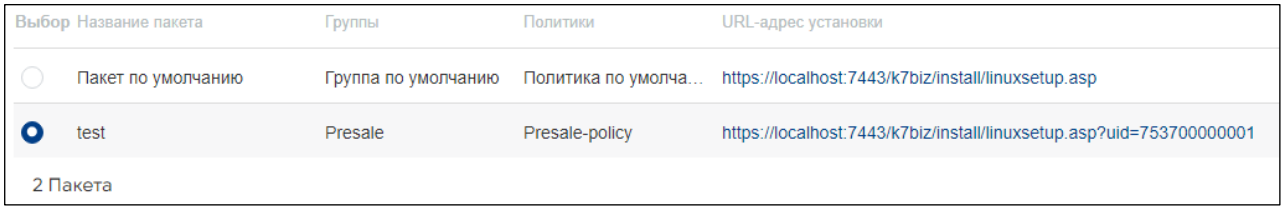
12. Установка PRO32 Endpoint Security на Linux

1. Локальная установка продукта
2. Удаленная установка через задачу в консоли администрирования
3. Установка через приглашение на электронную почту
4. Чтобы перейти к любому из вышеупомянутых способов установки, запустите консоль сервера и перейдите в **раздел Управление клиентами -> Установить защиту, затем нажмите Настройка защиты клиентов – Linux**



Локальная установка клиента для Linux:

Сгенерируйте мастер установки клиента Linux в консоли администрирования и загрузите данный пакет на Linux.



Для установки необходимо запустить установочный пакет со следующими параметрами последовательно:

1.tar –xf <downloaded setup file>

2.sudo ./k7installer <server ip address>:<ip port

Удаленная установка:

Перед запуском процесса удаленной принудительной установки следует выполнить указанные ниже условия в системе Linux, а затем продолжить установку в консоли администрирования

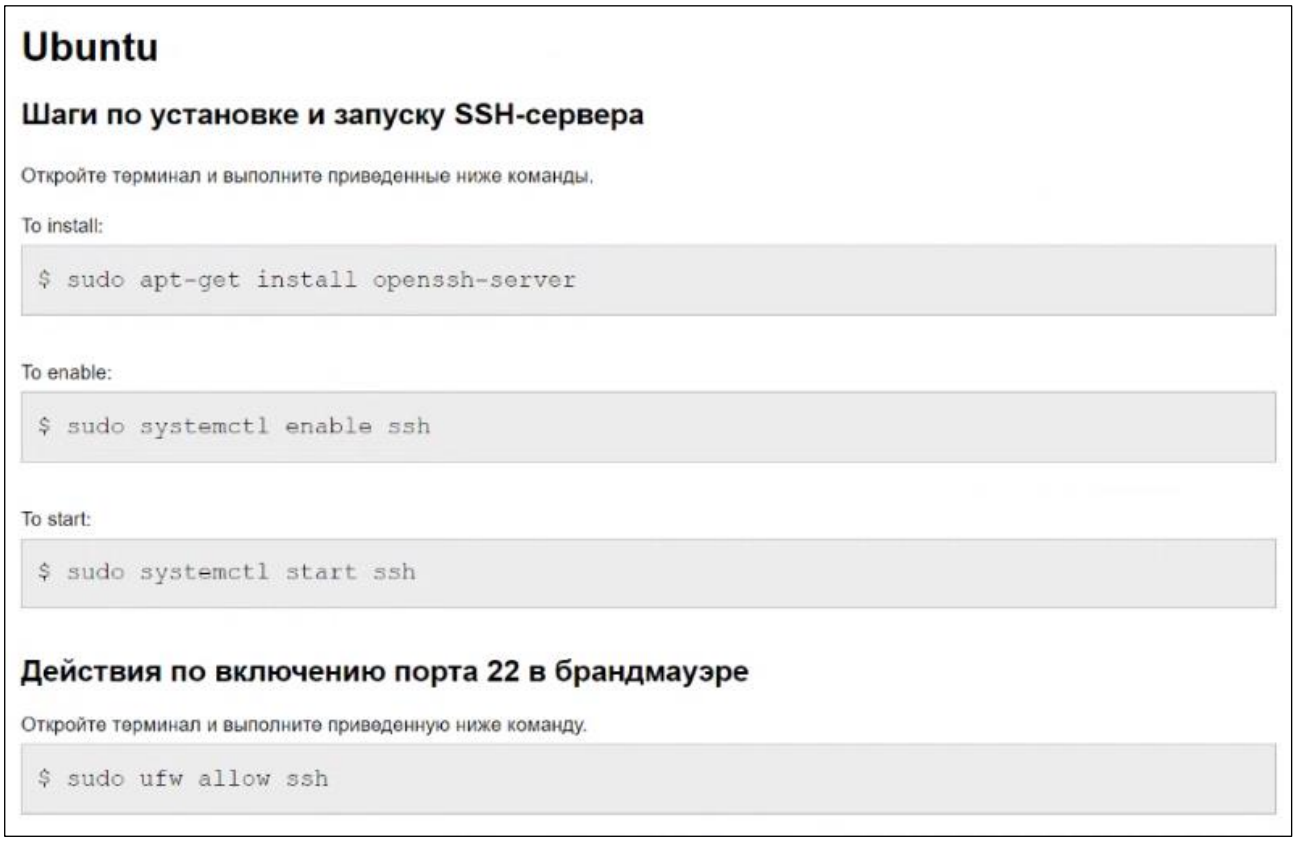
Для удаленной установки защиты конечных точек вам потребуются права администратора на целевом устройстве. Кроме того, вам также может потребоваться изменить настройки брандмауэра.

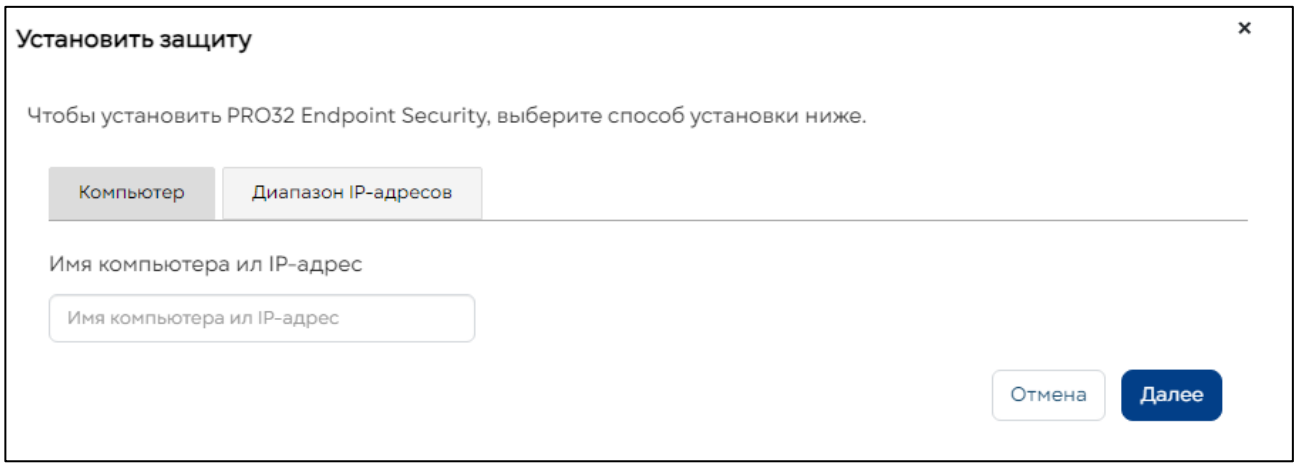
Пожалуйста, убедитесь в следующем:

- ✓ Имя пользователя, указанное во время удаленной установки, должно иметь права администратора на целевом устройстве.
- ✓ Сервер OpenSSH должен быть установлен и запущен на целевом устройстве.
- ✓ Порт 22 должен быть разрешен в брандмауэре для удаленного подключения к целевому устройству.

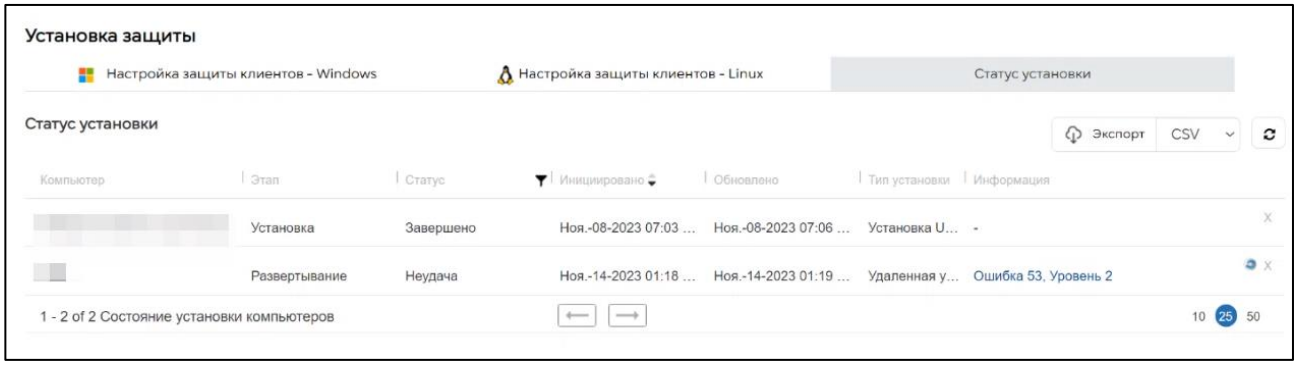
Нажмите "Установить защиту", затем введите IP-адрес системы Linux и нажмите **«Далее»**

Введите учетные данные для входа в систему Linux и нажмите **«Готово».**





Проверьте статус установки в разделе Статус установки:

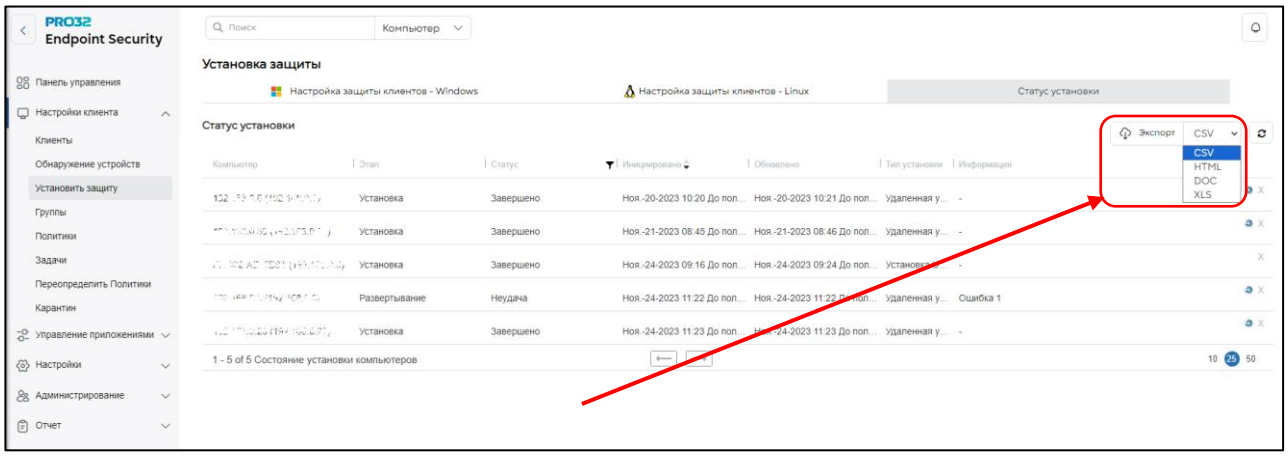


Экспорт результатов установки на клиентские компьютеры

Эта функция позволяет экспортировать информацию о статусах установки антивирусного ПО на клиентские компьютеры в различных форматах – CSV, HTML, DOC и XLS. Если в представлении установлен фильтр или сортировка, они тоже будут применены к экспортируемым данным.

Экспорт результатов установки на клиентские компьютеры

- **Шаг 1.** Перейдите по пути Настройки клиента → Установить защиту.
- **Шаг 2.** Откройте вкладку «Статус установки клиента».
- **Шаг 3.** Выберите тип экспортируемого файла из выпадающего списка (CSV, HTML, DOC или XLS).



13. Политики

Политики – это настраиваемые параметры безопасности для управления компьютерами, находящимися в сети (клиенты). Вы можете использовать различные политики для управления безопасностью своих компьютеров и сети.

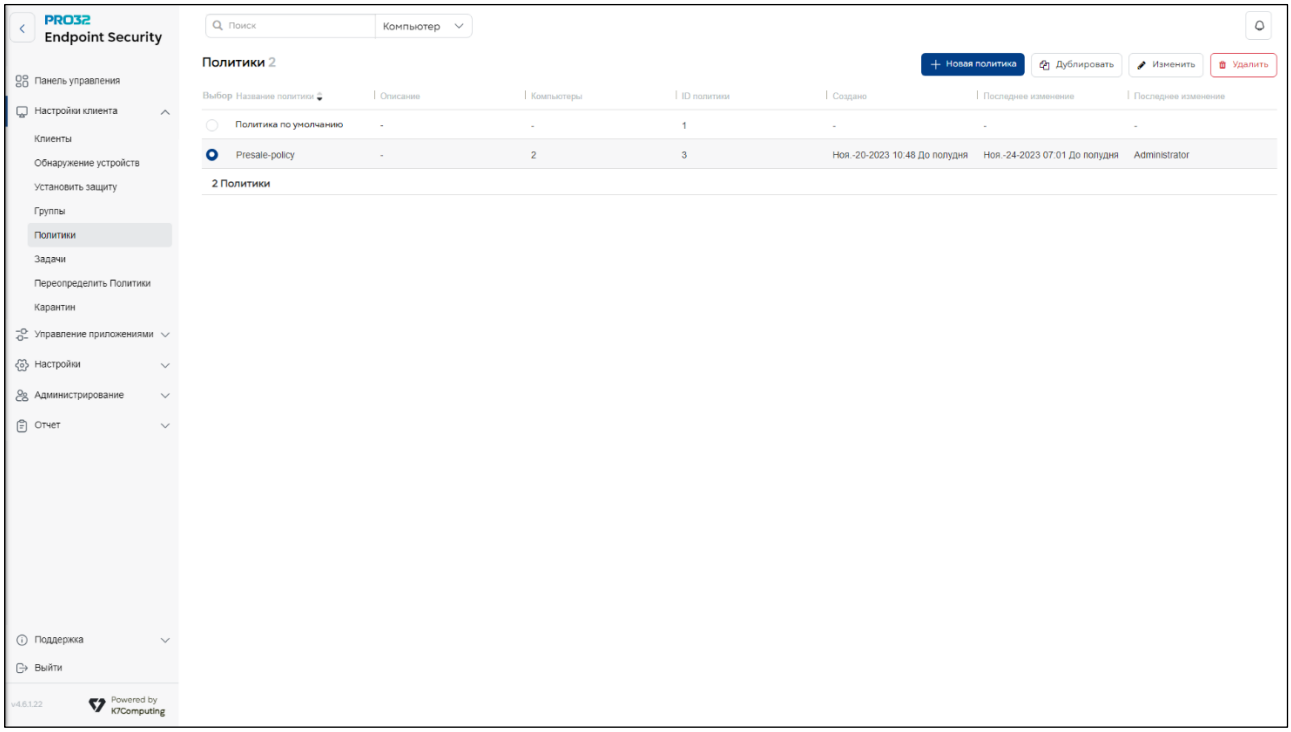
Политика по умолчанию всегда создается во время первоначальной установки. Вы можете применить политику по умолчанию к компьютерам или создать свои собственные политики в соответствии с вашими конкретными требованиями в области безопасности. Как только политика создана, она может быть назначена клиентскому компьютеру(ам) или группе(ам).

Созданные вами политики перечислены на странице Политики, а также содержат следующую информацию:

- ✓ Название политики
- ✓ Описание Политики
- ✓ Количество компьютеров, в группе
- ✓ ID политики
- ✓ Дата и время создания политики и
- ✓ Последнее изменение

Вы можете создать новую политику с определенными параметрами безопасности. Кроме того, вы можете редактировать, копировать или удалять любую существующую политику.

Если пользовательские политики не созданы, Политика по умолчанию будет применена ко всем вновь добавленным клиентам.



14. Политика по умолчанию

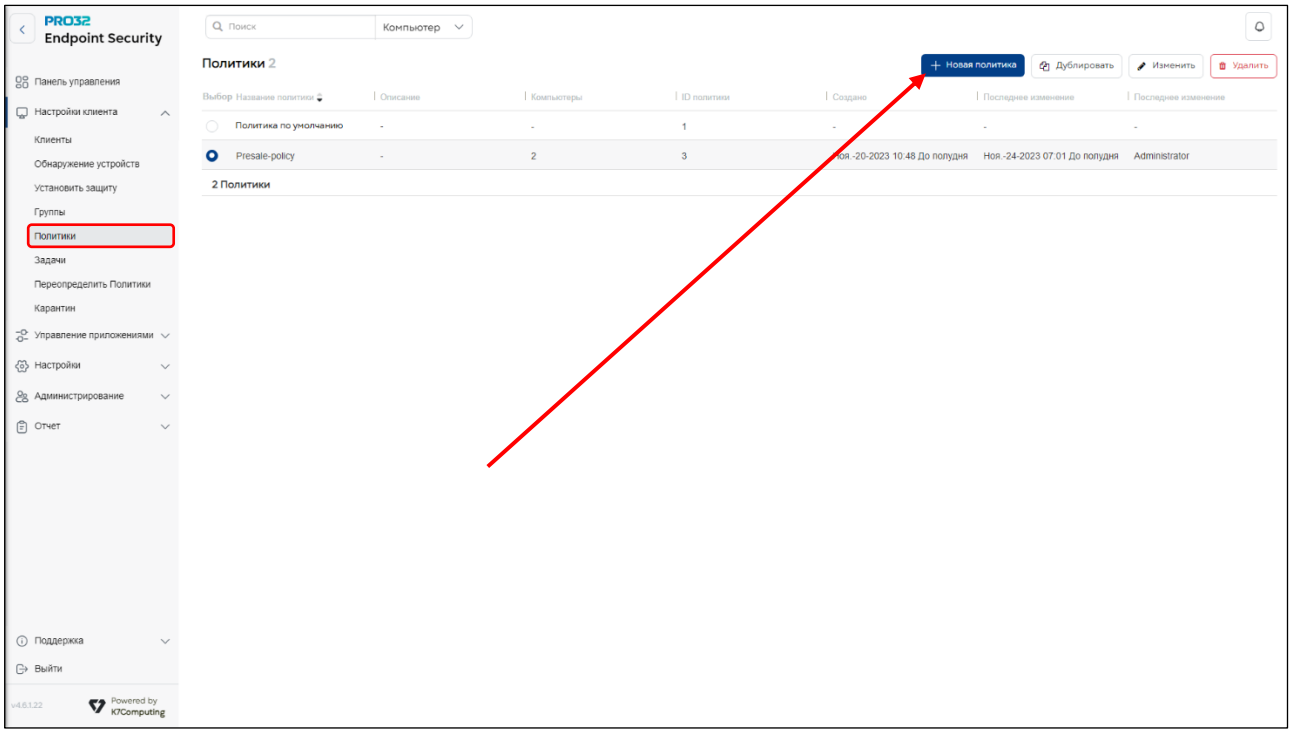
Политика по умолчанию с заводскими настройками поставляется вместе с продуктом. Политика по умолчанию автоматически применяется к группе компьютеров, если у группы нет назначенной пользовательской политики. Всякий раз, когда добавляется новый клиент или группа, политика будет установлена в качестве политики по умолчанию, если иное не указано в какой-либо конкретной пользовательской политике. Политика по умолчанию не может быть изменена или удалена. Однако его можно просмотреть или скопировать, чтобы создать новую политику.

15. Создание новой политики

Вы можете создать новую политику в меню «**Политики»**. Отдельные компьютеры и группы могут использовать одну и ту же политику. Политика может быть назначена только после ее создания.

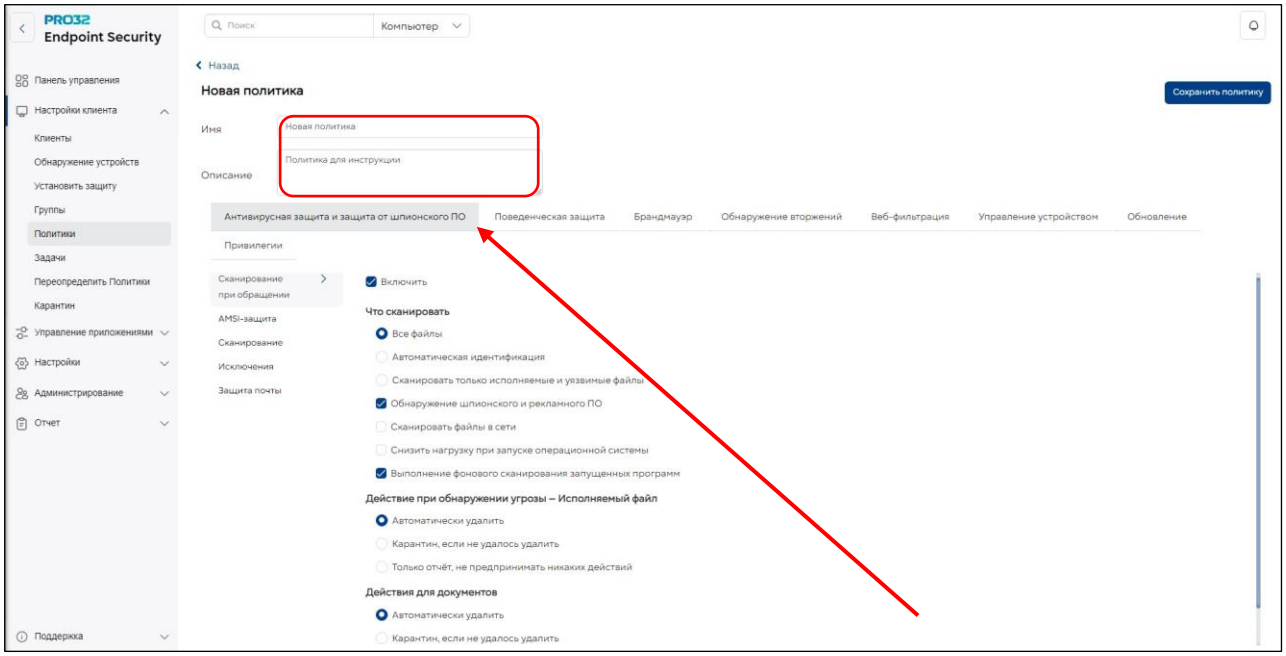
Выберите вкладку **«Настройки клиента»** в консоли администратора и выберите **«Политики»** на левой панели.

Нажмите кнопку **«Новая политика»**. На верхней панели отображаются различные разделы, такие как Антивирусная защита, поведенческая защита, брандмауэр, и.т.д. Введите подходящее имя и описание политики перед ее сохранением.



15.1 Вкладка «Антивирусная защита и защита от шпионского ПО»

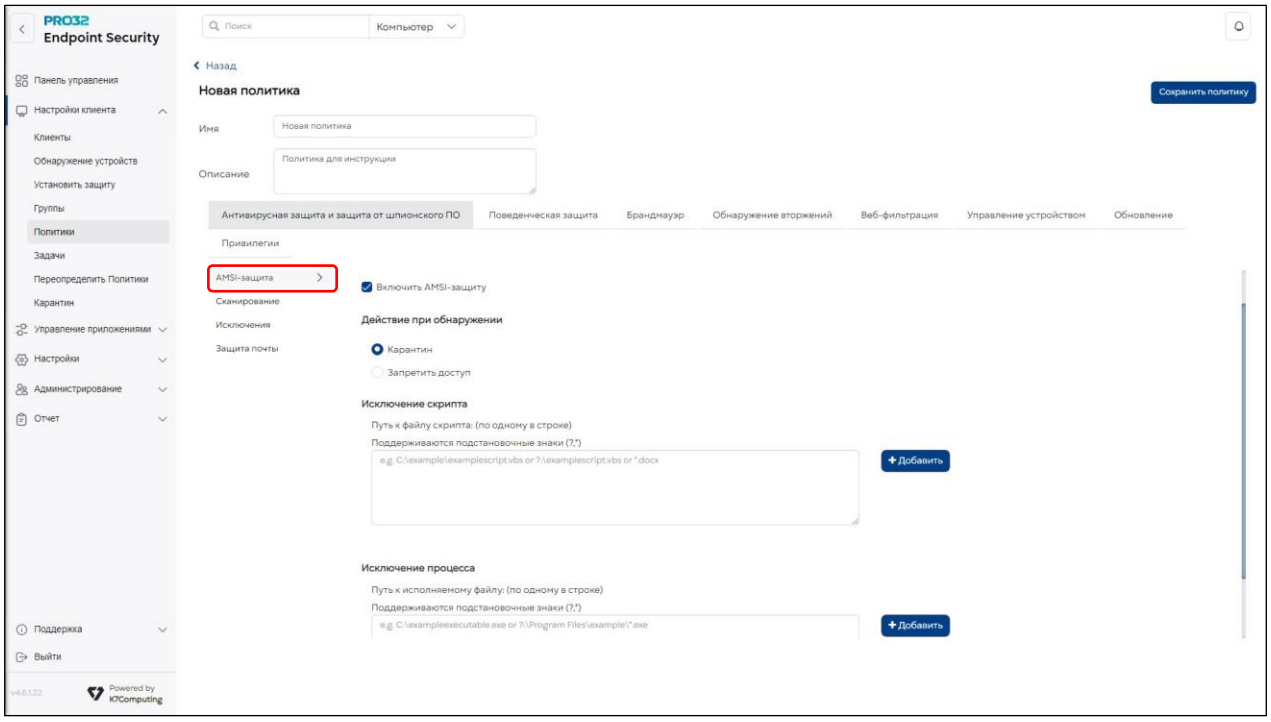
Укажите требуемые параметры работы антивирусного движка. Вы можете выбрать что сканировать, где сканировать и как сканировать. Так же задайте действия, которые должен производить антивирус при обнаружении угроз в исполняемых файлах или документах. На вкладке «Антивирусная защита и защита от шпионского ПО» есть разделы: Сканирование по обращению (автоматически сканирует новые файлы), AMSI защита, Пользовательское сканирование, Исключения и Защита почты.



15.1.1 Раздел «AMSI защита»

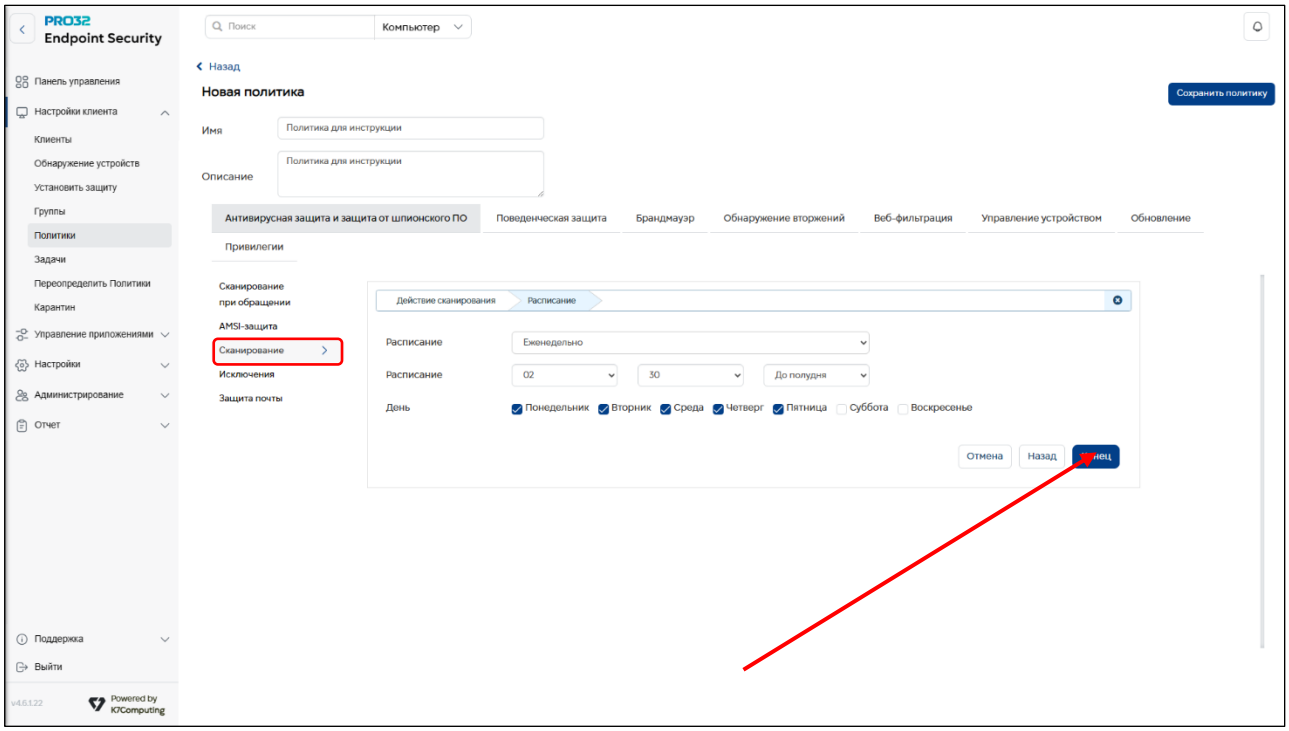
Antivirus Scan Interface (AMSI) защищает устройства от бесфайловых угроз, которые используют уязвимости программного обеспечения.

Эта функция применима для Endpoint под управлением операционных систем Windows 10, Windows Server 2016 или более поздних версий.



15.1.2 Раздел «Сканирование»

В данном разделе вы сможете выбрать типы оффлайн сканирования из уже преднастроенных или создать собственные правила и области сканирования, а также задать расписание, по которому будет производиться оффлайн сканирование. После завершения настройки, нажмите кнопку **«Завершить».** Настройки будут сохранены.

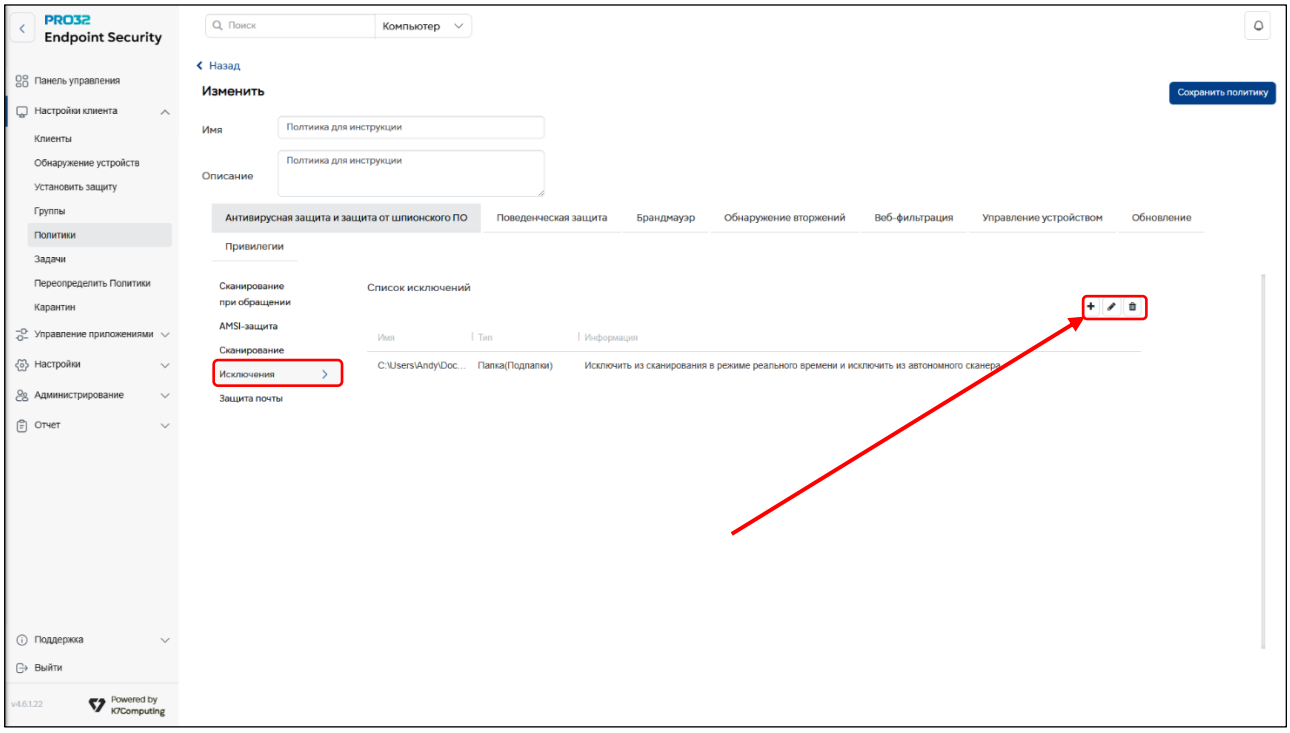


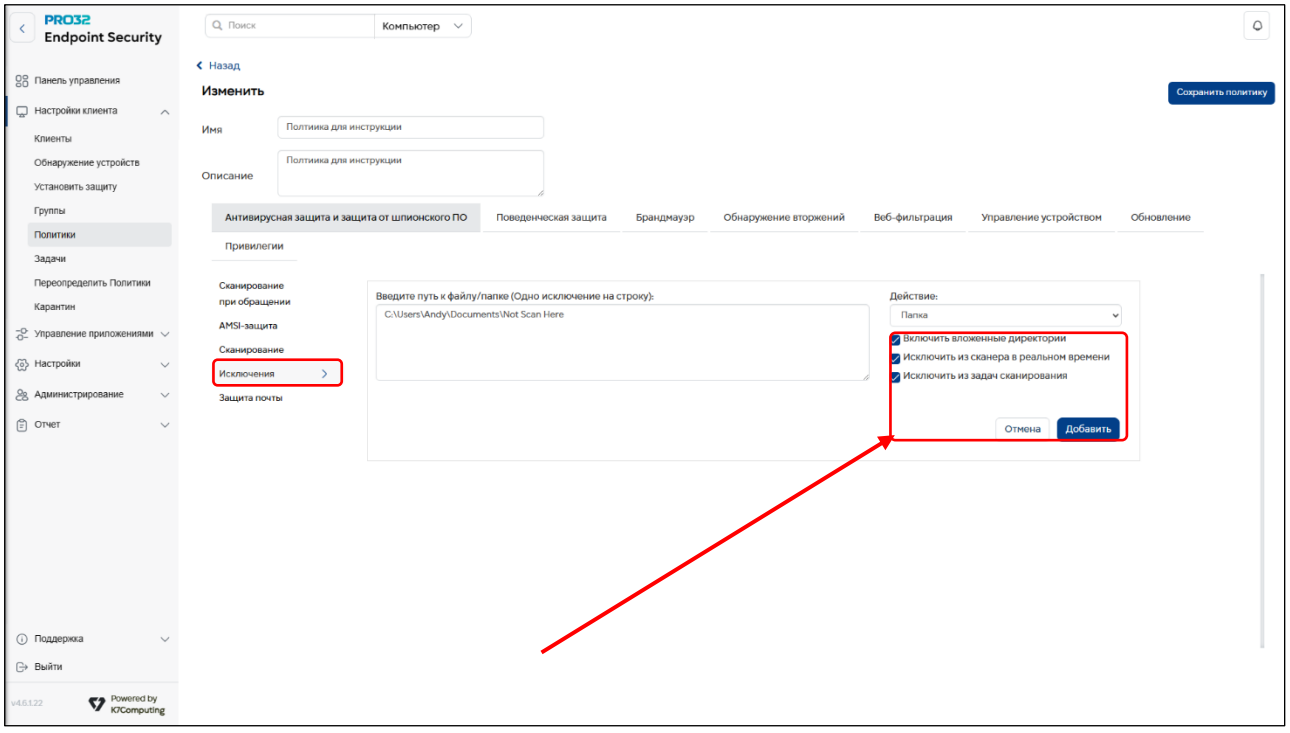
15.1.3 Раздел «Исключения».

Данный раздел позволяет добавить исполняемые файлы в исключение из сканирования. Таким образом продукт не будет детектировать исполняемые файлы, которые будут добавлены в исключения.

Важно!

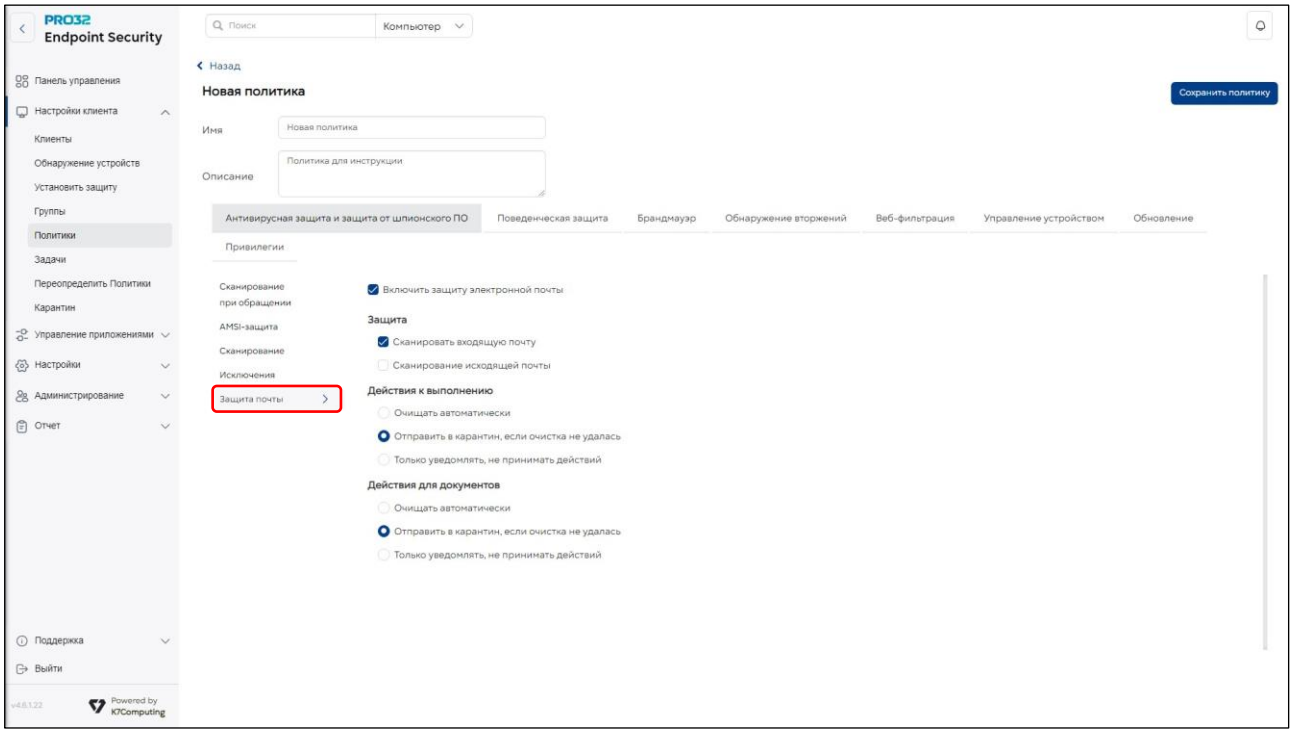
Для корректной работы инструмента исключений необходимо выбрать все опции исключений: из сканера в реальном времени и из оффлайн сканирования по расписанию, проставив соответствующие чекбоксы.





15.1.4 Раздел «Защита почты».

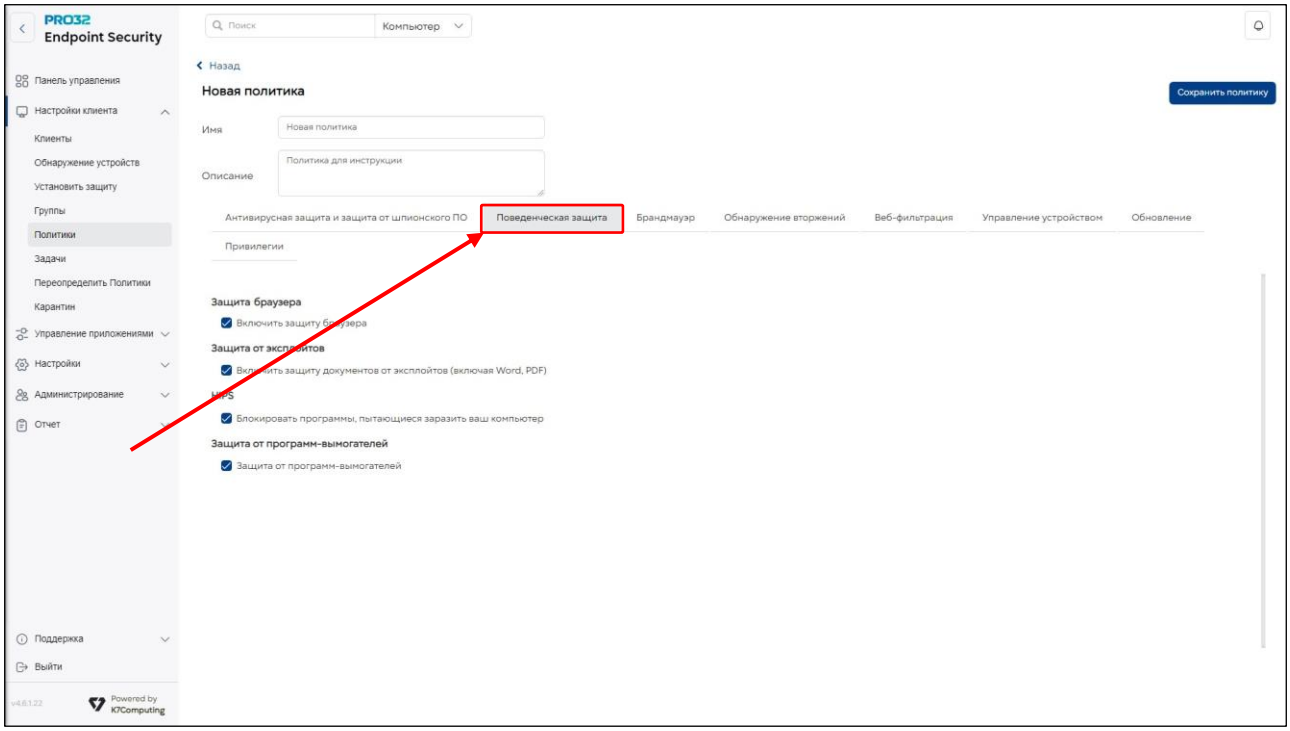
Антивирус может сканировать трафик на предмет протоколов IMAP и POP3. Вы можете выбрать сканировать ли только входящую почту, или только исходящую. Или весь трафик. Так же вы можете указать продукту, что делать с обнаруженными угрозами.



15.2. Вкладка «Поведенческая защита»

Позволяет вам настроить модули проактивной защиты. Вы можете включить защиту браузеров, Защиту от эксплойтов, HIPS [хостовая система предотвращения вторжений] - обнаруживает и блокирует подозрительные программы, чтобы не допустить повреждения вашей системы. А также модуль проактивной защиты от программ шифровальщиков.

Настоятельно рекомендуем не отключать данные опции для полноценной защиты.



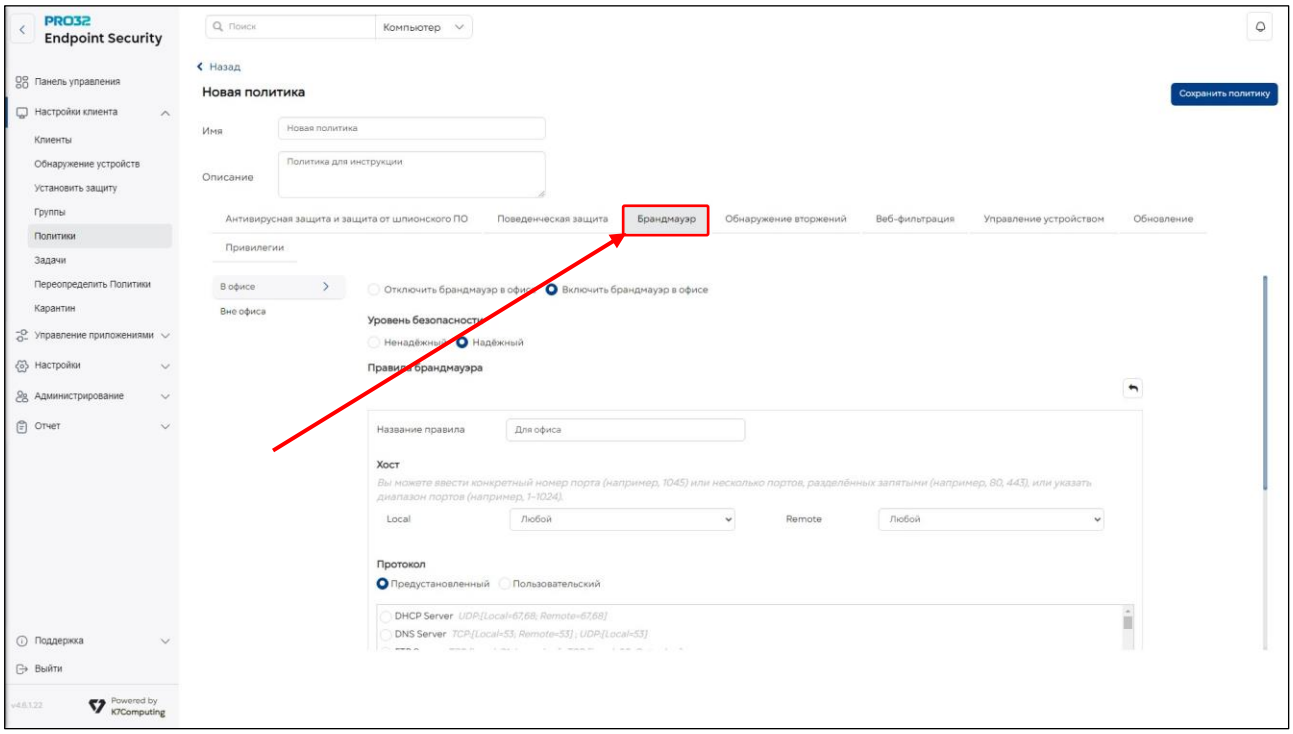
15.3. Вкладка «Брандмауэр».

Брандмауэр PRO32 защищает ваш компьютер от вторжений, нежелательных подключений, сканирования портов и хакерских атак. Он блокирует любые программы, которые пытаются получить доступ к Интернету, кроме тех, которые настроены вами как доверенные. Брандмауэр PRO32 обеспечивает упреждающую защиту для предотвращения входящих, исходящих и программных атак и делает ваш компьютер полностью невидимым для хакеров. Он предотвращает

отправку личной информации через Интернет шпионскими и другими вредоносными программами.

Когда брандмауэр PRO32 включен, он действует как барьер между вашим компьютером и Интернетом, незаметно отслеживая интернет-трафик, поступающий на ваш компьютер, на предмет подозрительной активности, а также предупреждая вас о потенциальных угрозах.

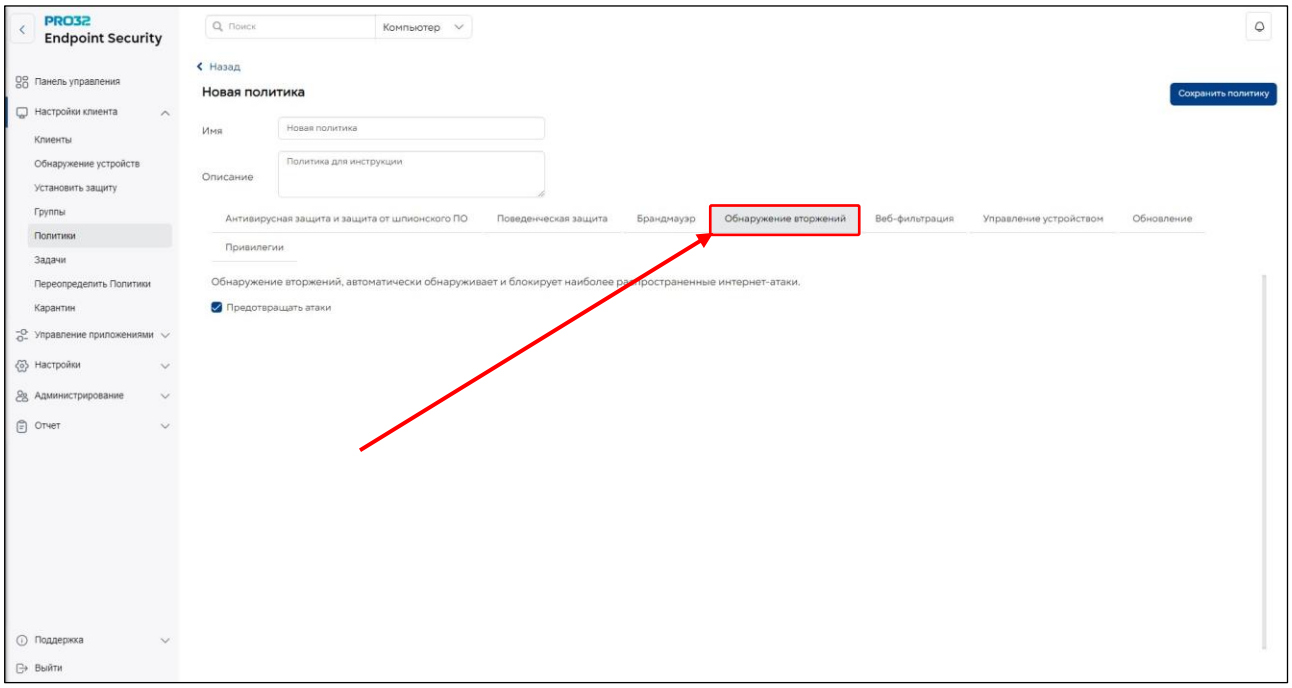
Вы можете настроить политику работы Брандмауера в зависимости от того где находится компьютер (клиент) «**В офисе»** или «**Вне офиса»**.



15.4. Вкладка «Обнаружение вторжений».

Данный модуль представляет собой защиту от наиболее распространенных интернет-атаки таких как переполнение буфера, Man-in-the-Middle (внедрение с целью получения пакетов, передаваемых внутри системы), XSS-атаки, Снифферы.

Настоятельно рекомендуем не отключать данные опции для полноценной защиты.



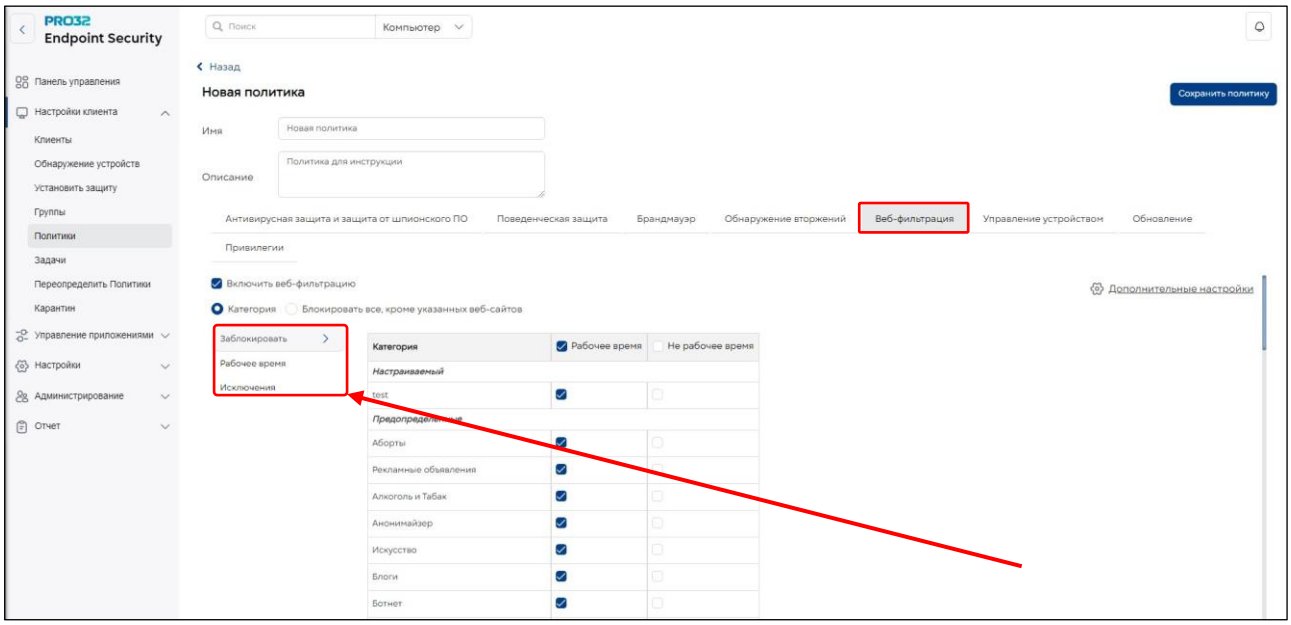
15.5. Вкладка «Веб-фильтрация».

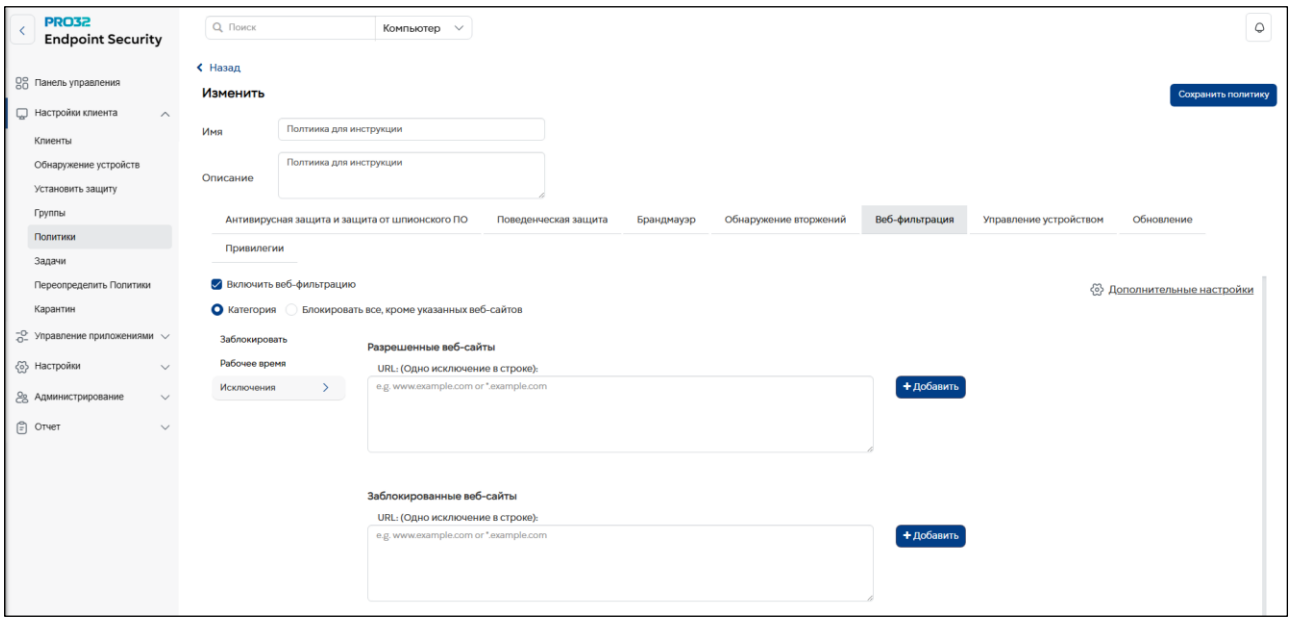
Доступ к различным веб-сайтам можно ограничить. Существует два способа ограничить доступ к веб-сайтам:

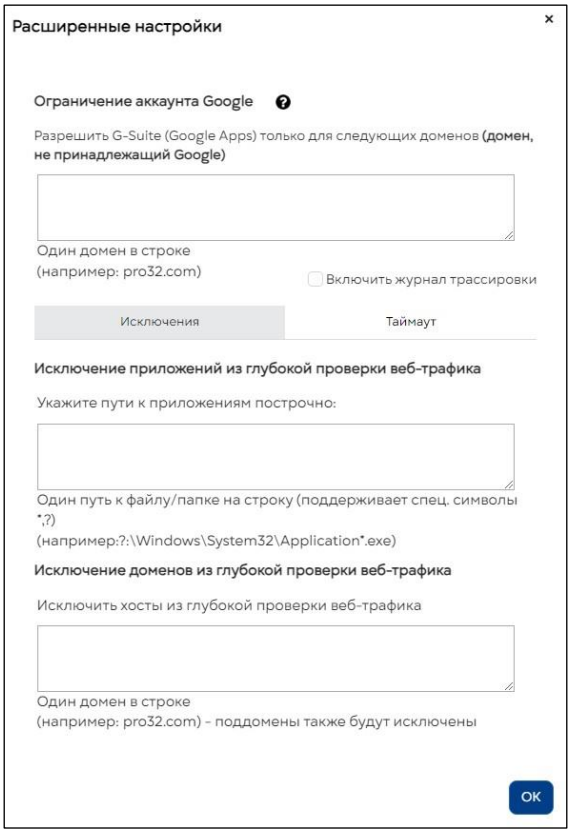
- Список разрешений: этот список содержит сайты, к которым пользователь имеет доступ. Доступ к сайтам, не включенным в этот список, заблокирован.

- Список блокировок: этот список содержит сайты, к которым у пользователя нет доступа. Доступ пользователя ко всем другим сайтам разрешен.

Вы можете настроить **«Фильтрацию по категориям»,** можете настроить политику в зависимости от рабочего времени **«Рабочее время» «Нерабочее время»**, или создать **«Собственные чёрные и белые списки»** url-адресов и доменов.



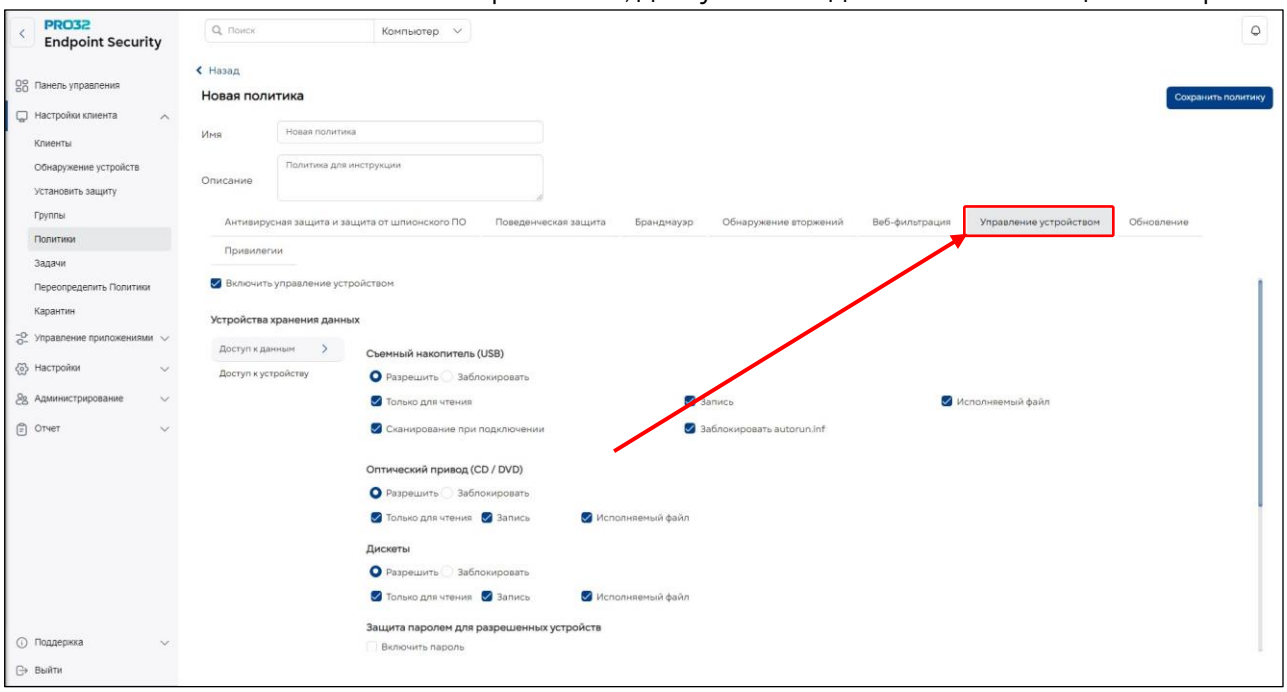




*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

15.6. Вкладка «Управление устройствами».

С ростом числа вредоносных программ, способных заражать вашу систему через такие устройства, как USB, важно обеспечить защиту доступа к этим устройствам. Функция доступа к устройствам позволяет контролировать доступ к USB-накопителям, CD-, DVD-дискам и дисководам гибких дисков. Вы можете управлять возможностью копирования файлов на диск или с диска, а также возможностью их выполнения. Кроме того, доступ к этим дискам можно защитить паролем.



*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

15.7. Вкладка «Обновление»

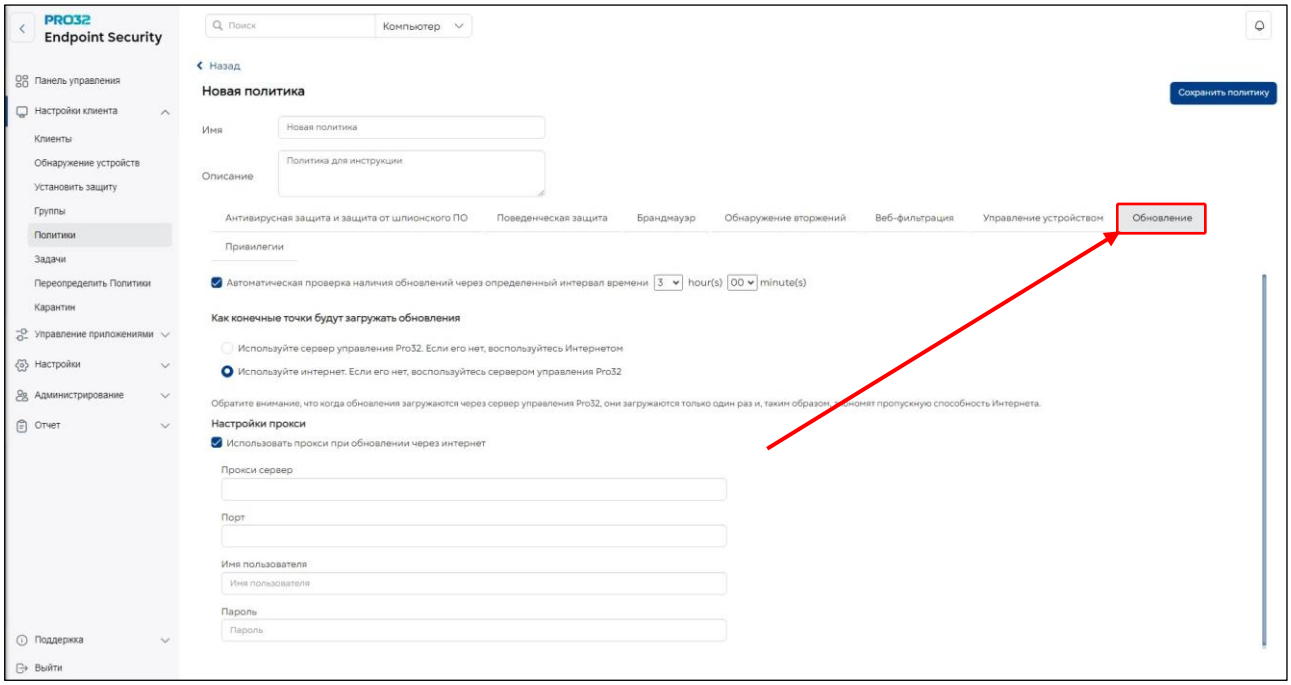
Позволит вам настроить политику обновления антивирусных сигнатур на клиентских компьютерах. Доступные опции:

- Сначала скачать обновлённую базу сигнатур на сервер администратора, на котором установлена консоль, а клиентские ПК будут обновляться уже с неё.

Обратите внимание, что, когда обновления загружаются через сервер управления, они загружаются только один раз и,

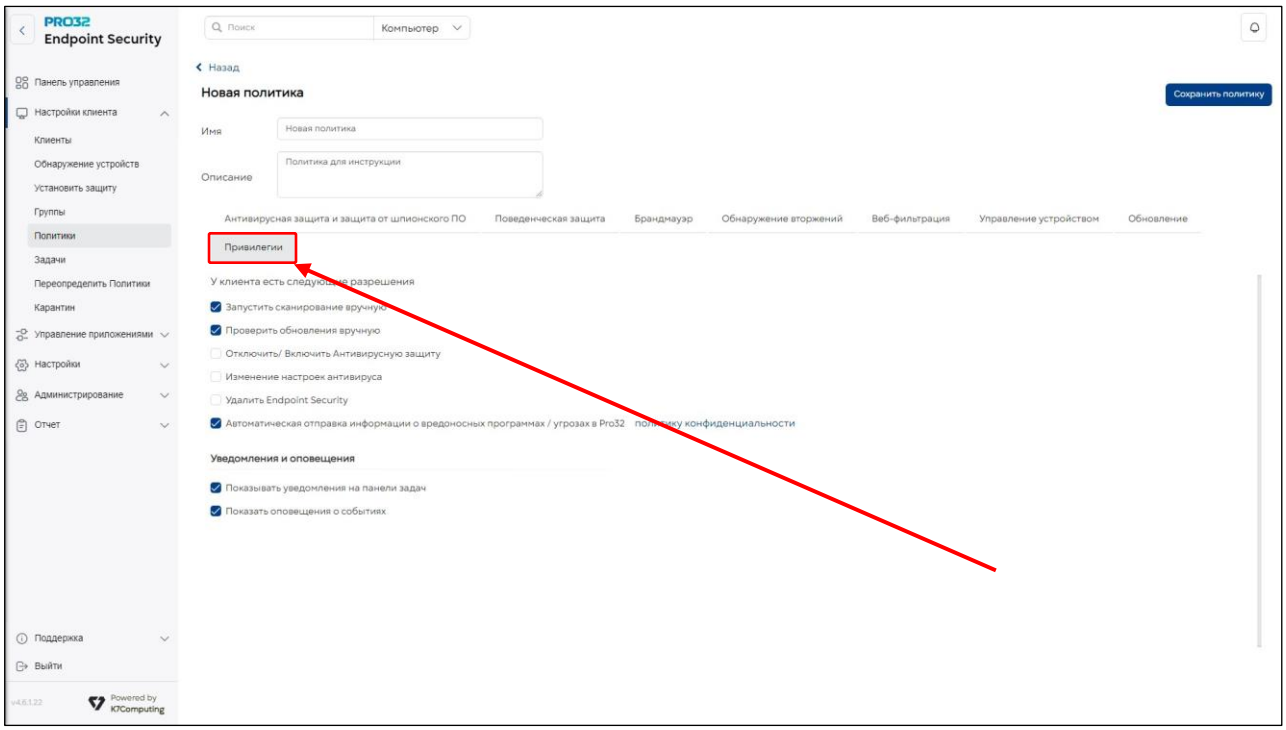
таким образом, экономят пропускную способность Интернета.

- Разрешить клиентским ПК самостоятельно скачивать сигнатуры при наличии подключения к Интернету
- Использовать прокси сервер для скачивания обновлённых сигнатур.



15.8. Вкладка «Привилегии»

Здесь вы можете задать набор прав для пользователей ПК, на котором установлен клиентский дистрибутив (Сотрудников).



Нажмите «**Сохранить**» и затем «**ОК**» в появившемся диалоговом окне с сообщением о добавлении новой политики.

16. Редактирование политики

Вы можете изменять существующие политики в разделе **«Политики».**

1. В консоли администрирования перейдите на вкладку «**Настройки клиента»** и на панели слева откройте страницу «**Политики»**.
2. На главной панели будет отображен список существующих политик. Выберите политику, которую хотите изменить, и нажмите кнопку «**Редактировать»**. (Обратите внимание, что нельзя редактировать политику по умолчанию.)
3. Внесите необходимые изменения во вкладки, такие как Антивирусная защита и защита от шпионского ПО, Поведенческая защита и т. д.,
4. По окончании нажмите **«Сохранить»** и затем **«ОК»** в появившемся диалоговом окне, сообщающем об обновлении политики.

17. Удаление политики

Вы можете удалять существующие политики в разделе **«Политики».**

1. В консоли администрирования перейдите на вкладку **«Настройки клиента**» и на панели слева откройте страницу **«Политики».**
2. На главной панели будет отображен список существующих политик. Выберите политику, которую хотите удалить, и нажмите кнопку **«Удалить».**
3. Нажмите **«ОК»** для подтверждения удаления.
4. Если выбранная политика назначена одному или нескольким компьютерам, появится предупреждение, предлагающее назначить стандартную политику после удаления текущей. Нажмите кнопку **«ОК»,** чтобы удалить политику и применить стандартную политику к затронутым компьютерам. Нажмите **«Отмена»,** чтобы отменить удаление.

Обратите внимание, что нельзя удалить «Политику по умолчанию».

18. Копирование существующей политики для создания новой

Вместо добавления новой политики вы можете скопировать существующую политику, чтобы использовать ее в качестве основы для новой политики.

1. В консоли администрирования перейдите на вкладку «**Настройки клиента»** и на панели слева откройте страницу «**Политика»**.
2. На главной панели будет отображен список существующих политик. Выберите политику, которую хотите скопировать, и нажмите кнопку «**Дублировать».**
3. Укажите необходимое имя и описание новой политики и внесите необходимые добавления/изменения к политике, выбирая различные вкладки, такие как Антивирусная защита и защита от шпионского ПО, Поведенческая защита и т. д.
4. Нажмите «**Сохранить»**, чтобы сохранить новую политику.

19. Группы

Группа – это организованный набор клиентских компьютеров в сети с одинаковыми требованиями к безопасности. Вы можете управлять группой компьютеров как единым блоком в зависимости от их роли и использования. Например, можно создать отдельные группы для различных отделов – маркетинг, бухгалтерия, проектирование, сбыт и т. д. В результате компьютеры каждого отдела получат одинаковые настройки безопасности. При наличии географически распределенной сети вы можете создать группы не только по отделам и необходимым уровням безопасности, но и по местоположению компьютеров. Каждый клиентский компьютер может входить только в одну группу. По умолчанию все клиентские компьютеры принадлежат стандартной группе. Эту группу нельзя изменить или удалить.

19.1 Создание группы

Вы можете создать любое количество групп, соответствующих сходным по функциям компьютерам вашей организации. Чтобы добавить новую группу:

1. В консоли администрирования перейдите в раздел «**Настройки клиента»** в раскрывшемся меню слева откройте страницу «**Группы»**.
2. Нажмите «**Создать группу»** и введите имя и описание новой группы.

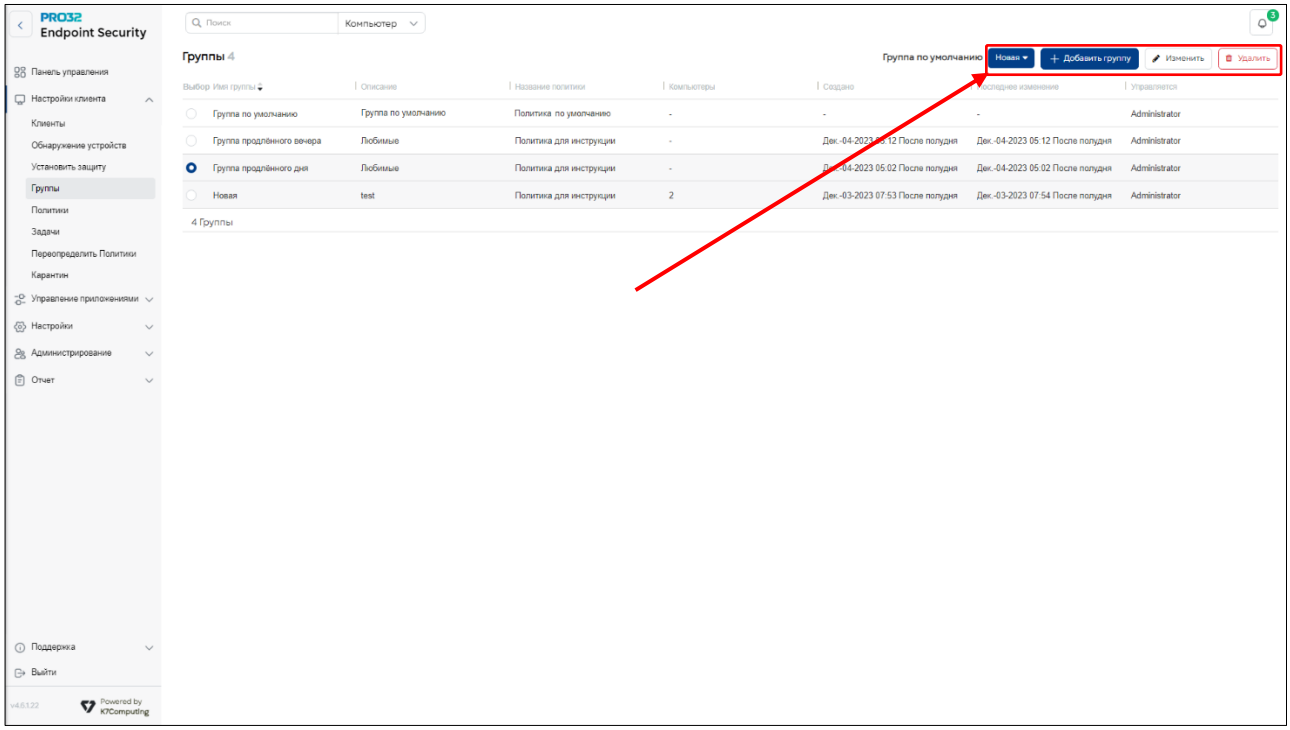
3. Список существующих и\или настроенных ранее политик отображается в раскрывающемся списке **«Политика».** Выберите политику, которую вы хотите применить к новой группе, и нажмите «Добавить».
4. Нажмите ОК в диалоговом окне для подтверждения добавления новой группы.

Имя группы может иметь длину до 255 символов и содержать любые символы, кроме некоторых специальных символов, таких как [: " / \ * ? < > |]
Длина описания группы не ограничена.

19.2 Редактирование группы

Вы можете изменить имя группы и назначить группе другую политику.

1. В консоли администрирования перейдите в раздел «**Настройки клиента»** в раскрывшемся меню слева откройте страницу «**Группы»**.
2. Выберите группу, которую вы хотите отредактировать, и нажмите «**Изменить».**
3. Вы можете указать новое имя или описание группы и/или изменить политику, которая ей назначена.
4. Когда закончите нажмите кнопку **«Обновить»,** и **«ОК»** в диалоговом окне, подтверждающем изменение.



19.3 Удаление группы

Можно удалить любую группу, кроме «**Группы по умолчанию**». Любая пользовательская группа может быть помечена группой по умолчанию. Для ее удаления нужно назначить в качестве стандартной другую группу.

Если какие-либо из клиентских компьютеров принадлежат к удаляемой группе, они будут помещены в стандартную группу.

1. В консоли администрирования перейдите в раздел «**Настройки клиента**» в раскрывшемся меню слева откройте страницу «**Группы**».
2. Выберите группу, которую хотите удалить, и нажмите «**Удалить**».
3. Нажмите «**ОК**» для подтверждения удаления.
4. Если в удаляемую группу входит один или несколько компьютеров, появится предупреждение с вопросом, хотите ли вы добавить эти компьютеры в группу по умолчанию. Нажмите «**Да**», чтобы продолжить. Нажмите «**Нет**», чтобы отменить удаление.

19.4 Изменение группы по умолчанию

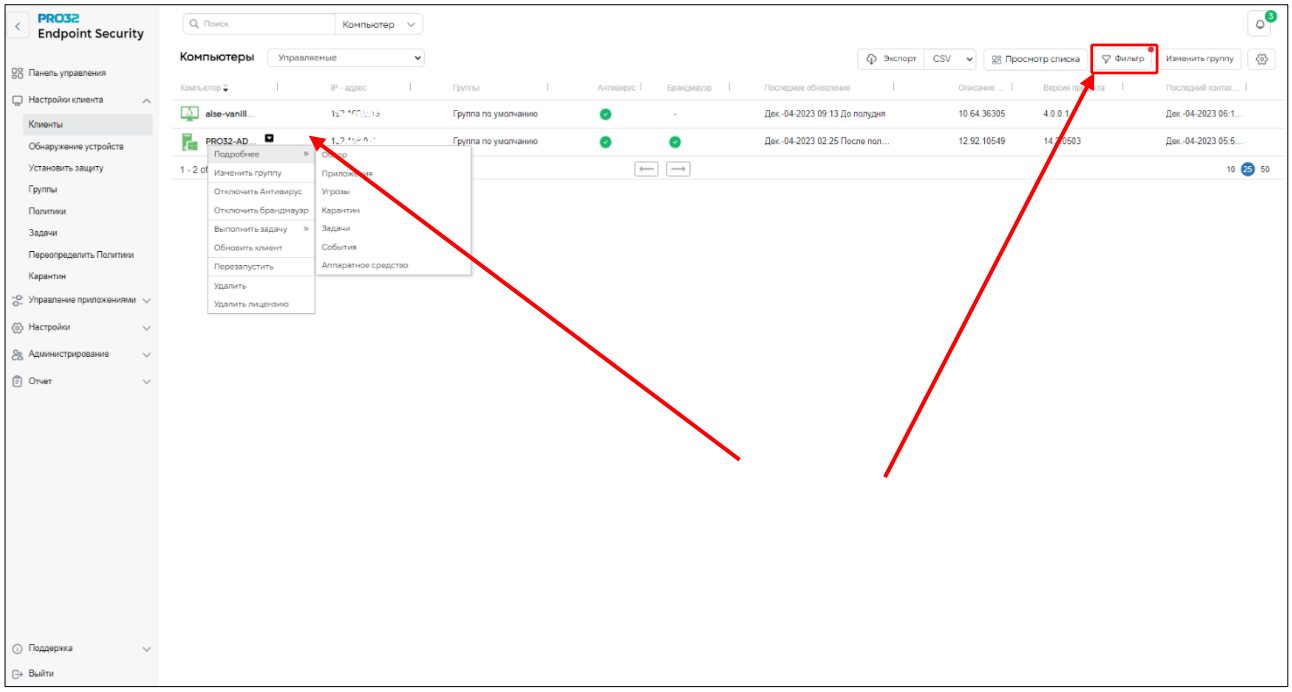
Любую пользовательскую группу можно пометить как стандартную. При добавлении нового клиентского компьютера он по умолчанию помещается в стандартную группу.

1. В консоли администрирования перейдите на вкладку **Настройки клиента** и на панели слева откройте страницу **Группы**.
2. По нажатию кнопки раскрывающегося списка рядом с полем **Группа по умолчанию** будет отображен список всех существующих групп. Выберите группу для установки в качестве стандартной группы.
3. После этого при добавлении нового клиентского компьютера он будет помещен в эту группу.

20. Управление клиентами

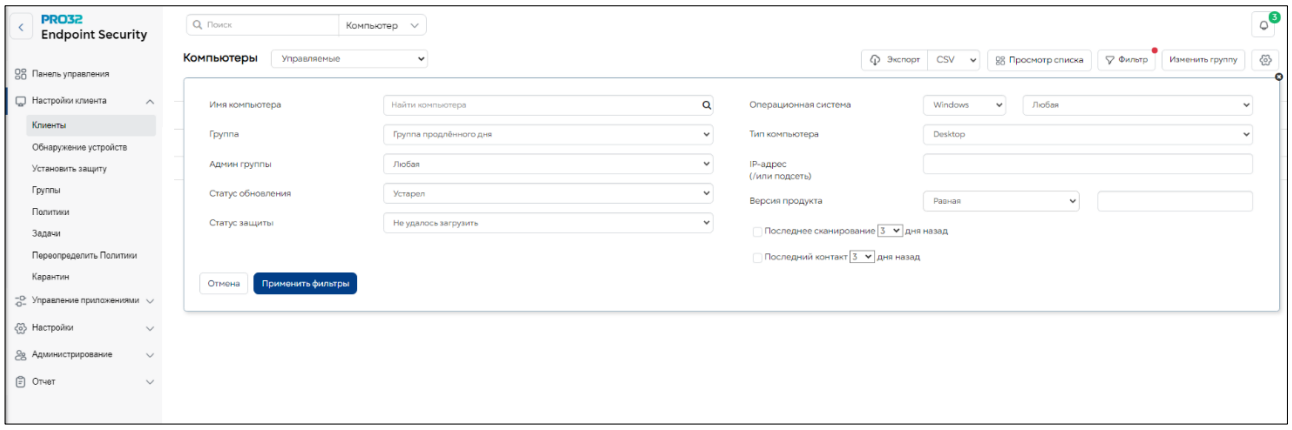
В консоли администрирования на вкладке «Клиенты» отображается список клиентских компьютеров, на которых установлена программа PRO32 Endpoint Client, и их статус безопасности. На этой вкладке содержится следующая информация для администратора:

- ✓ Имя компьютера
- ✓ Группа
- ✓ Статус антивируса и брандмауэра
- ✓ Версия Endpoint Security
- ✓ Версия вирусных сигнатур
- ✓ Дата и время последнего обновления
- ✓ Дата и время последнего контакта



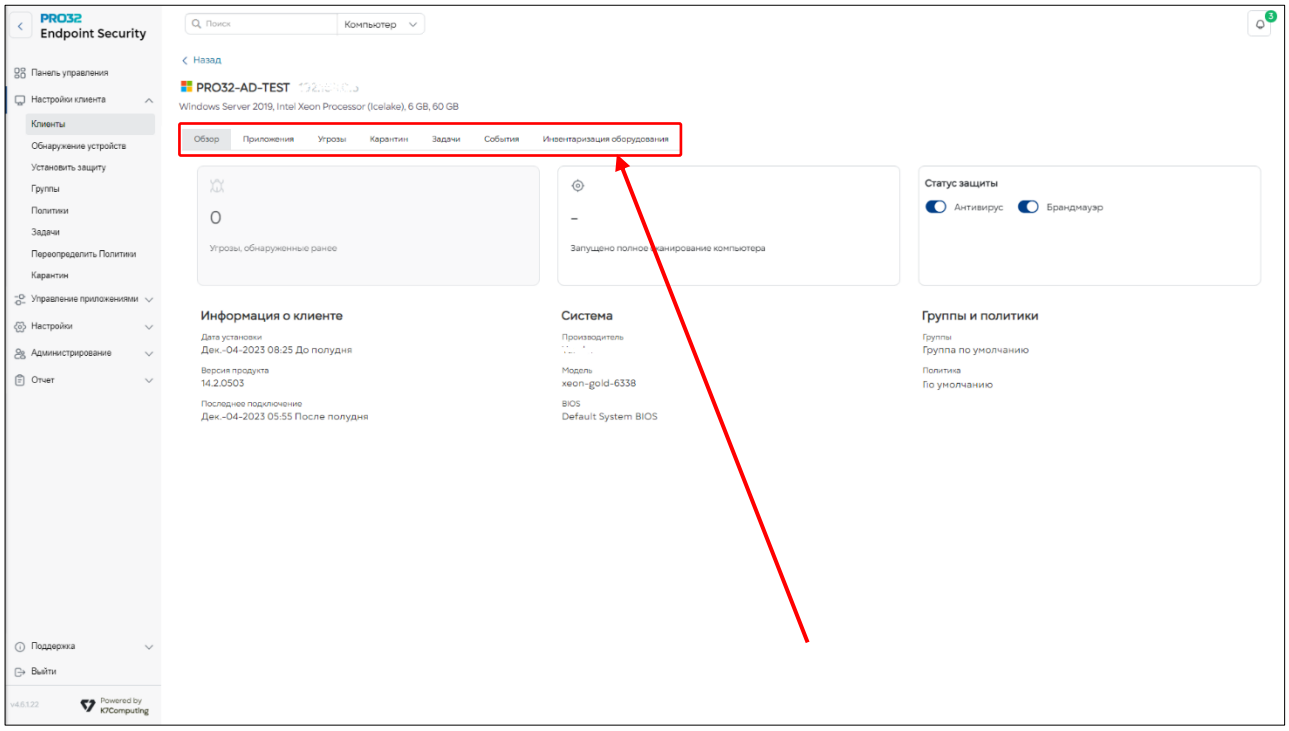
Чтобы отобразить компьютеры, удовлетворяющие определенным критериям, используйте команду **Фильтр**. Доступны следующие критерии фильтрации:

- ✓ Имя компьютера
- ✓ Группа
- ✓ Администратор группы
- ✓ Статус обновления
- ✓ Статус защиты
- ✓ Операционная система
- ✓ Тип компьютера
- ✓ IP-адрес



По щелчку имени определенного компьютера появится полная информация о нем, в частности:

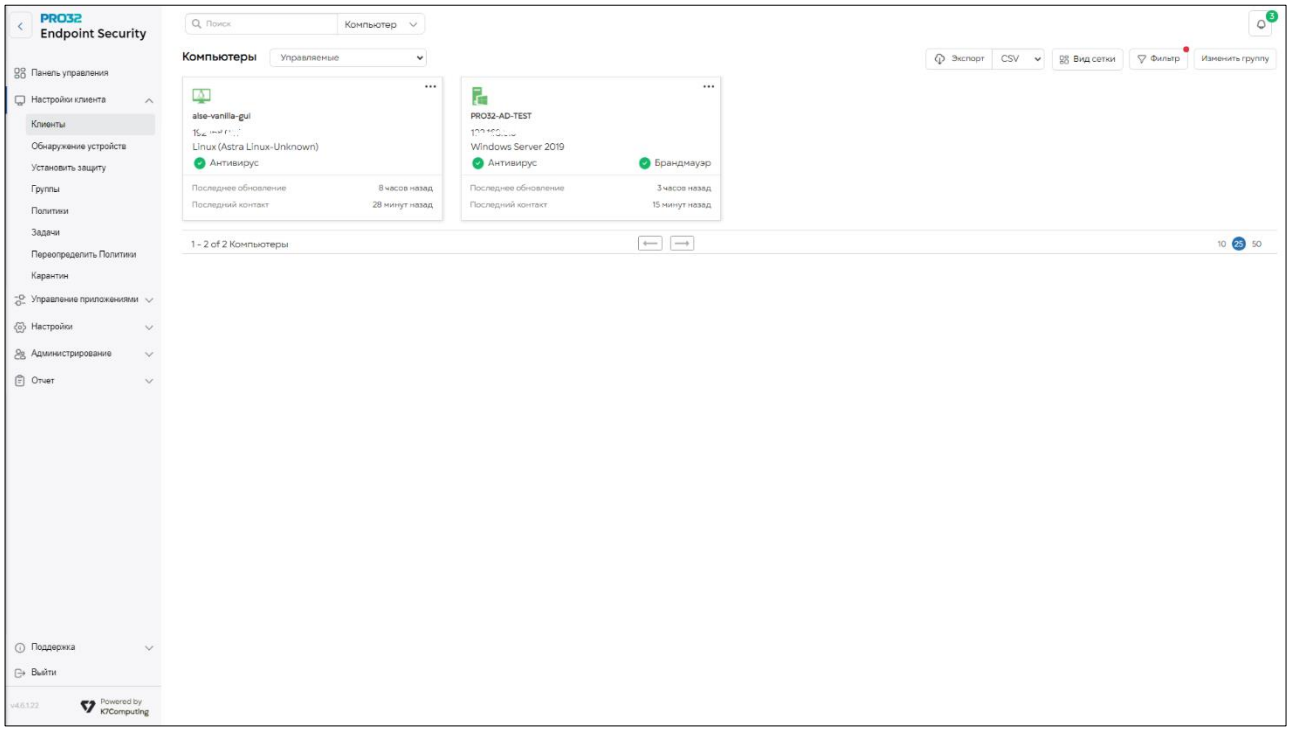
- ✓ Имя компьютера
- ✓ IP-адрес
- ✓ Операционная система
- ✓ Сведения о клиенте
  - ➢ Дата и время установки
  - ➢ Версия продукта
  - ➢ Дата и время последнего контакта
  - ➢ Данные полного сканирования компьютера
  - ➢ Угрозы, обнаруженные на данный момент
- ✓ Статус защиты
  - ➢ Группа
  - ➢ Политика
- ✓ Системная информация
  - ➢ Производитель
  - ➢ Модель
  - ➢ BIOS
  - ➢ Политика
    - ▪ Группа
    - ▪ Политика
    - ▪ Приложения, которые запускались
    - ▪ Информация об обнаруженных угрозах
    - ▪ Информация о файлах, помещенных в карантин
    - ▪ Информация о задачах
    - ▪ События
    - ▪ Аппаратные средства



При выборе команды «Табличное представление» отображаются все клиентские компьютеры со следующей минимальной информацией:

- ✓ Имя компьютера
- ✓ Операционная система
- ✓ Включен ли антивирус

- ✓ Включен ли брандмауэр
- ✓ Последнее обновление
- ✓ Последний контакт



Команда «Экспорт» позволяет экспортировать информацию обо всех клиентских компьютерах, отображаемую в таблице, в формате CSV, HTML, DOC, XLS.

Экспортируются только те столбцы, которые выбраны видимыми в таблице. Можно выбрать следующие столбцы:

- ✓ Домен
- ✓ Антивирус
- ✓ Последнее обновление
- ✓ Версия продукта
- ✓ Последний контакт
- ✓ Операционная система
- ✓ Последнее сканирование

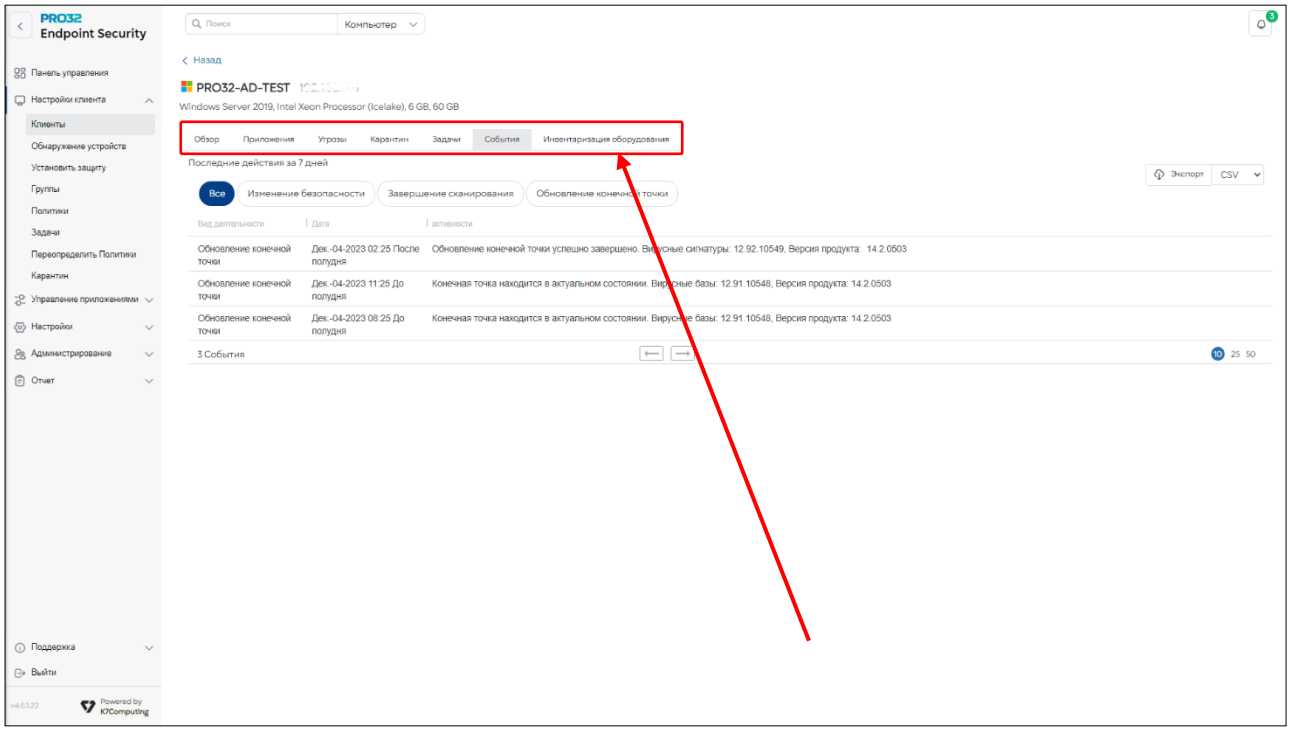
Управлять группами, политиками и т.д. легко на вкладке «Настройки клиента», на левой панели которой вы можете выполнить следующие действия:

- ➢ Установка Endpoint Security на клиентские компьютеры
- ➢ Управление группами: создать/редактировать/удалить группу
- ➢ Управление политиками: создать/редактировать/скопировать/удалить политику
- ➢ Управление задачами для отдельных компьютеров или групп
- ➢ Настройка переопределяющей политики
- ➢ Карантин
- ➢ Создать задачу на заданные клиенты

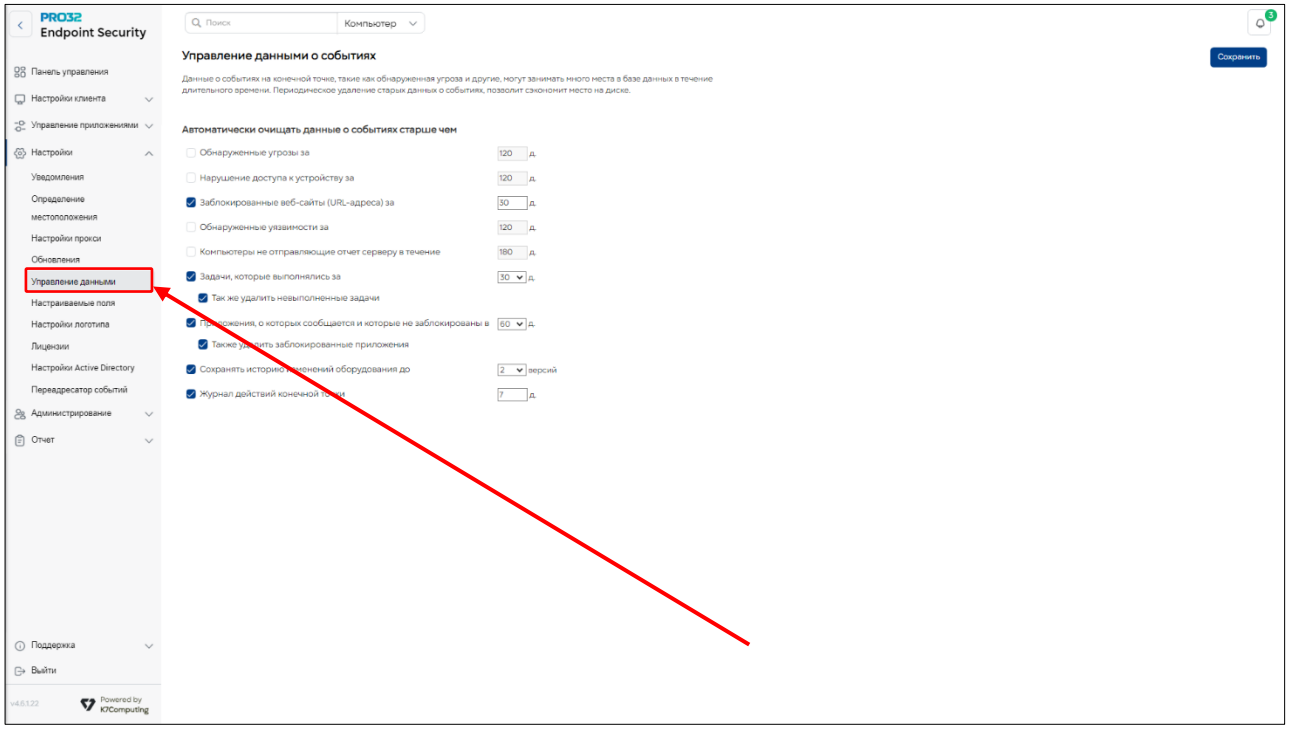
21. Просмотр событий изменения статуса антивируса и брандмауэра

Когда выбирается конкретный клиент из списка клиентов и фильтруются события “Изменения безопасности” на вкладке “События”, отображаются изменения статуса функций антивируса и брандмауэра, выполненные конечными пользователями. Теперь также отображаются события, инициированные администратором.

Добавлена функция экспорта событий в различных форматах.



В базе данных информация о событиях хранилась в течение 7 дней. Теперь можно указать срок хранения данных о событиях вплоть до 999 дней в разделе ***Настройки → Управление данными→*** **«Журнал действий конечной точки»** – с помощью этого параметра администратор может указать срок хранения от 7 до 999 дней. По умолчанию этот параметр включен, и данные о событиях хранятся только в течение 7 дней. Если этот параметр отключен, данные о событиях не будут удаляться.



22. Добавление дополнительных полей на страницу «Управление клиентами»

Веб-консоль PRO32 Endpoint Security отображает для администраторов стандартный набор полей, позволяющих идентифицировать компьютеры с установленным клиентами PRO32 Endpoint Security Client и управлять ими. В стандартном наборе включены такие поля, как имя компьютера, IP-адрес, статус антивируса и т. д. Когда количество конечных точек значительно увеличивается, например до тысяч, этого набора стандартных полей может быть уже недостаточно для целей администрирования.

В настоящее время страница «**Настройки клиента»** PRO32 Endpoint Security содержит фиксированный перечень следующих столбцов, и этот перечень не может быть изменен администратором:

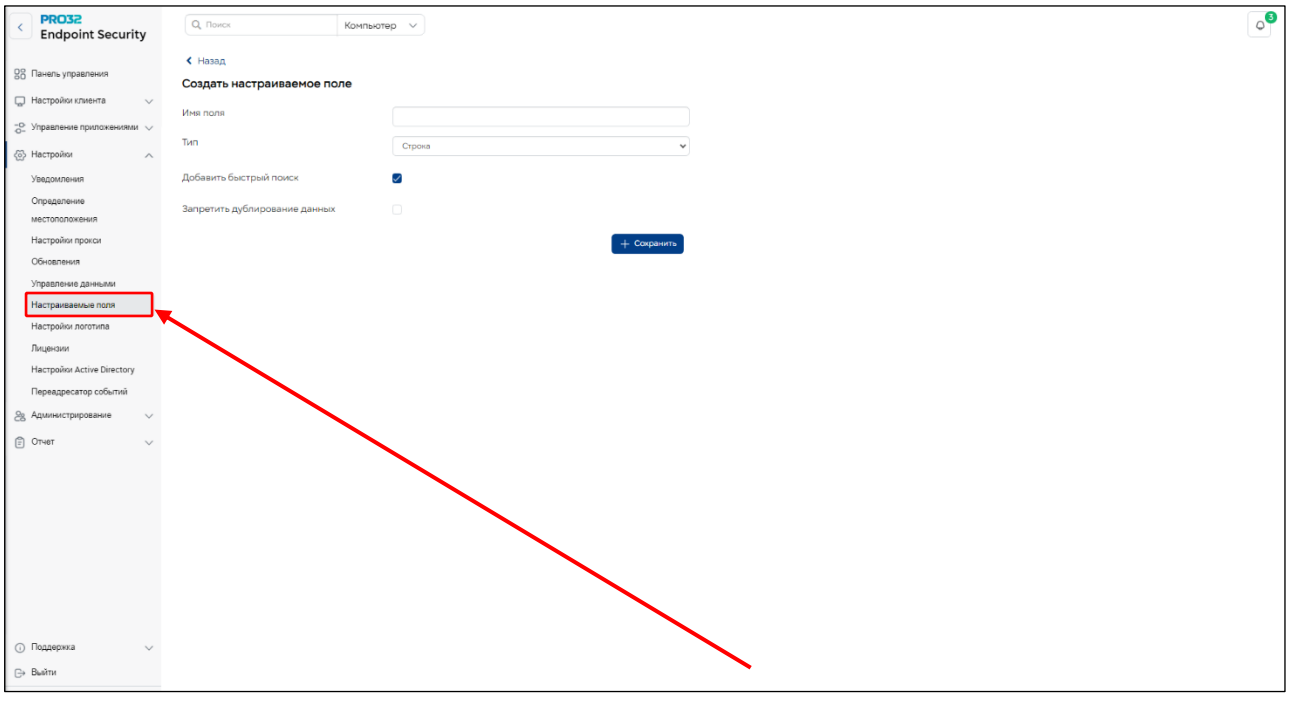
- ✓ Компьютер
- ✓ Группа
- ✓ Антивирусная программа / брандмауэр
- ✓ Последнее обновление
- ✓ Версия продукта
- ✓ Версия вирусных сигнатур
- ✓ Операционная система
- ✓ Последнее сканирование

Потребность в дополнительных полях

Если в организации тысячи конечных точек, приведенного выше стандартного списка полей недостаточно, чтобы администраторы могли однозначно идентифицировать компьютер и управлять им. Администраторам может потребоваться добавить поля, например уникальный идентификатор ПК, псевдоним для каждого ПК или некоторую дополнительную информацию о группе или домене и т. д., чтобы облегчить идентификацию конкретного ПК из огромного списка.

Теперь реализована функция добавления настраиваемых полей, благодаря которой администраторы могут добавлять необходимые им поля строкового или числового типа.

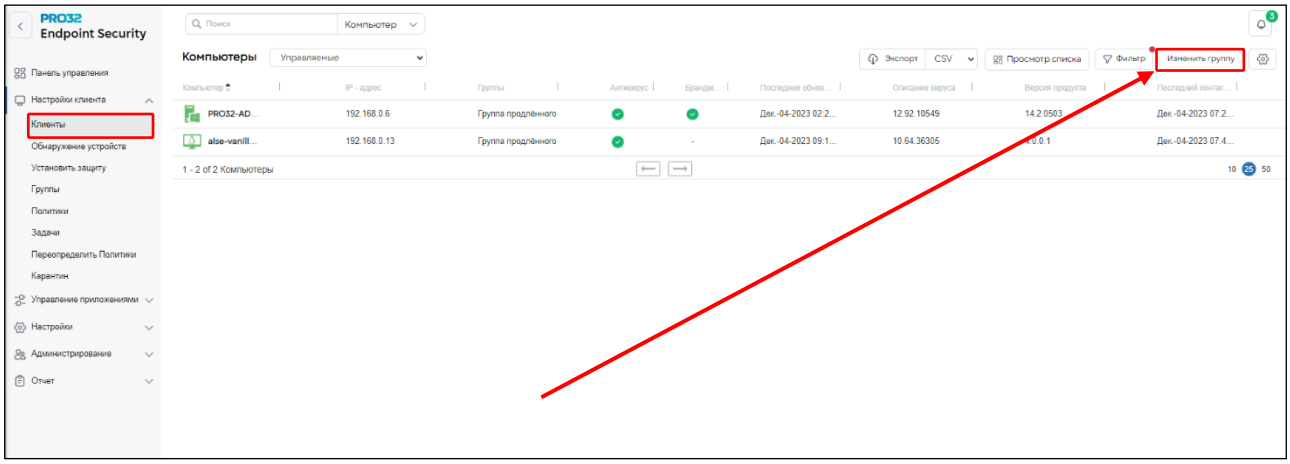
Перейдите в раздел **«Настройки».** В ниспадающем меню выберите **«Настраиваемые поля».**

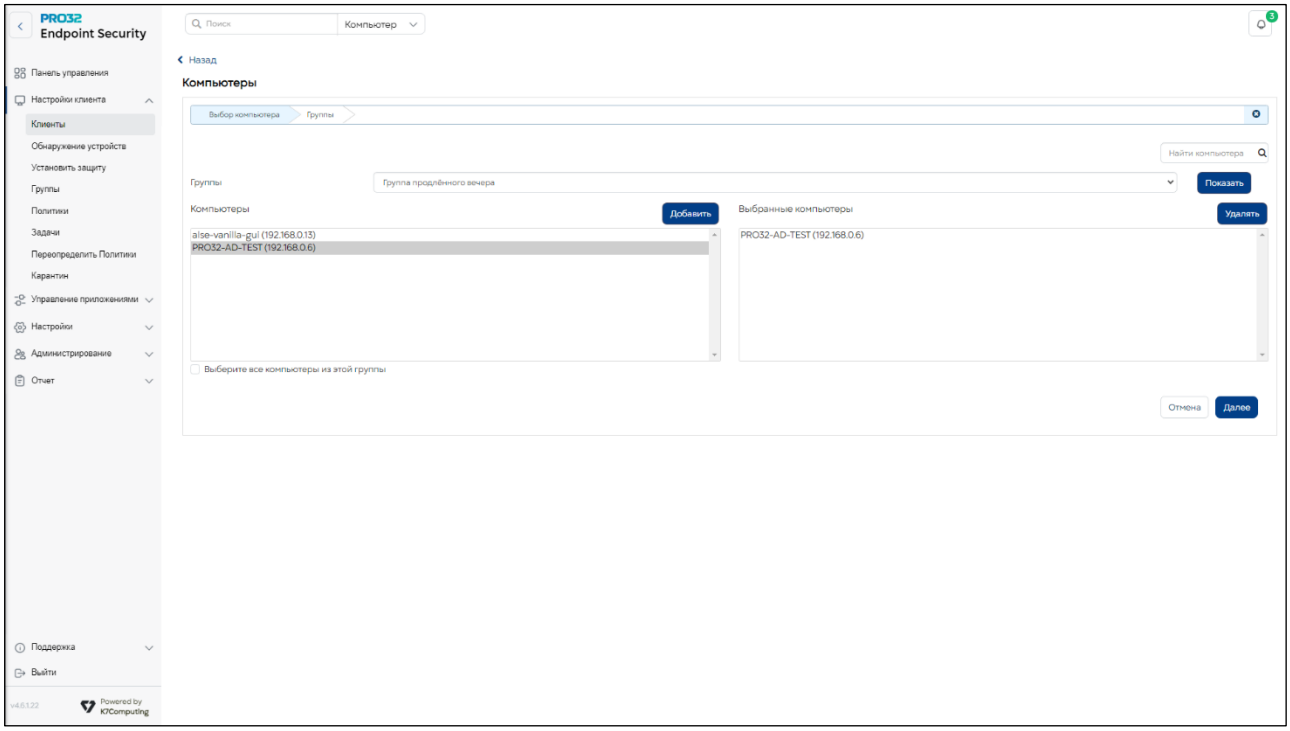


23. Смена группы

Вы можете сменить группу для одного или нескольких компьютеров. Таким образом можно применять разные политики для разных отделов в компании. Чтобы сменить группу для компьютеров:

1. В разделе **«Настройки клиента» → «Клиенты»** нажмите кнопку **«Сменить группу» –** появится диалоговое окно **«Смена группы».**
2. Выберите группу из выпадающего списка и нажмите кнопку **«Показать»,** чтобы просмотреть компьютеры, связанные с выбранной группой.
3. Выберете компьютеры из списка, которые вы хотите переместить в другую группу, и нажмите кнопку **«Добавить».**
4. Нажмите кнопку **«Готово».**





24. Управление задачами

В дополнение к функции защиты в режиме реального времени, доступной на клиентских компьютерах с PRO32 Endpoint Client, администратор можете указать режим сканирования клиентских компьютеров: по запросу или по расписанию. Для этого необходимо создать новую

задачу и указать компьютеры или группы, которым она должна быть назначена. Администратор может просматривать статус задач и удалять задачи.

При создании задачи ей можно назначить одно из следующих действий:

- Быстрое сканирование
- Полное сканирование
- Поиск руткитов
- Сканирование на наличие уязвимостей
- Отслеживающие куки-файлы
- Выборочное сканирование
- Обновить клиент
- Аппаратные средства

Действия удаления/помещения в карантин можно отдельно настроить для исполняемых файлов и документов. По умолчанию для обоих этих форматов выбрано действие «Удалять автоматически».

24.1 Создание новой задачи

Перейдите в раздел **«Настройки Клиента».** В ниспадающем меню выберите **«Задачи».** В правом верхнем углу нажмите кнопку «Новая Задача»

При создании задачи ей можно назначить одно из следующих действий:

«Быстрое сканирование» – сканирует важные диски и папки (диск C, папку Windows и папку Program Files) на наличие вирусов и других потенциальных угроз.

«Полное сканирование» – сканирует всю систему, включая все файлы, папки и диски.

«Поиск руткитов» – сканирует систему на наличие руткитов.

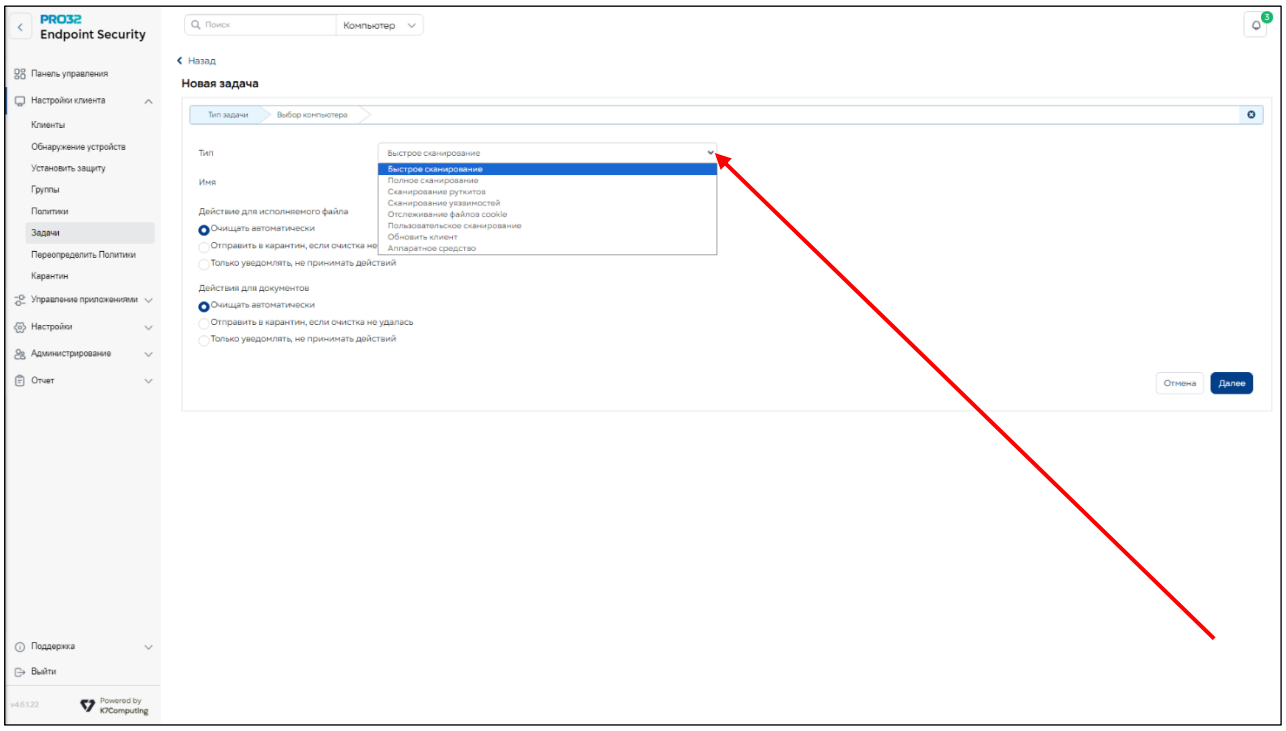
«Сканирование на наличие уязвимостей» – сканирует и информирует пользователей об уязвимостях в системе.

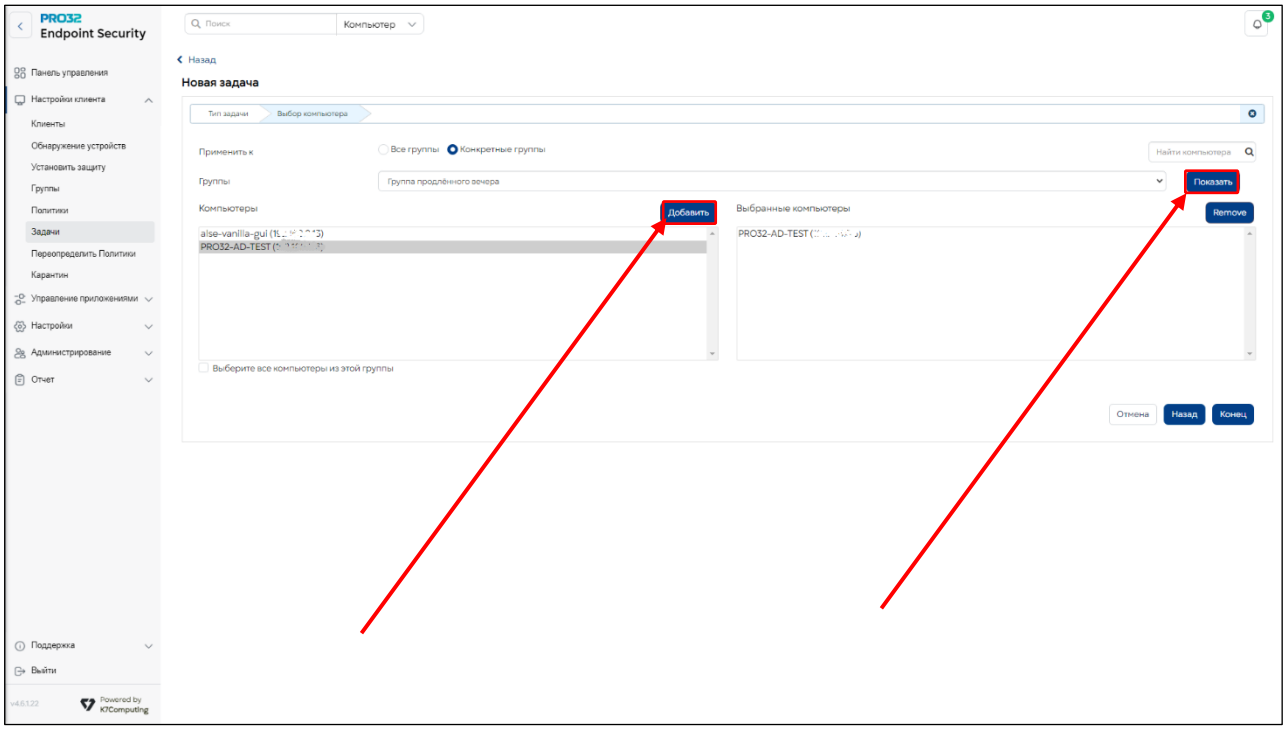
«Отслеживающие куки-файлы» – это данные, сохраняемые в системе браузером, которые позволяют веб-сайту однозначно идентифицировать пользователя. В этом режиме сканируются отслеживающие куки-файлы текущего пользователя, вошедшего в систему.

«Выборочное сканирование» – позволяет указать область сканирования. Вы можете выбрать места и типы файлов для сканирования и принять решение о том, какие действия следует предпринять в случае обнаружения вредоносного ПО.

«Обновить клиент» – обновить антивирусное ПО на выбранных компьютерах или в выбранных группах.

«Аппаратные средства» – проанализировать любые изменения в составе аппаратных средств на выбранных компьютерах или в выбранных группах.

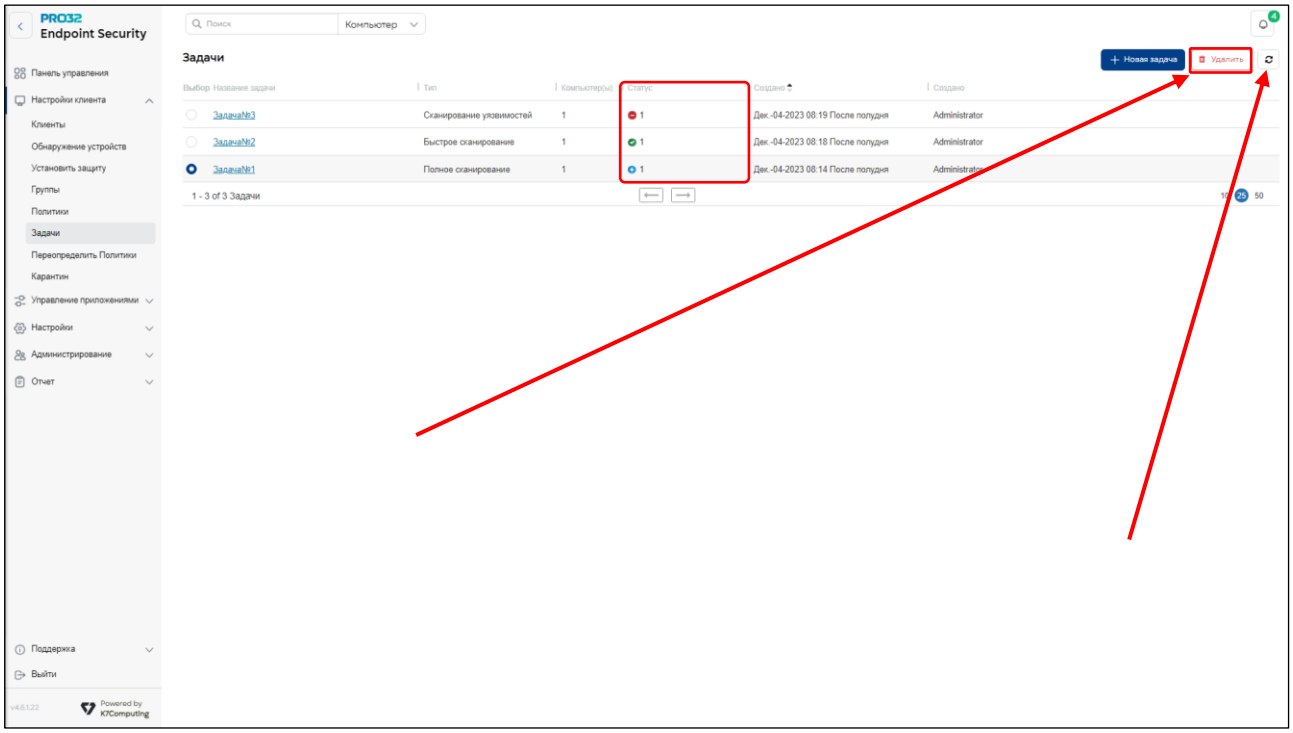




24.2 Статусы задач

В отображаемом списке задач вы можете быстро определить их статус в соответствии со следующими цветовыми кодами:

- ✓ Красный цвет – Ожидание завершения – Задача все еще выполняется
- ✓ Синий цвет – Передано на выполнение – Выполнение задачи было начато на клиентском компьютере
- ✓ Зеленый цвет – Завершено – Задача успешно выполнена на клиентском компьютере



24.3 Удаление задачи

Список задач отображается на странице «Управление задачами». Выберите задачу, которую хотите удалить, и нажмите кнопку **Удалить**.

24.4 Обновление статусов задач

Чтобы обновить статус всех задач, нажмите кнопку **«Обновить»** .

25. Переопределяющая политика

Если требуется применить какой-либо набор параметров сразу на нескольких компьютерах, это можно сделать без изменения их политик с помощью функции **«Переопределяющая политика».** Администраторы могут использовать эту функцию для быстрого применения общего правила или ограничения на всех компьютерах.

Переопределяющая политика может содержать настройки двух типов.

1) **Переопределение:** настройки этого типа переопределяют настройки политик. Например, первоначально вы не установили в политиках никаких ограничений на использование съемных носителей. В дальнейшем возникла необходимость заблокировать доступ к съемным носителям на всех компьютерах. Вы можете легко заблокировать использование съемных носителей в переопределяющей политике. Изменять настройки управления устройствами во всех политиках не требуется.

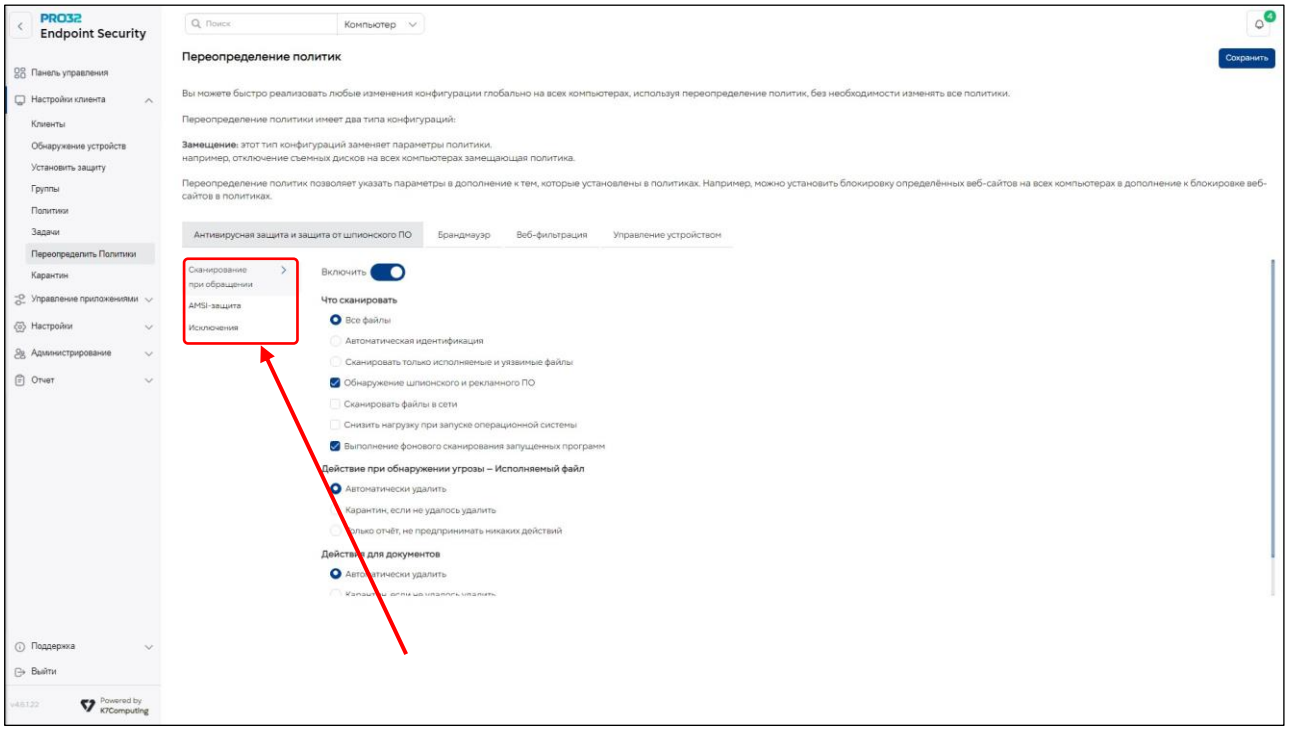
2) **Расширение:** настройки этого типа являются дополнительными к тем, которые уже содержатся в политиках. Например, во всех политиках уже настроена веб-фильтрация. Теперь вам необходимо заблокировать доступ к определенным веб-сайтам со всех компьютеров. Это можно легко сделать на странице «Переопределяющая политика». Вам не нужно добавлять эти веб-сайты в каждую политику.

Перейдите в раздел **«Настройки Клиента».** В ниспадающем меню выберите **«Предопределить Политики».** Вы можете использовать расширяющую политику для детализации области сканирования. Настройки расширяющей политики сгруппированы по следующим разделам:

Антивирусное и антишпионское ПО

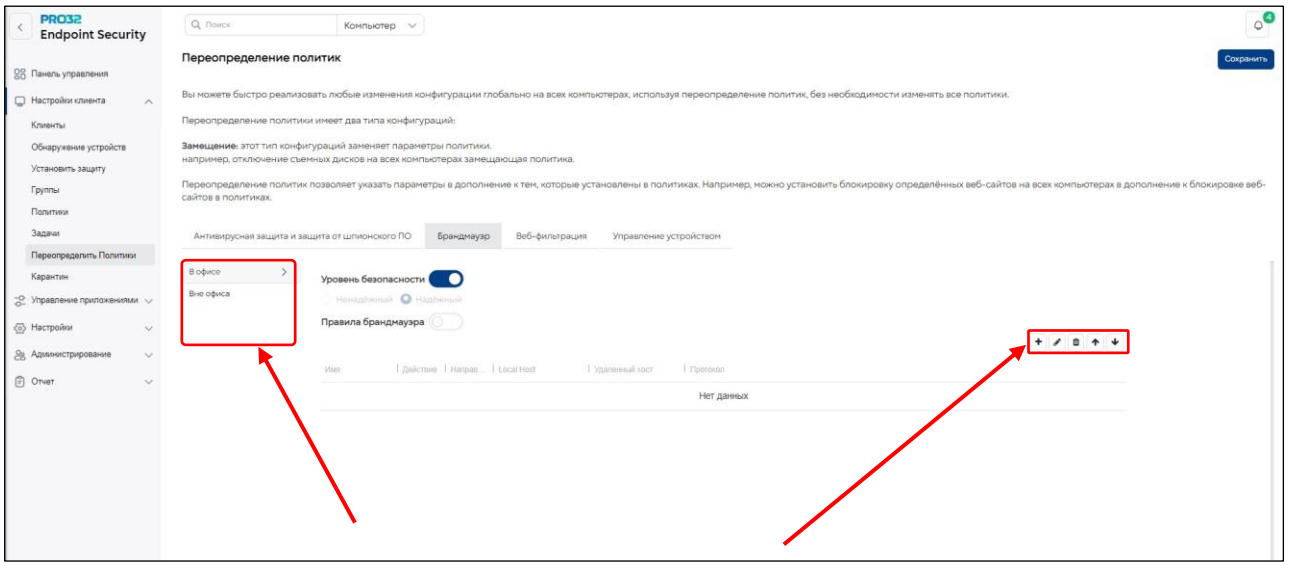
- При доступе
  - Что сканировать
  - Действия для исполняемых файлов
  - Действия для документов
- AMSI-защита
  - Действие для обнаружения
  - Исключение сценариев
  - Исключение процессов
- Исключение

Исключить определенный файл или папку из сканирования



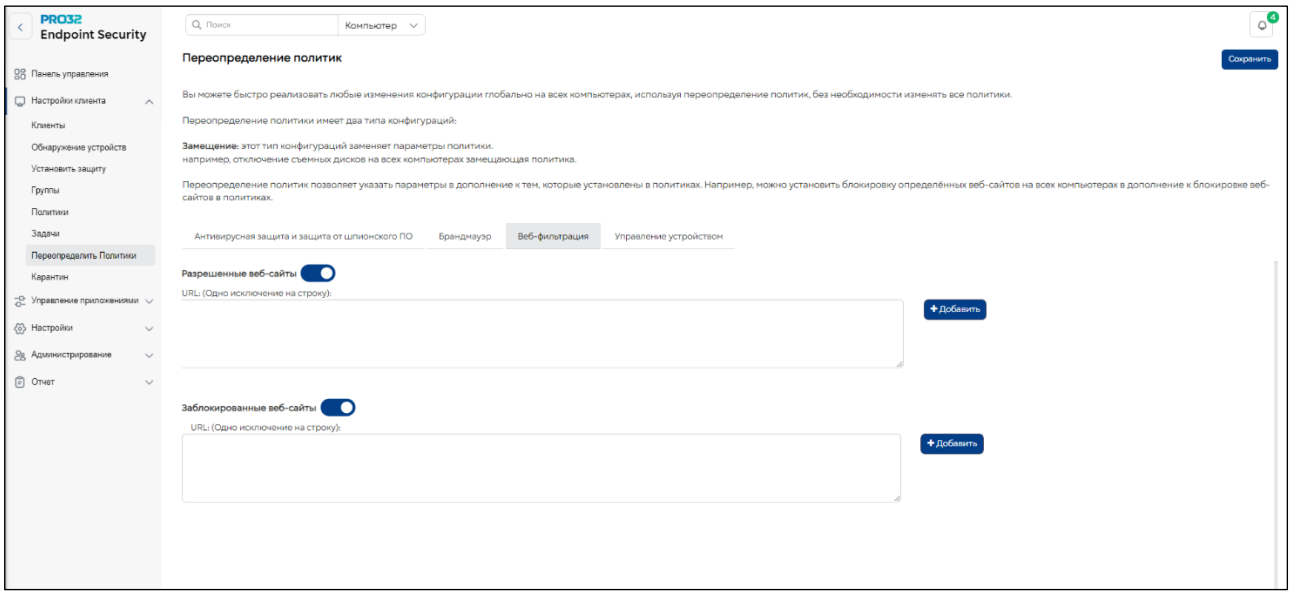
Брандмауэр

- В офисе
  - Уровень безопасности: включить / отключить
  - Дополнительные правила брандмауэра
- Вне офиса
  - Уровень безопасности: блокировать всё / доверенные/ недоверенные / запрос
  - Дополнительные правила брандмауэра



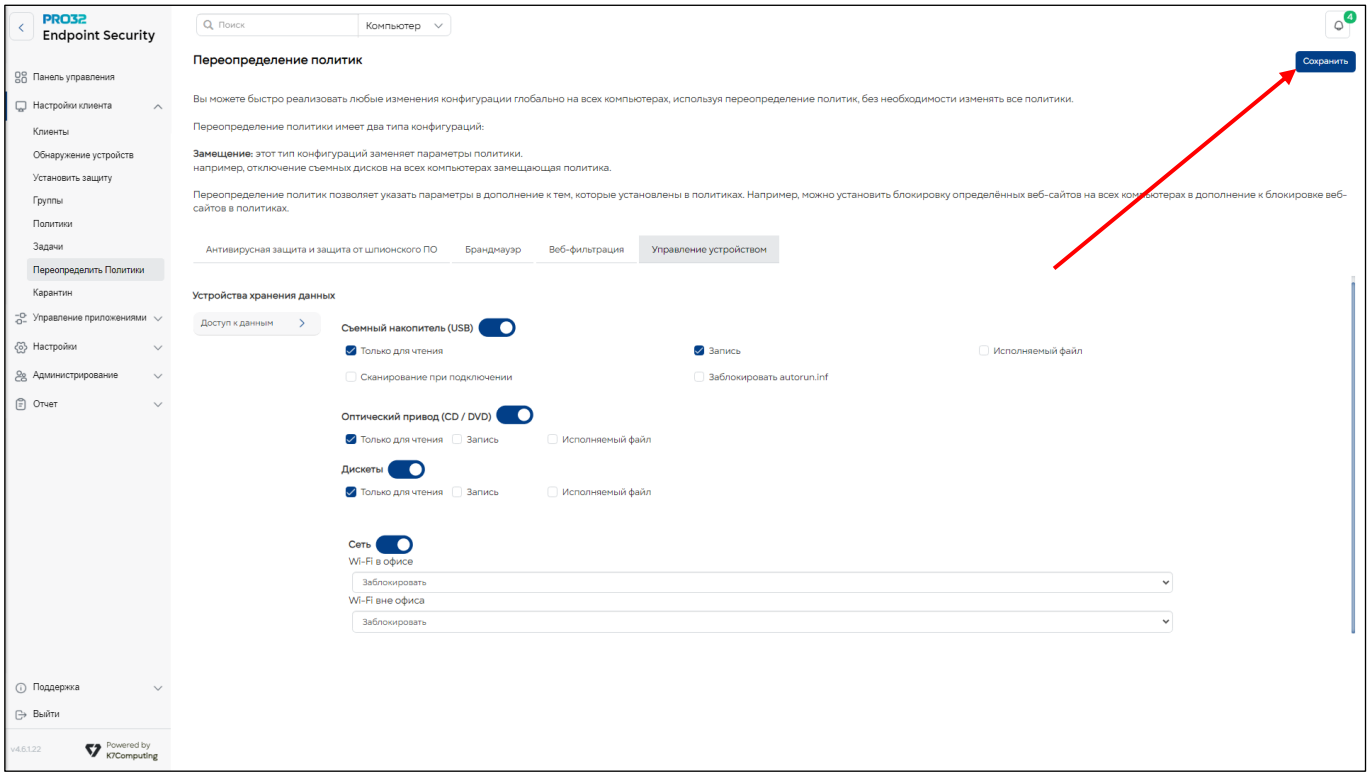
Веб-фильтрация

- Список разрешенных веб-сайтов
- Список заблокированных веб-сайтов



Управление устройствами

- Доступ к устройствам хранения
  - Съемный носитель
  - CD-привод
  - Дисковод гибких дисков
- Доступ к сети
  - В офисе: Wi-Fi – разрешить / заблокировать
  - Вне офиса: Wi-Fi – разрешить / заблокировать



Чтобы сохранить параметры переопределяющей политики и применить изменения, нажмите кнопку **«Сохранить»** в правом верхнем углу.

26. Карантин

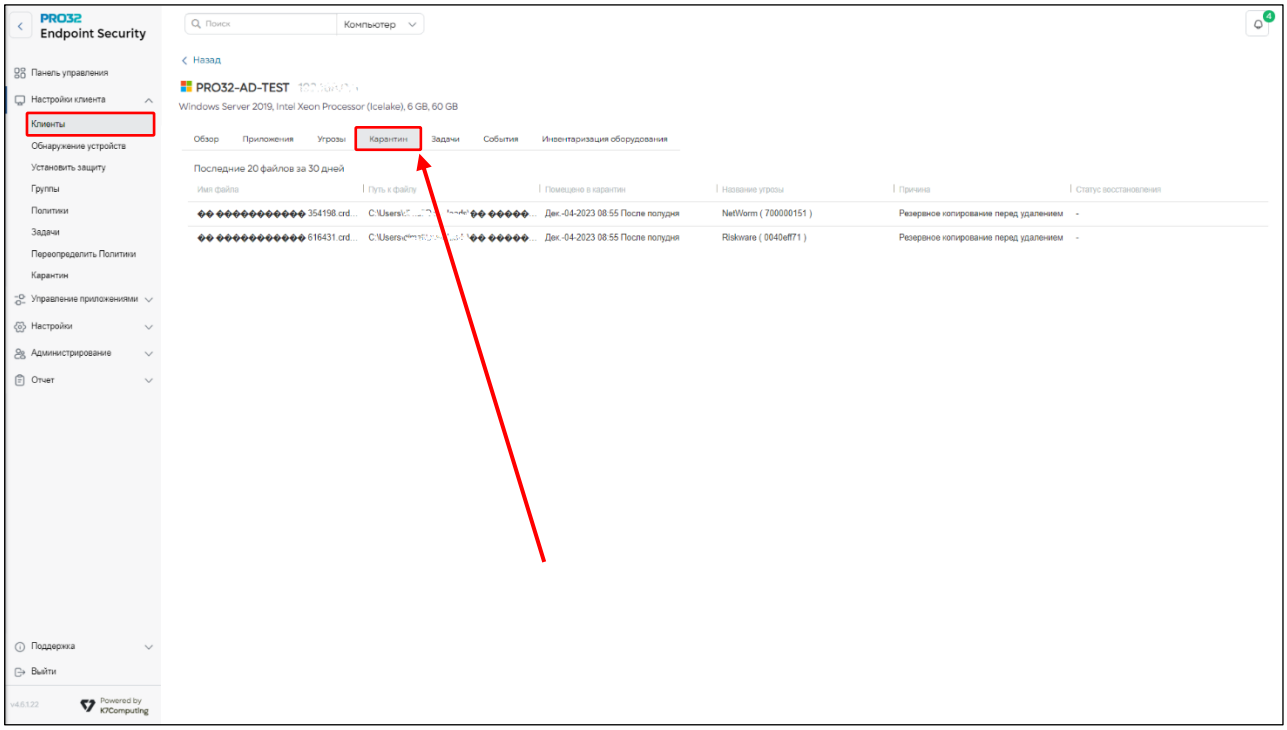
Функция карантина заключается в изоляции зараженных и подозрительных файлов до тех пор, пока не будут предприняты соответствующие действия. Карантин является специально зарезервированным местом для зараженных или подозрительных файлов и связанных с ними побочных эффектов. Будучи изолированными в карантине, вредоносное ПО и другие угрозы не могут повреждать компьютер или распространяться на нем.

Всякий раз, когда PRO32 Endpoint Security определяет файл как зараженный, программа перемещает его в карантин и запускает очистку или удаление файла. Файлы, перемещенные в карантин, могут содержать вирус или вредоносную программу. Файлы на карантине можно просмотреть по пути в разделе **«Настройки Клиента».** В ниспадающем меню выберите **«Карантин».** Файлы можно удалить, если они действительно являются вирусами/вредоносными программами, или восстановить их, если вы считаете эти файлы полезными и безопасными. Обратите внимание, что за один раз можно восстановить только один файл на нескольких компьютерах.

Всякий раз, когда вы восстанавливаете какой-либо файл на выбранном компьютере или компьютерах, он будет исключен из последующего сканирования на всех компьютерах независимо от политики сканирования, чтобы избежать повторного помещения этого файла в карантин.

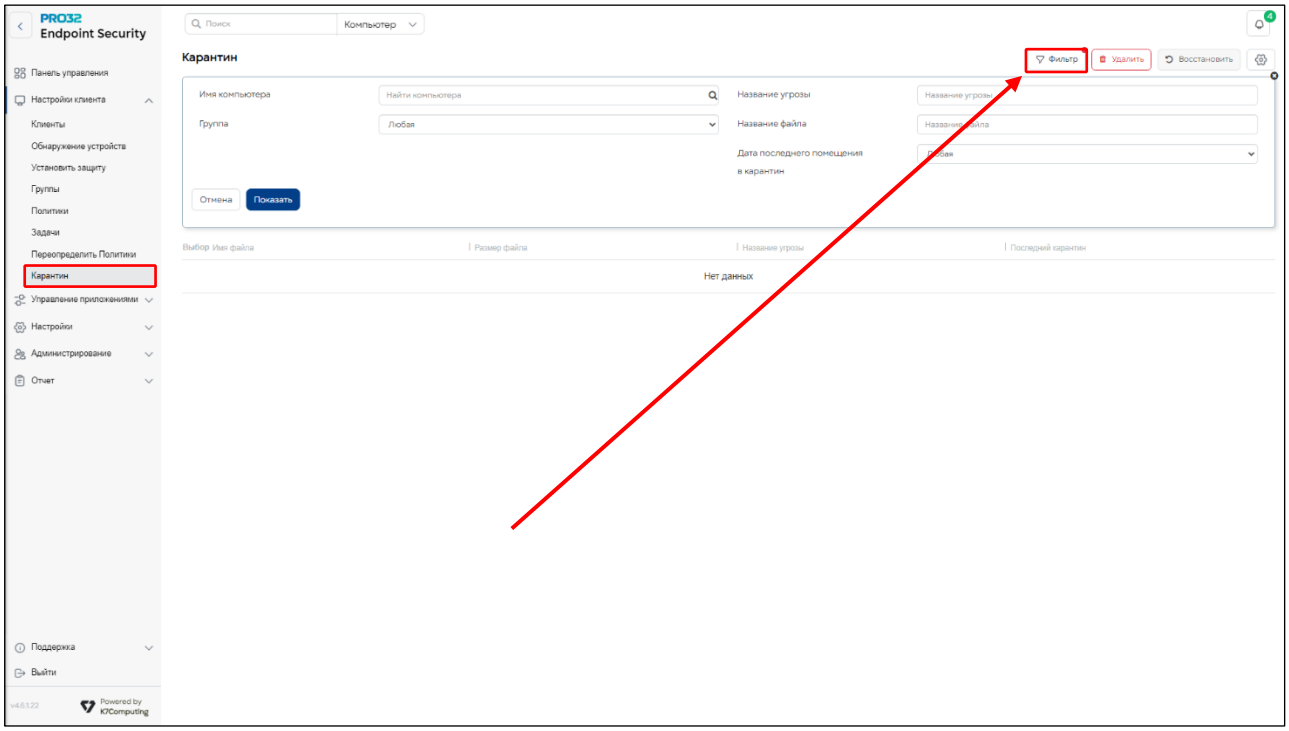
По умолчанию файлы, помещенные в карантин, хранятся как на сервере, так и на локальных компьютерах и автоматически удаляются через 30 дней.

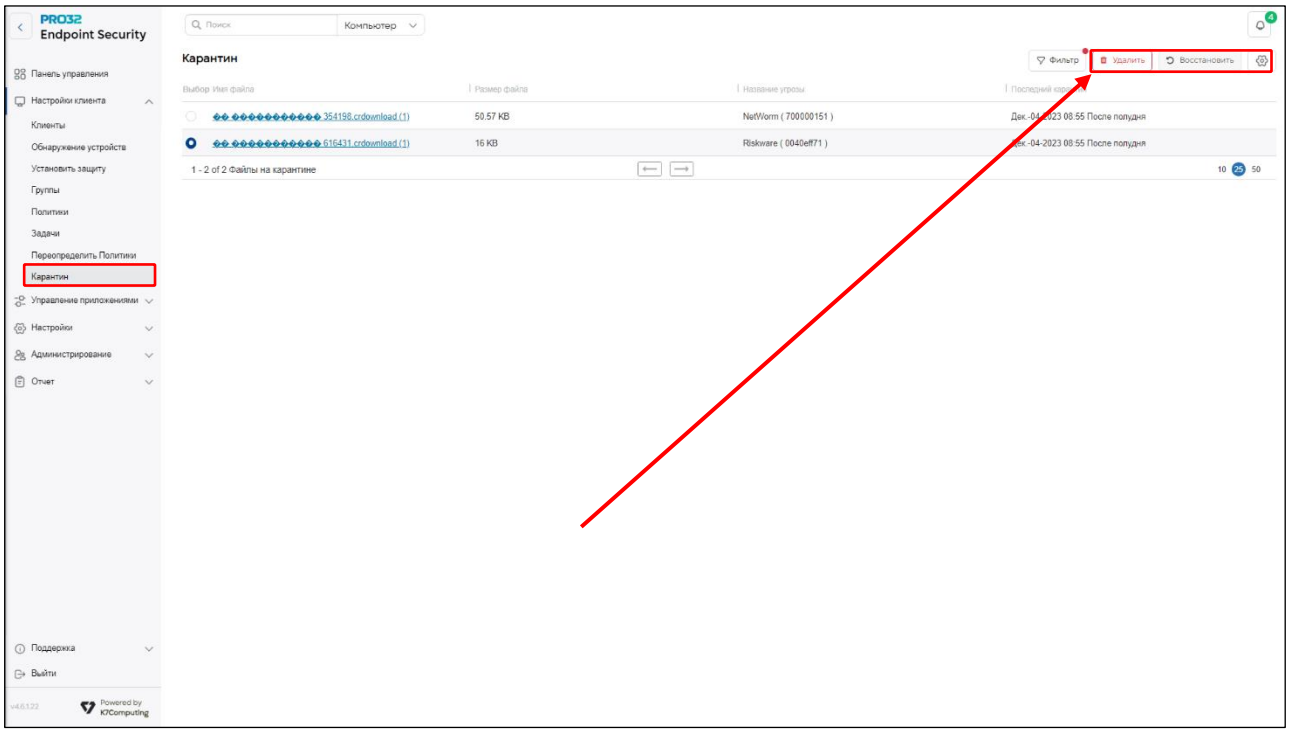
Файлы в карантине можно просмотреть, нажав раздел **«Настройки клиента» → Клиенты → Выберете нужное вам Имя компьютера →** вкладка **Карантин**.



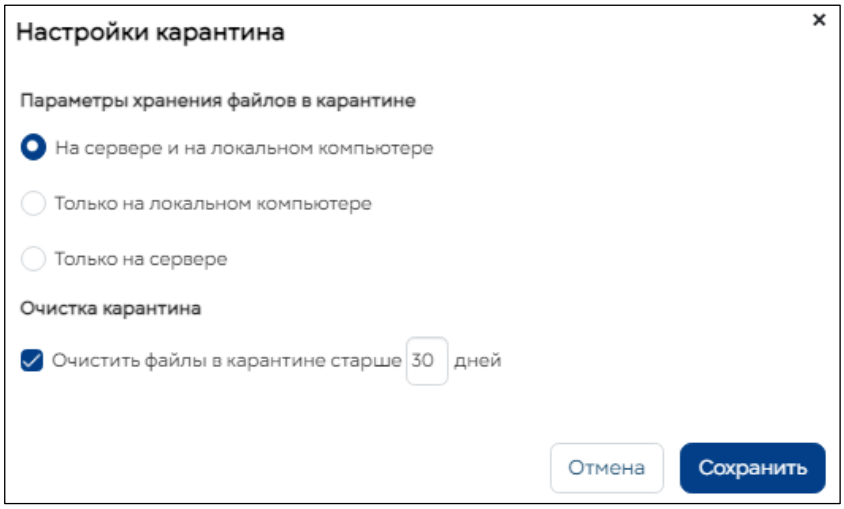
Для просмотра файлов в карантине доступны следующие параметры фильтрации:
В разделе **«Настройки Клиента».** В ниспадающем меню выберите **«Карантин».**

- ✓ Имя компьютера
- ✓ Название угрозы
- ✓ Группы
- ✓ Имя файла
- ✓ Дата карантина





Выберите файлы на карантине и нажмите кнопку **«Восстановить»,** чтобы восстановить файлы. Выберите файлы на карантине и нажмите кнопку **«Удалить»,** чтобы удалить файлы. Нажмите кнопку **«Настройки»** , чтобы изменить местоположение папки карантина и периода очистки файлов.



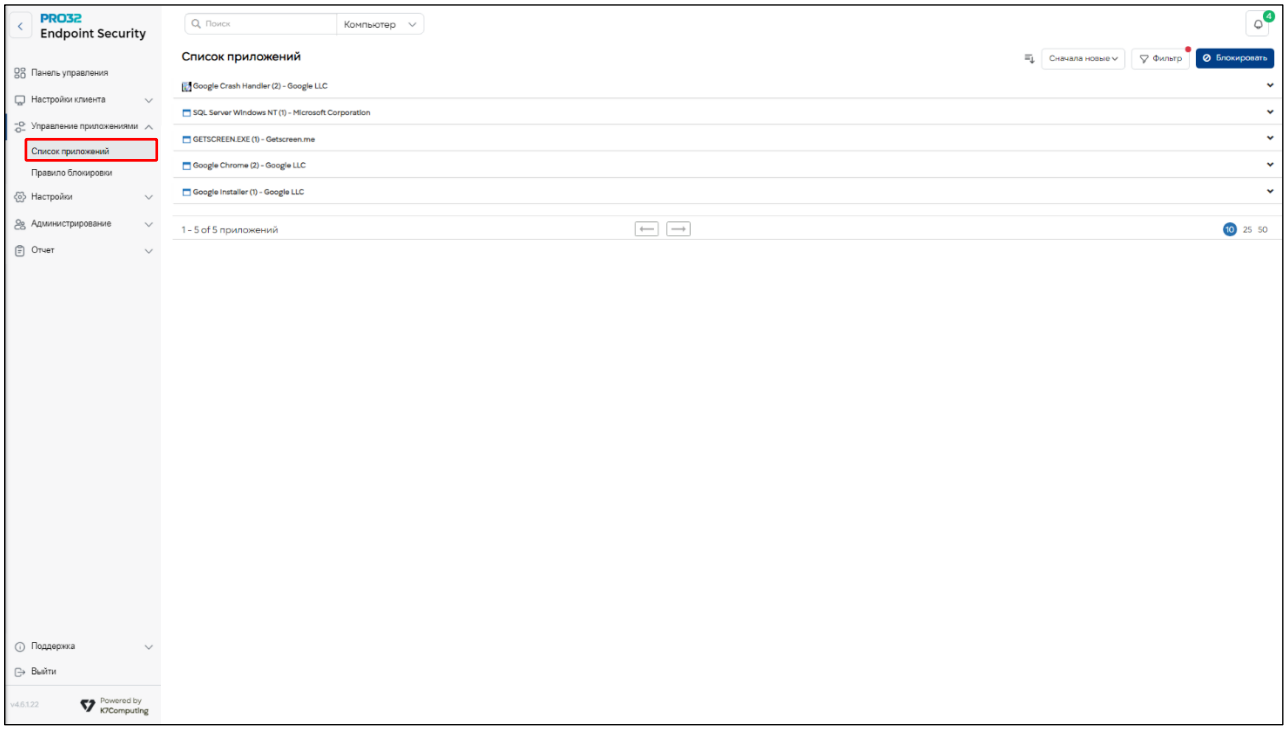
27. Управление приложениями

*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

устройКонтроль приложений - связан с безопасностью, целостностью и доступностью приложений только для конкретных пользователей. Цели контроля приложений связаны с безопасностью, целостностью и доступностью приложений только для предполагаемых пользователей. Используя управление приложениями, вы можете реализовать ограничения на использование приложений на клиентских компьютерах. Сетевые администраторы смогут контролировать нежелательные приложения, которые засоряют сеть. Эта функция эффективно решает проблемы безопасности, вызванные некоторыми приложениями, такими как мессенджеры, менеджеры загрузки и т.д.

- ✓ Вы можете заблокировать запуск приложения
- ✓ Вы можете заблокировать подключение приложения к Интернету
- ✓ Вы можете заблокировать полный доступ к сети для приложения

Раздел **«Управление приложениями».** В ниспадающем меню выберите **«Список приложений»:**



27.1 Просмотр списка приложений

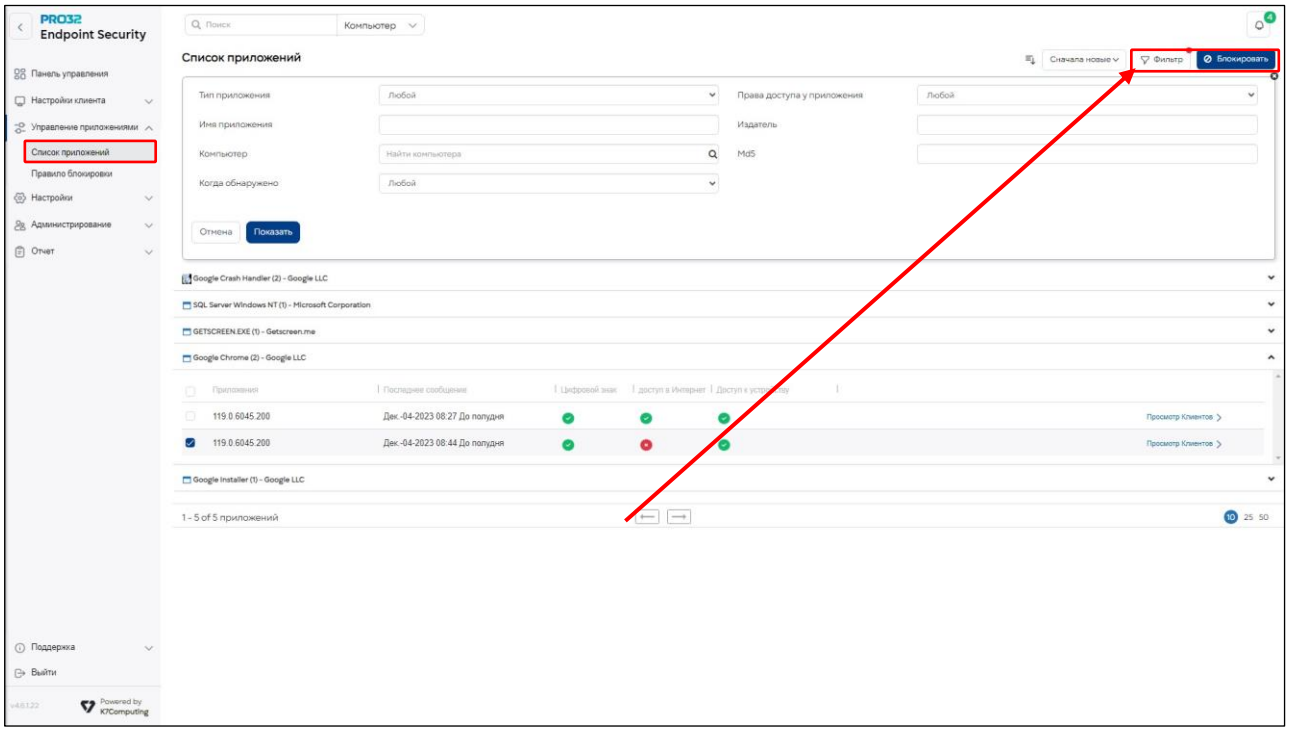
Управление приложениями осуществляется с помощью набора правил, которые определяют, могут ли указанные вами приложения выполняться, подключаться к Интернету или сети. Список приложений доступен на странице "Список приложений". Тип приложения:

- ✓ Название приложения
- ✓ Версия приложения
- ✓ Последний отчет
- ✓ Детали цифровой подписи
- ✓ Доступ к информации в Интернете
- ✓ Сведения о доступе пользователя
- ✓ Информация о клиенте

Вы можете использовать фильтры для просмотра списка приложений на основе следующих критериев

- ✓ Тип применения
- ✓ Чтение
- ✓ Название приложения

- ✓ Издатель
- ✓ Имя компьютера
- ✓ MD5
- ✓ Отчет



28. Блокировка приложений

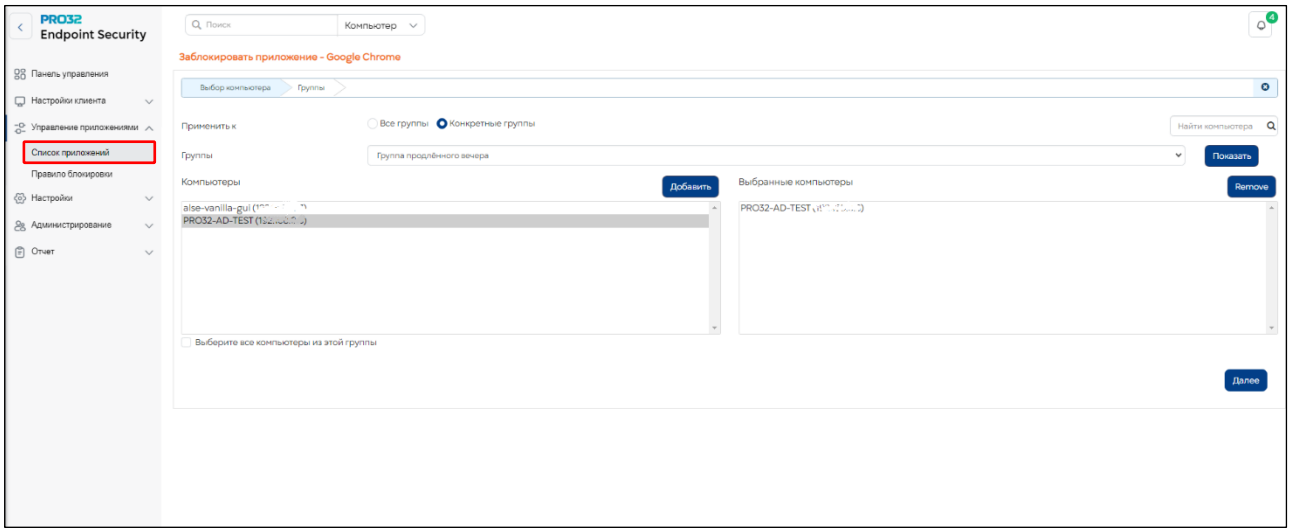
*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

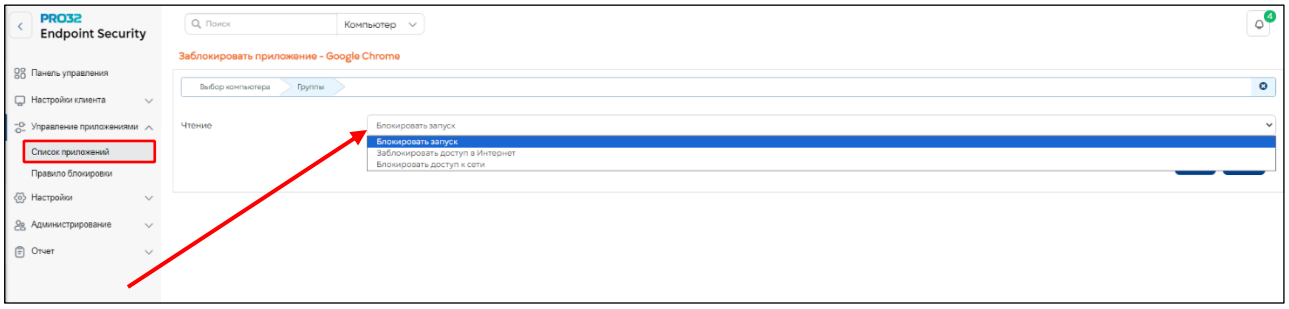
Вы можете искать приложения на основе параметров правообладателя/компьютера или фильтра, и выбранные приложения могут быть заблокированы на одном компьютере или на нескольких компьютерах в группе или нескольких группах.

Вы можете выбрать приложение из списка и нажать кнопку Заблокировать, для его блокировки.

Ограничение доступа возможно в следующих вариантах:

- ✓ Запретить запуск приложения
- ✓ Запретить приложению доступ в Интернет
- ✓ Запретить приложению доступ в Интернет и локальную сеть



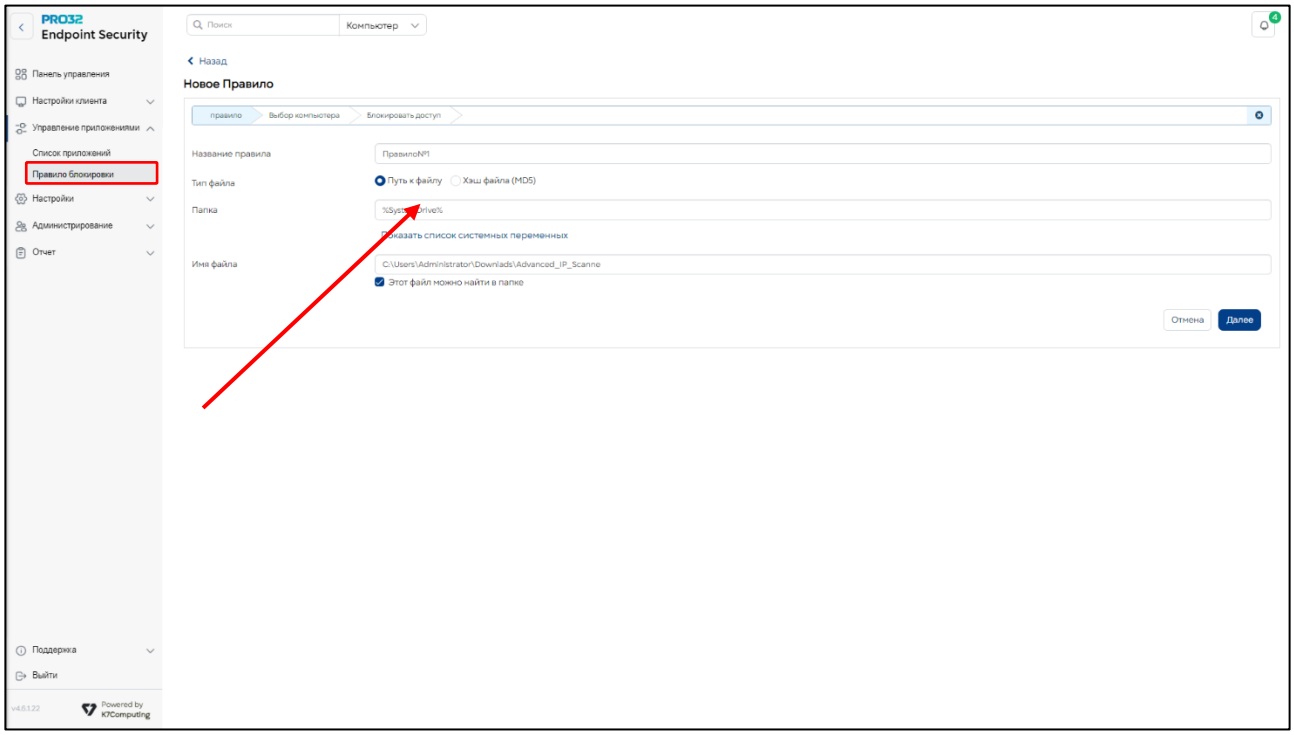


28.1 Правило блокировки приложений

*Данная опция доступна только в пакете PRO32 Endpoint Security Advanced

Эта функция позволяет администраторам блокировать приложения на основе их названия или MD5-хеша файла. Правило блокировки приложений может применяться к одному или нескольким компьютерам в одной или нескольких группах. Эта функция обеспечивает гибкость при выборе блокируемых приложений и позволяет сетевым администраторам решать проблемы безопасности и производительности, возникающие в результате неконтролируемого использования приложений в организации.

Чтобы добавить новое правило для приложения, нажмите «**Создать правило»**. Укажите имя правила и «координаты» блокируемого приложения: «Тип файла» («Путь к файлу» или «Хеш файла» (MD5)), «Папка» и «Имя файла».



29. Настройки

На странице настроек администраторы могут просматривать и настраивать все параметры продукта.

Чтобы открыть страницу настроек, откройте раздел **«Настройки».**

Можно настроить следующие параметры:

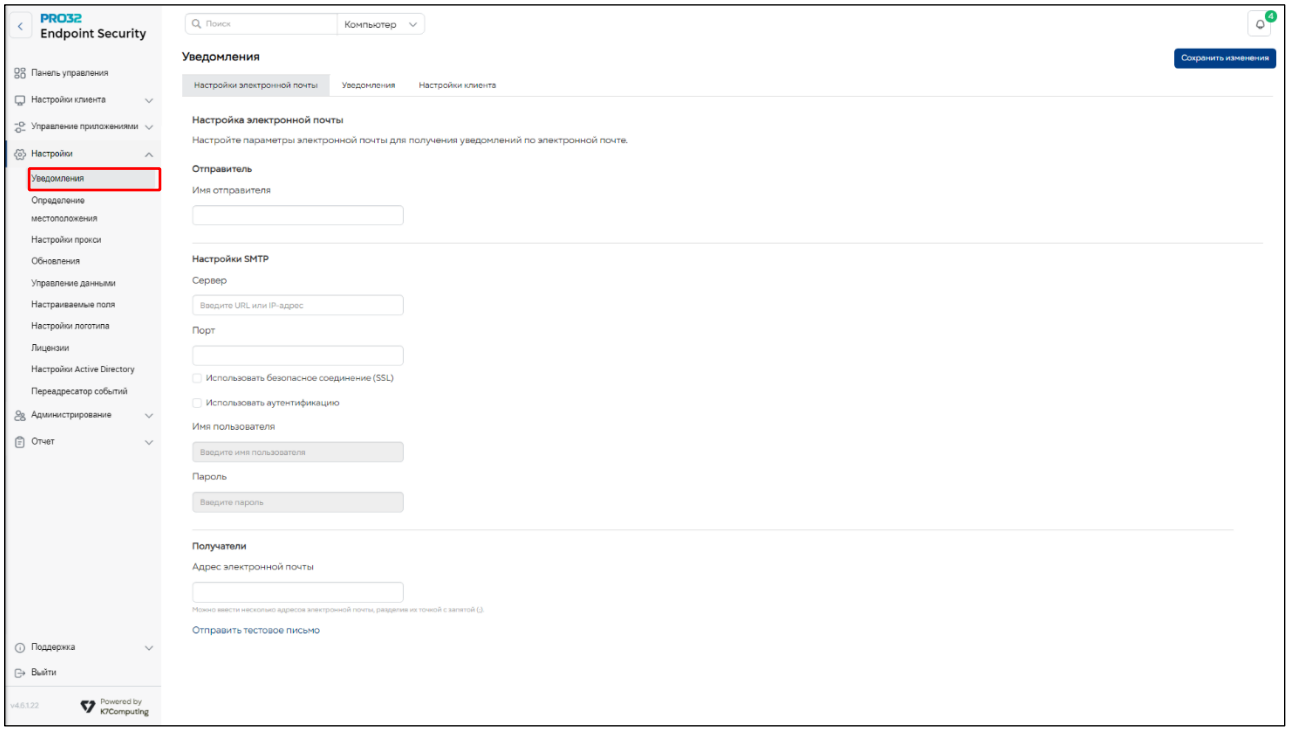
- ✓ Уведомления
- ✓ Обнаружение местоположения
- ✓ Настройки прокси

- ✓ Обновления
- ✓ Управление данными
- ✓ Управление настраиваемыми полями
- ✓ Веб-категории
- ✓ Лицензия
- ✓ Настройки Active Directory
- ✓ Переадресатор событий (Интеграция с SIEM)

29.1 Уведомления

Вы можете настроить параметры электронной почты для получения с клиентских компьютеров уведомлений о событиях PRO32 Endpoint Client и других уведомлений, связанных с безопасностью. Для этого необходимо указать параметры сервера SMTP, включая номер порта. Адреса электронной почты указываются в поле **«Получатели».**

Администратор может определить псевдонимы для отправителей электронных писем-уведомлений о событиях, связанных с безопасностью. Получив такое письмо, администратор с помощью имени пользователя может легко идентифицировать человека. При наличии большого числа конечных точек администратору может быть непросто определить, от какого именно пользователя пришло уведомление. **«Имя пользователя»** помогает быстро идентифицировать пользователя.



Администратор может определить псевдонимы для отправителей электронных писем-уведомлений о событиях, связанных с безопасностью. Получив такое письмо, администратор с помощью псевдонима может легко идентифицировать человека. При наличии большого числа конечных точек администратору может быть непросто определить, от какого именно пользователя пришло уведомление. Псевдоним помогает быстро идентифицировать пользователя.

Параметры SMTP можно протестировать перед сохранением, чтобы убедиться в их правильной настройке.

Укажите необходимые значения и нажмите кнопку **«Отправить тестовое сообщение».**

29.1.1 Настройка уведомлений о событиях по e-mail

Уведомления безопасности всегда приходят на информационную панель консоли и опционально – по электронной почте. В столбце «Оповещение по e-mail» для соответствующих событий указано, должны ли уведомления безопасности также присылаться по электронной почте. В столбце «Триггер» указан критерий возникновения события.

Администратор может настроить получение уведомлений о том, что клиентский компьютер не синхронизирован с антивирусной базой или в течение заданного периода времени не отправлял отчеты серверу управления. По умолчанию эти уведомления посылаются также по электронной почте. Можно указать количество дней, в течение которых ожидается отчет от клиентского компьютера. Значение по умолчанию – 7 дней. Срок ожидания выбирается администратором в интервале от 2 до 180 дней.

Также можно указать максимальный период ожидания обновления на клиентском компьютере определений вирусов до отправки уведомления администратору. Значение по умолчанию – 2 дня. Срок ожидания выбирается администратором в интервале от 2 до 180 дней.

В разделе **«Настройки» → «Уведомления»** можно настроить продолжительность хранения данных. Хранение данных по умолчанию отключено. Если оно включено, то срок хранения по умолчанию составляет 180 дней.

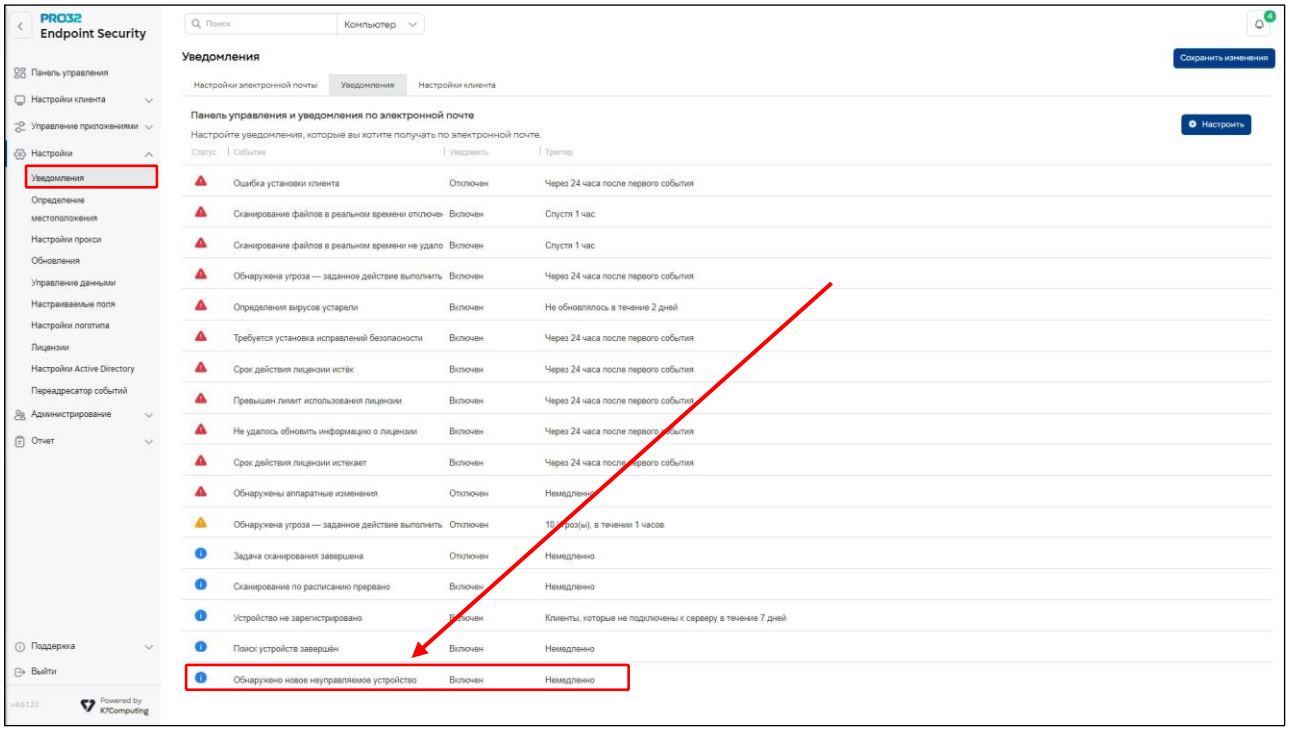
Срок хранения выбирается администратором в интервале от 2 до 180 дней.

29.1.2 Уведомления о не зарегистрированных устройствах

Шаг 1. Откройте раздел **«Настройки» → «Уведомления».**

Шаг 2. Перейдите на вкладку **«Уведомления».**

Шаг 3. Выберите в списке событие **«Компьютер, не отправляющий отчеты».**



Шаг 4. Нажмите кнопку **«Настроить»** в правом вернем углу.

Шаг 5. Разрешите оповещение по электронной почте и нажмите кнопку ОК.

Шаг 6: Нажмите кнопку **«Сохранить»,** чтобы сохранить настройки конфигурации уведомлений.

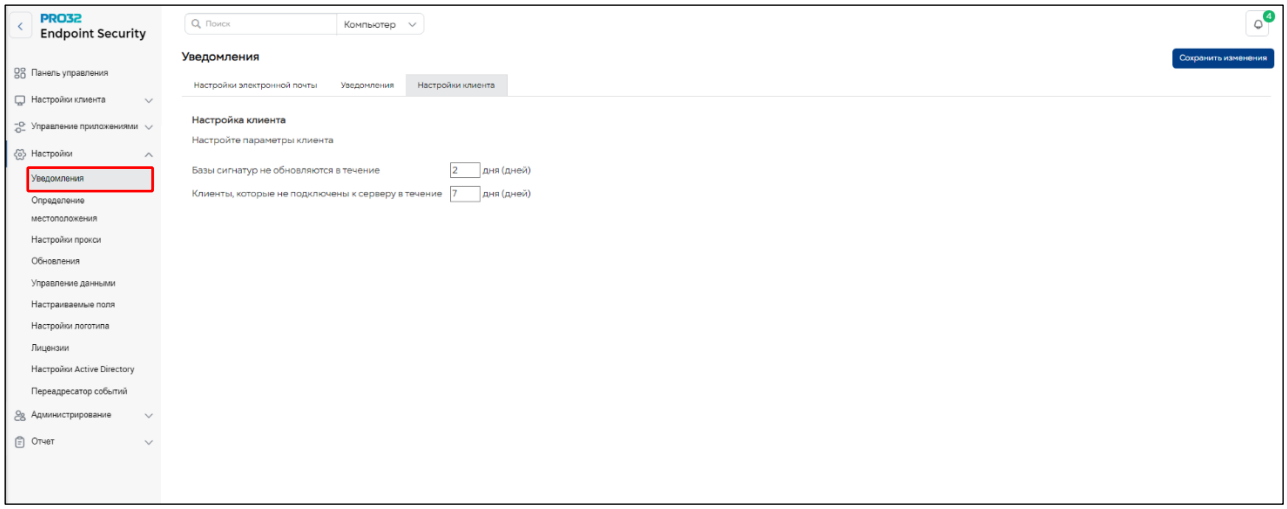
Шаги по настройке параметров клиента

Шаг 1: Выберите **«Настройки»** → **«Уведомления»** в меню настроек слева

Шаг 2: Выберите вкладку **«Настройки клиента»**

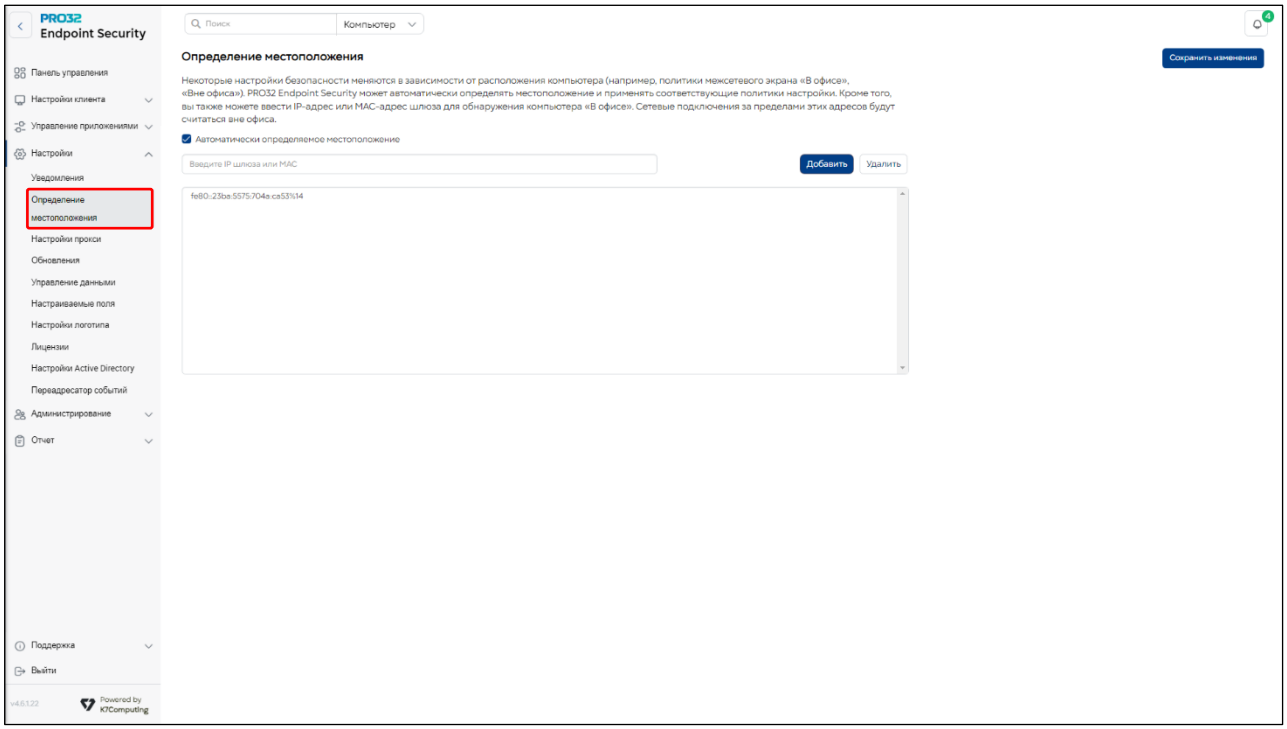
Шаг 3. Введите количество дней, по истечении которых будут отправлены уведомления о не подключающихся компьютерах.

Шаг 4. Нажмите кнопку «Сохранить», чтобы сохранить настройки.



29.2 Обнаружение местоположения

Некоторые настройки безопасности меняются в зависимости от расположения компьютера (например, политики межсетевого экрана «В офисе», «Вне офиса»). PRO32 Endpoint Security может автоматически определять местоположение и применять соответствующие политики настройки. Кроме того, вы также можете ввести IP-адрес или MAC-адрес шлюза для обнаружения компьютера **«В офисе».** Сетевые подключения за пределами этих адресов будут считаться вне офиса.

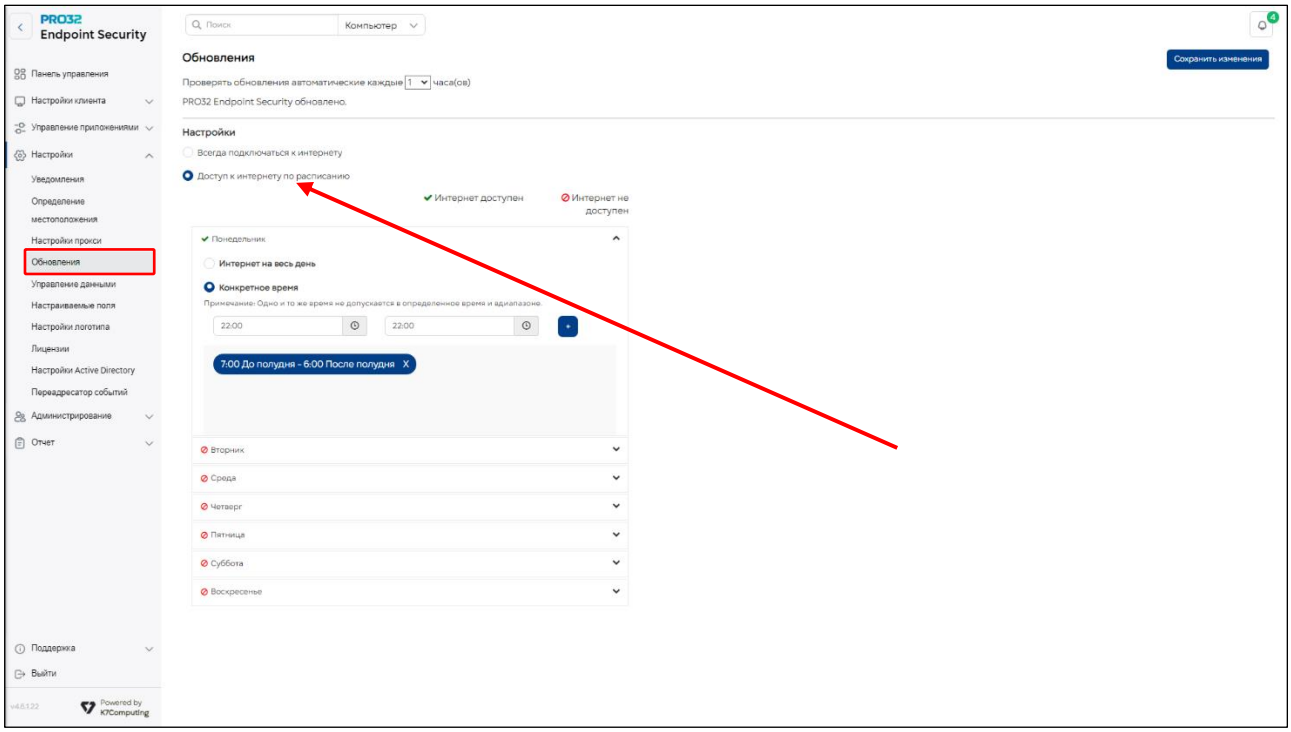


29.3 Настройки прокси

Вы можете настроить прокси для получения обновлений клиентского ПО. Для этого укажите прокси-сервер, номер порта и имя пользователя.

29.4 Обновления

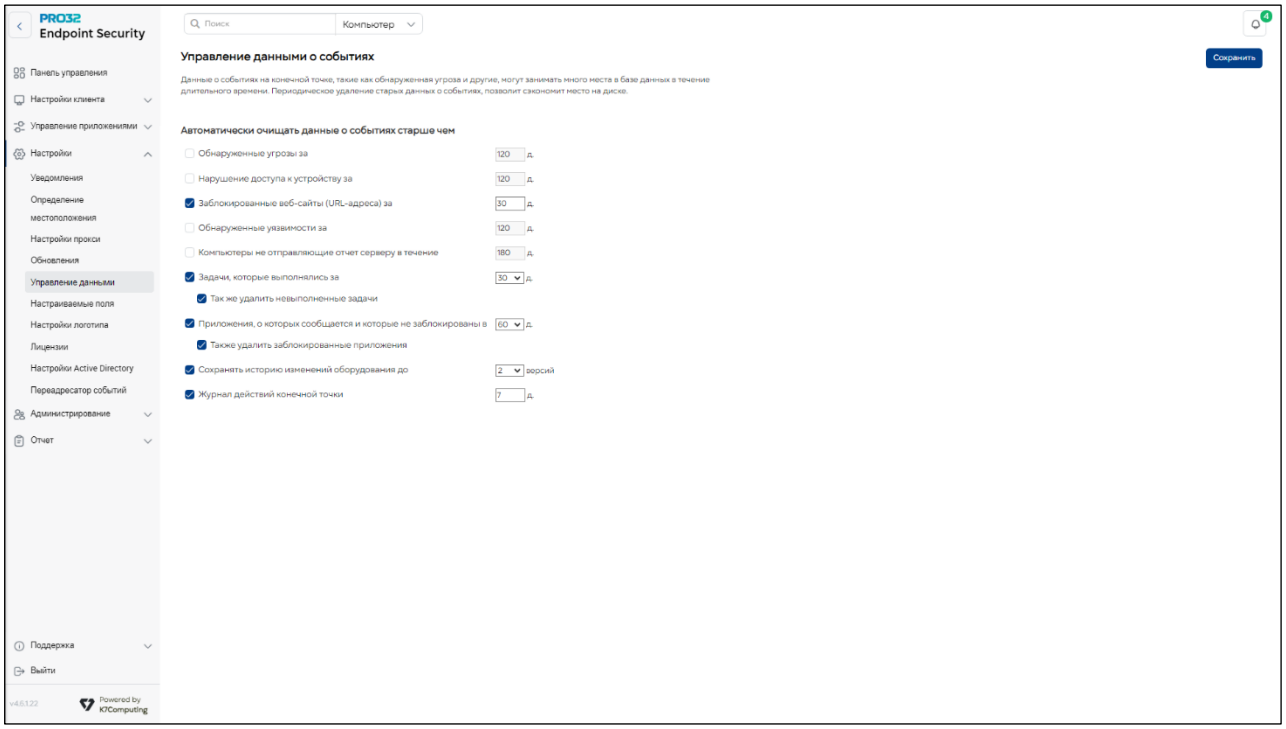
Вы можете настроить периодичность проверки сервером наличия обновлений. А также задать расписание доступности интернета для проверки наличия обновлений.



29.5 Управление данными

Для правильного управления хранилищем необходимо регулярно удалять старые и ненужные данные. Вы можете настроить периодичность автоматического удаления данных о различных событиях.

Такими событиями являются обнаружение угроз, нарушение правил доступа к устройствам, попытки доступа к заблокированным веб-сайтам и т. д.

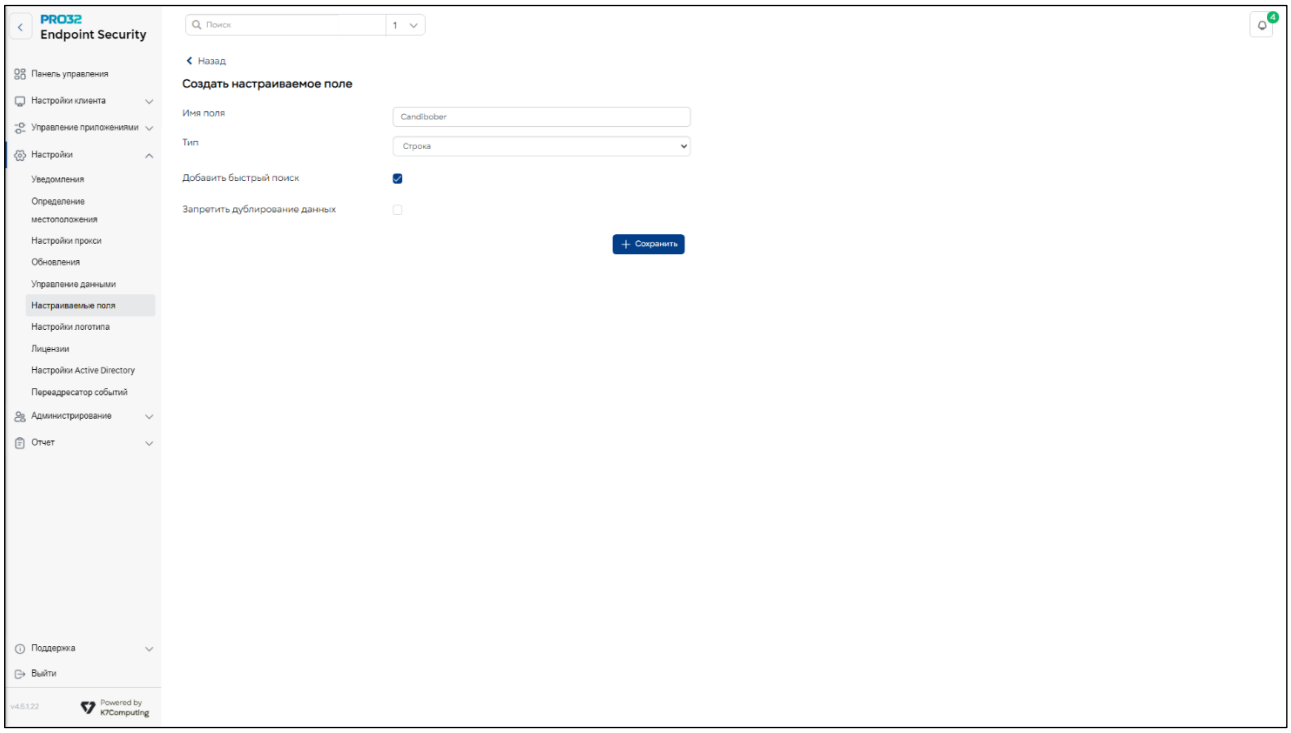


29.6 Добавление настраиваемых полей

Настраиваемые поля позволяют создавать новые поля в дополнение к существующим клиентским полям по умолчанию.

Благодаря функции добавления настраиваемых полей администратор может вставить на страницу **«Настройки клиента»** необходимые ему данные строкового или числового типа. Затем эти данные администратор может использовать при поиске клиентских компьютеров всякий раз, когда ему требуется создать отчет или назначить задачу (сканирование, обновление и т. д.) отдельному компьютеру или группе компьютеров.

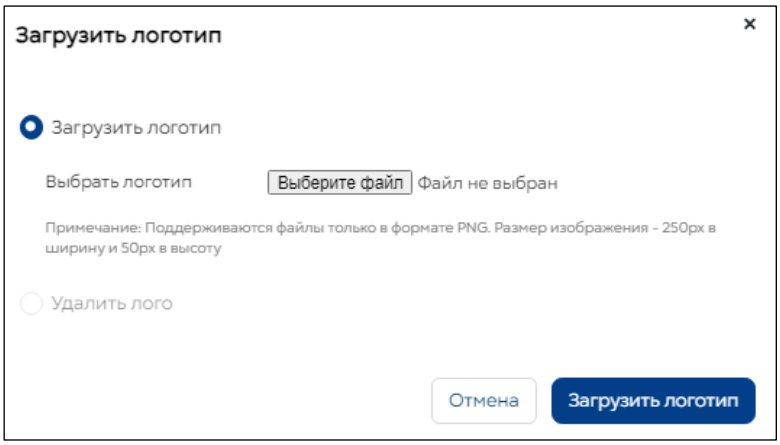
Благодаря настраиваемым полям администратор получает больше возможностей для управления конечными точками.



Важно! Поддерживаются только латинские символы.

29.7 Изменение логотипа

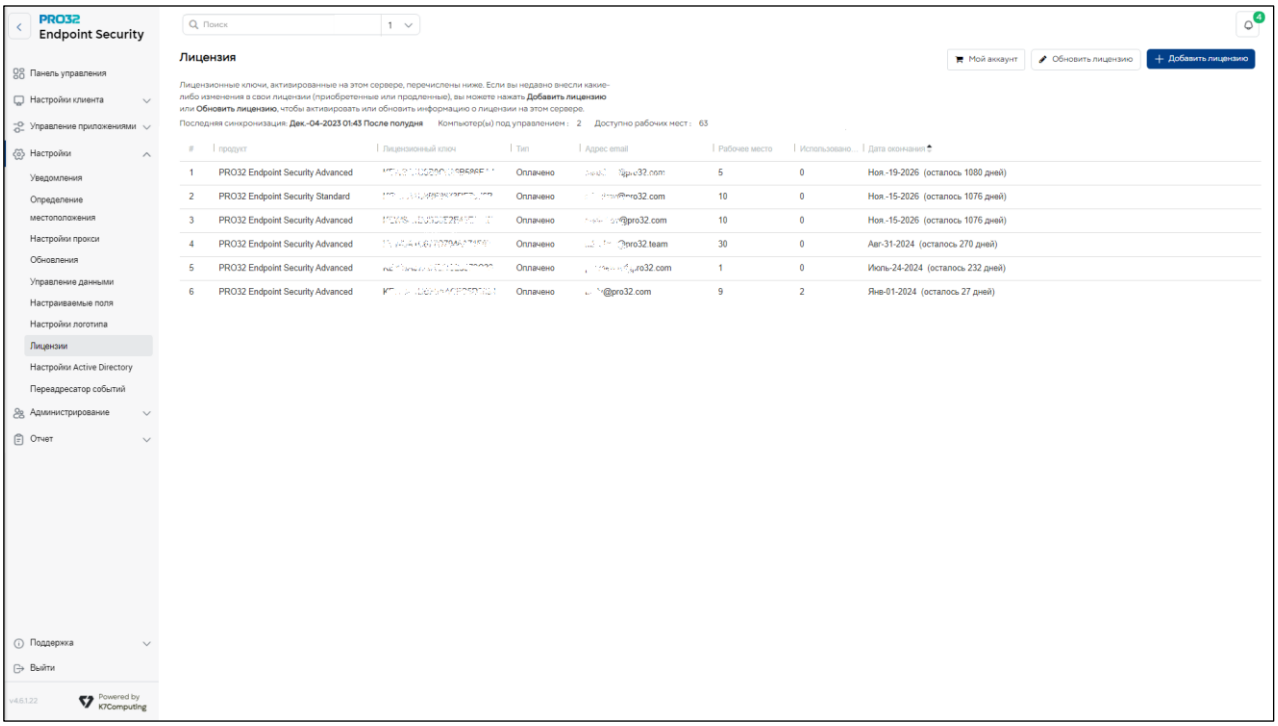
С помощью этой функции можно сменить логотип, который отображается на экране входа в систему, консоли администрирования и на страницах отчетов. Загруженный администратором логотип должен иметь такой размер, чтобы поместиться на вышеупомянутых страницах. После добавления логотипа его можно сменить в любое время, нажав кнопку «Сменить логотип».



29.8 Лицензии

После авторизации на сервере вы можете просмотреть свои «Активированные лицензионные ключи». Если вы недавно внесли какие-либо изменения в свои лицензии (приобрели или продлили их), нажмите «Добавить лицензию» или «Обновить лицензию», чтобы активировать или обновить информацию на этом сервере.

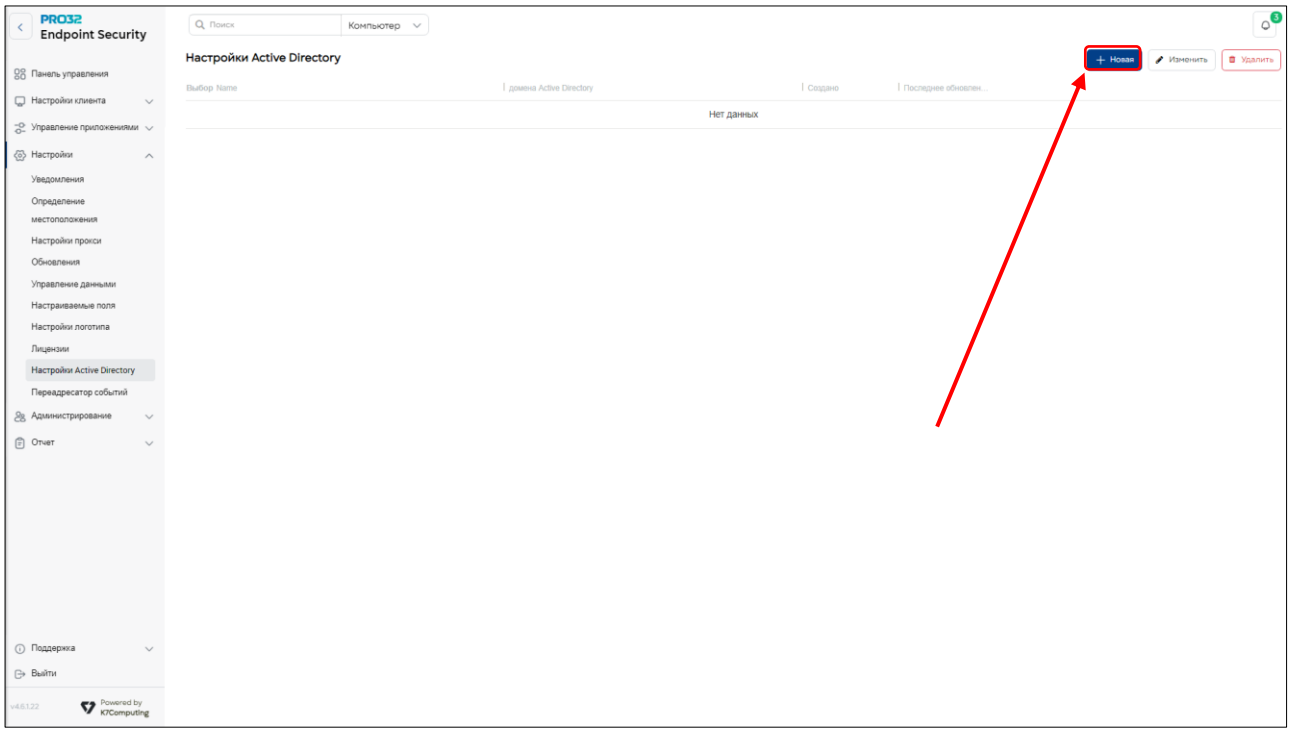
Со страницы настройки лицензий вы можете перейти на страницу авторизации для входа на сервер под другой учетной записью и управления соответствующими лицензиями.



29.9 Настройки Active Directory

Раздел обнаружение устройств позволяет запустить процесс поиска необходимых устройств в структуре Active Directory. Первоначально необходимо добавить информацию о домене в консоль администрирования в разделе настройки Active Directory. После успешного добавление информации о домене необходимо запустить Поиск неуправляемых устройств для этого необходимо выполнить следующие шаги:

1. Для добавления параметров домена необходимо перейти по пути **Настройки → Настройки Active Directory**. Затем нажмите кнопку **«Новая»** в правом верхнем углу.



2. Задайте параметры домена Active Directory. Вы можете проверить состояние соединения, нажав кнопку «Тестовое соединение». Сохраните настройки.

Домен

Полное доменное имя должно быть введено в формате Distinguished Name (DN). Например,

Каноническое имя	Выдающееся имя
mydomain.com	DC=mydomain,DC=com
division.mydomain.com	DC=division,DC=mydomain,DC=com
sales.division.mydomain.com	DC=sales,DC=division,DC=mydomain,DC=com

Примечание: Если у вас есть OU, домен должен быть введен в формате OU=Staff,DC=mydomain,DC=com

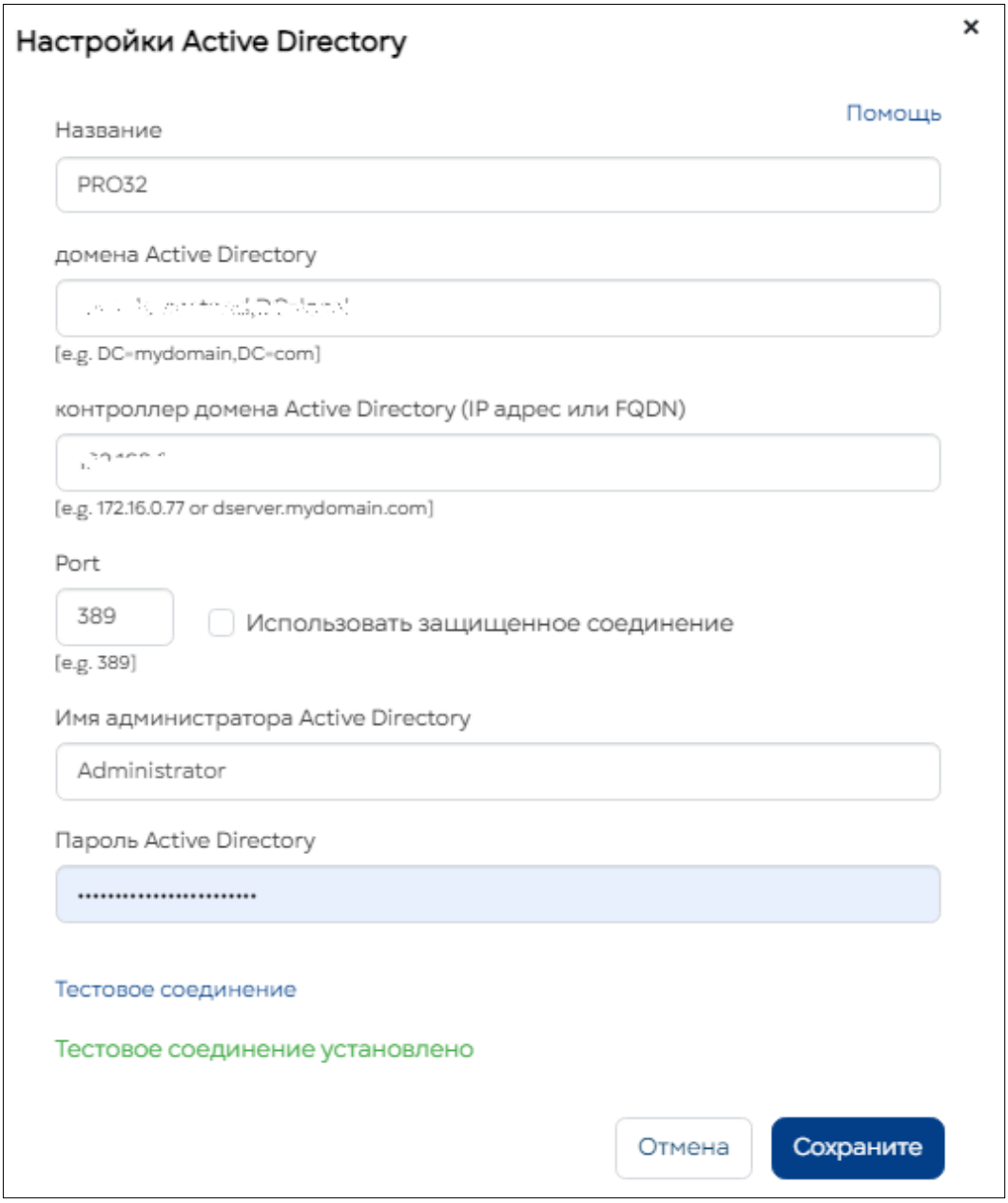
Контроллер домена

Необходимо ввести имя сервера контроллера домена. Имя компьютера не должно включать доменное имя.

Например, если имя компьютера контроллера домена **dserver.mydomain.com**, Только **dserver** необходимо ввести.

Domain Administrator Credentials

Имя пользователя и пароль администратора домена необходимы для получения списка компьютеров из Active Directory.

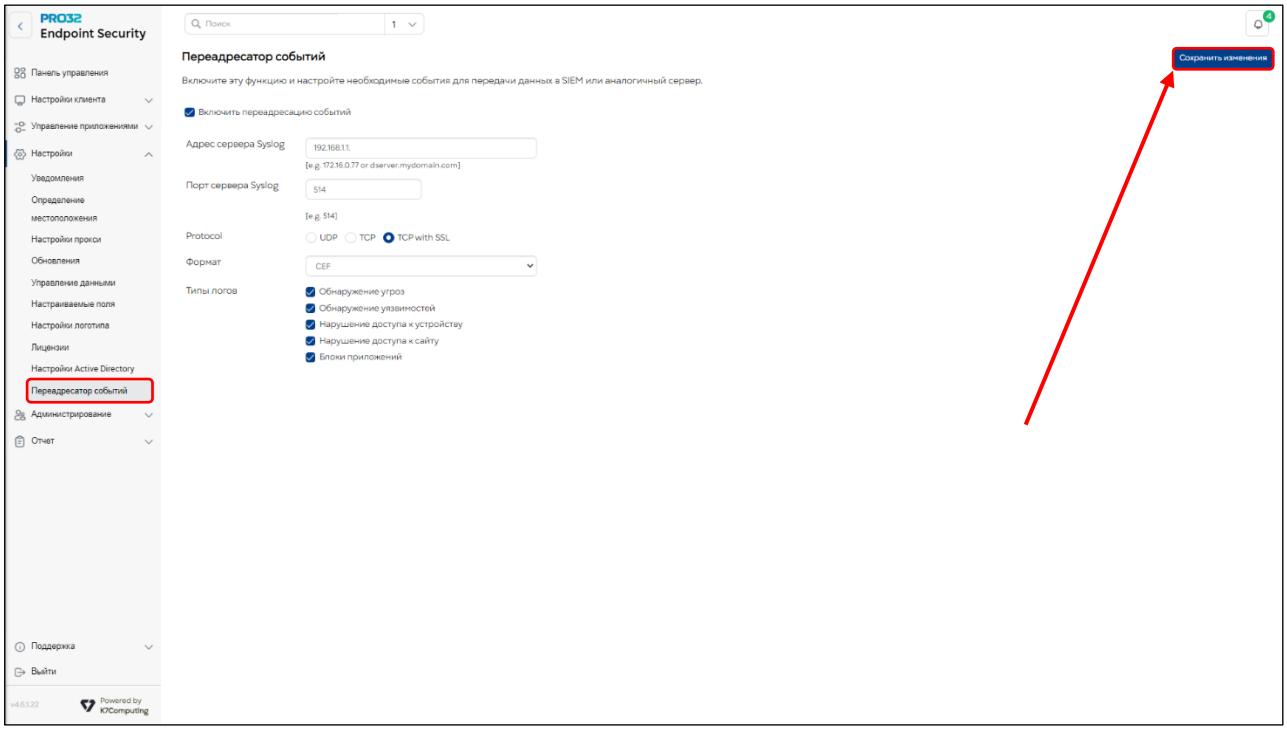


29.10 Переадресатор событий (Интеграция с SIEM)

Данный радел позволяет переадресовывать данные в SIEM систему по протоколу Syslog. Откройте раздел **«Настройки».** Слева, в ниспадающем меню выберите **«Переадресатор событий»:**

Для переадресация необходимо выполнить следующие шаги:

1. Указать сервер куда необходимо отправить данные
2. Указать порт сервера SIEM
3. Выбрать протокол передачи данных в SIEM и формат передаваемых данных
4. Выбрать типы логов, которые необходимо передать в сервер SIEM
5. После ввода всех данных необходимо сохранить изменения в данном разделе, нажав кнопку «Сохранить изменения» в правом верхнем углу. Если данные были введены корректно, то все необходимые журналы будут отправлены в SIEM



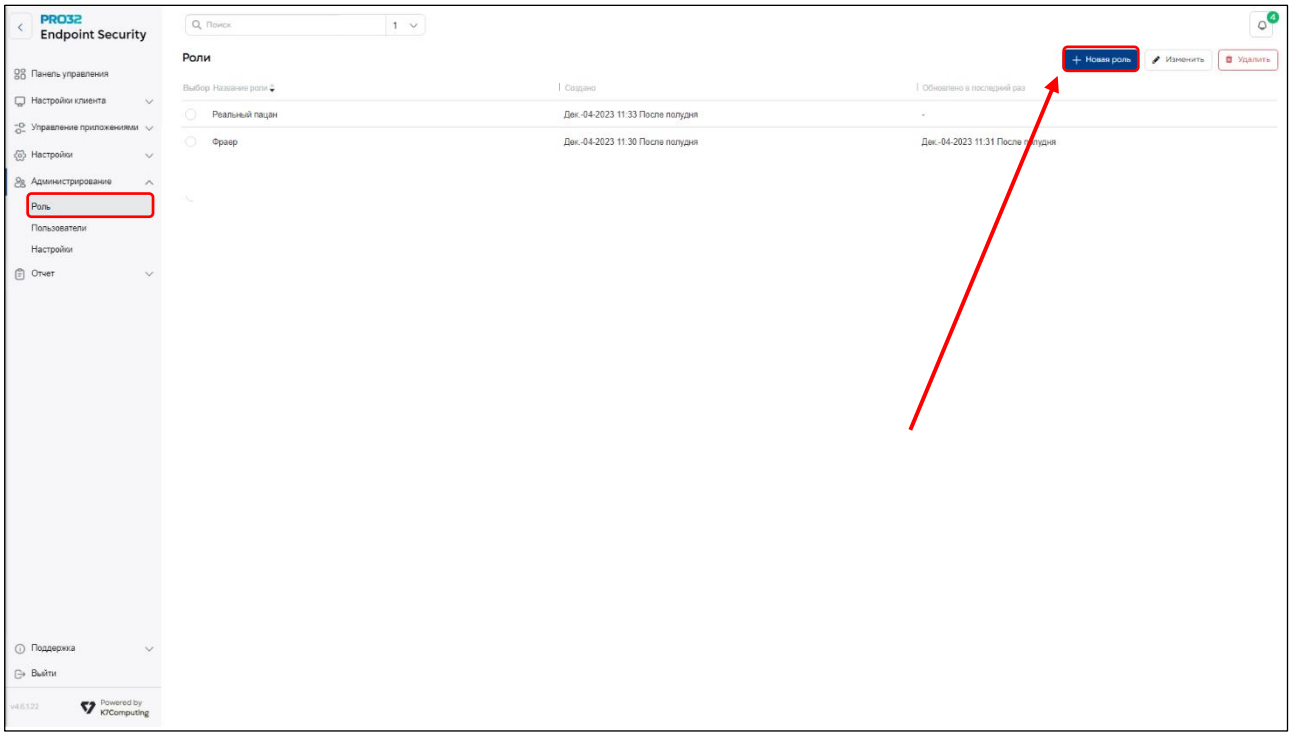
30. Администрирование

Эта функция позволяет создавать пользователей-администраторов и настраивать роли. Вы можете назначить созданных администраторов определенным группам и предоставить им посредством ролей необходимые права.

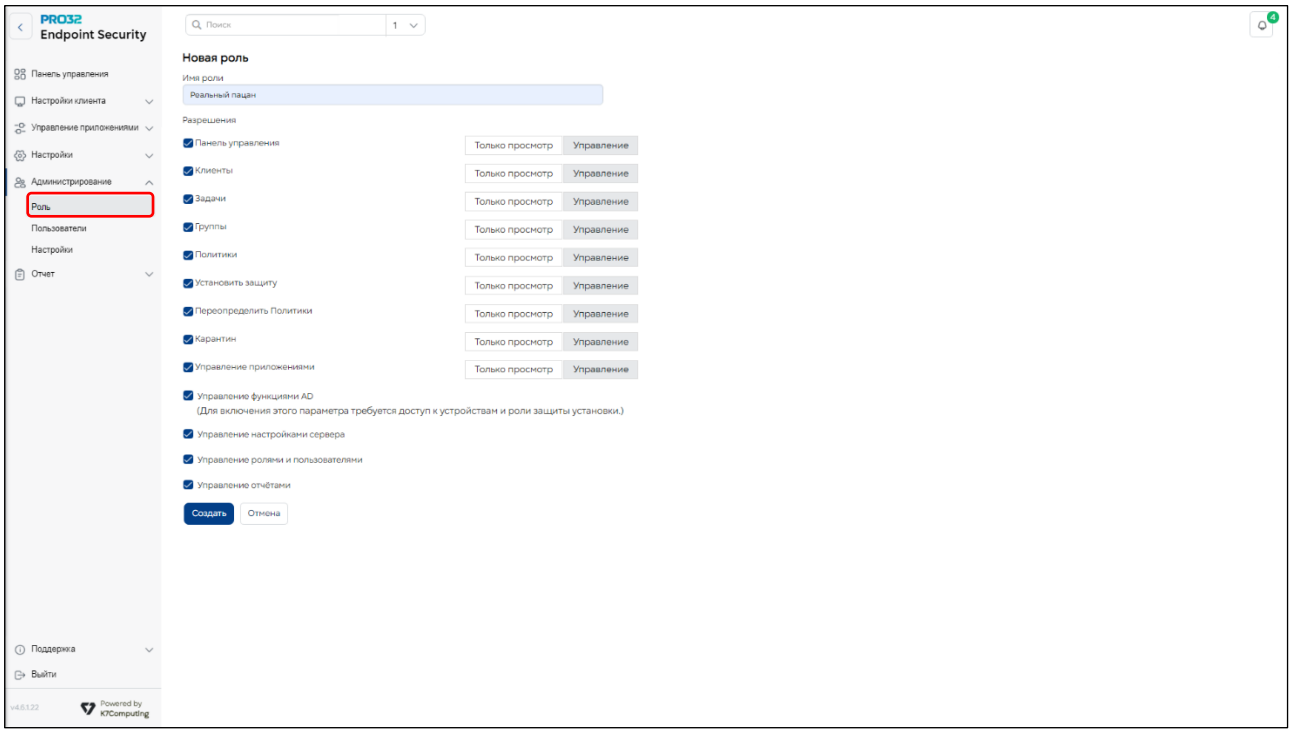
30.1 Роли администраторов

Вы можете создавать роли, которые дают пользователям право либо выполнять определенные действия, либо только просматривать определенную информацию. Позднее созданные роли могут быть назначены вновь созданным пользователям-администраторам.

Откройте раздел **«Администрирование».** Слева, в ниспадающем меню выберите **«Роль»:**



Для создания роли нажмите кнопку **«Новая роль»** в правом верхнем углу. Введите релевантное название для нее и укажите необходимые разрешения для выполнения следующих действий:



- Информационная панель
- Клиенты
- Задачи
- Группы
- Политики
- Установка PRO32 Endpoint Client
- Переопределяющая политика
- Карантин
- Управление приложениями
- Управление настройками сервера
- Управление ролями и пользователями
- Управление отчетами

Чтобы создать новую роль с выбранным разрешениями, нажмите кнопку **«Создать».**

30.2 Пользователи

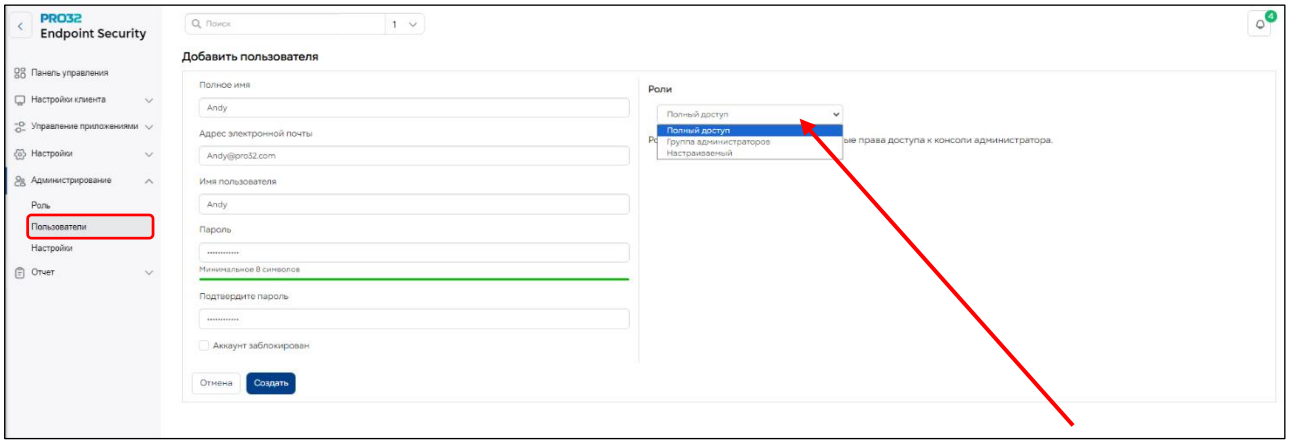
Этот раздел позволяет создать учётные записи администраторов консоли PRO32 Endpoint Security с разными правами доступа к данным и управлением продуктом.

Откройте раздел **«Администрирование».** Слева, в ниспадающем меню выберите **«Пользователи».**

Чтобы создать нового пользователя, укажите следующие параметры и нажмите кнопку **«Добавить Пользователя»:**

- ✓ Полное имя
- ✓ Адрес электронной почты
- ✓ Имя пользователя
- ✓ Пароль
- ✓ Повторный ввод пароля
- ✓ Активная/неактивная учетная запись

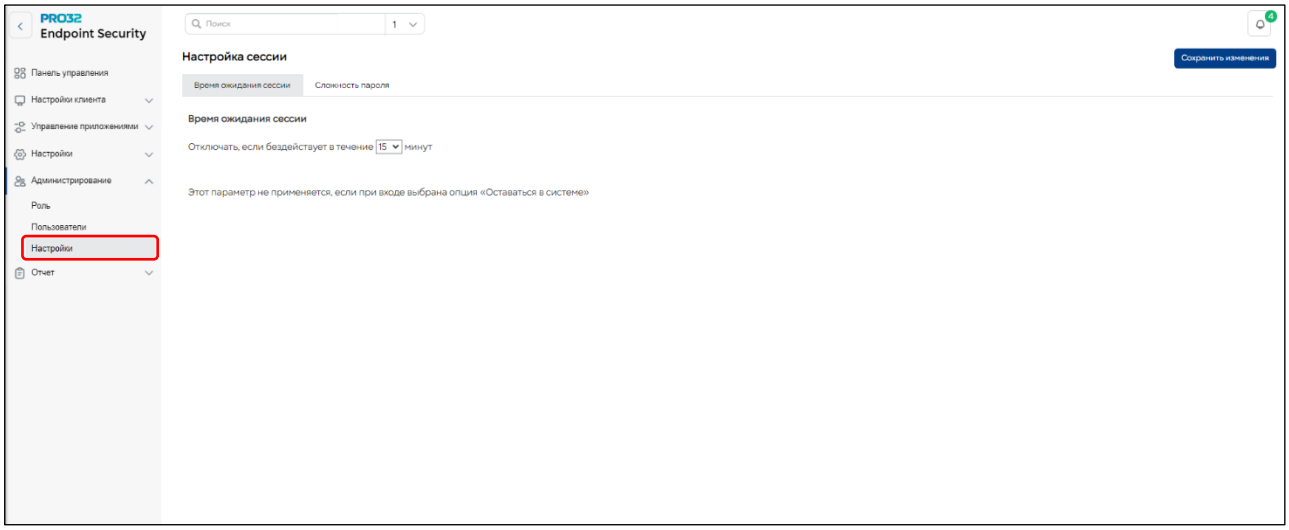
Для выбора роли используйте выпадающий список «Роли». В нем перечислены уже созданные ранее роли. По умолчанию новым пользователям назначается роль «Полный доступ».



30.3 Настройки сеанса

Эта функция позволяет задать продолжительность ожидания завершения сеанса самим пользователем до принудительного завершения системой. По умолчанию – 15 минут. Максимальное значение – 60 минут. Этот параметр не используется, если при входе в систему был установлен флажок «Оставаться в системе».

Откройте раздел **«Администрирование».** Слева, в ниспадающем меню выберите **«Настройки».**



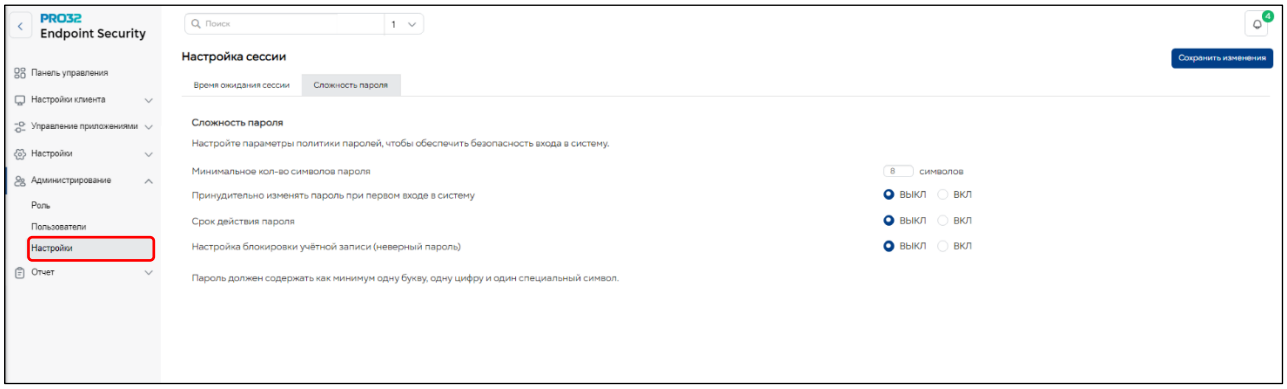
30.4 Настройка параметров пароля для входа в консоль

Пароль для входа в консоль имеет ряд параметров, которые могут быть настроены. Ниже приведен список этих параметров.

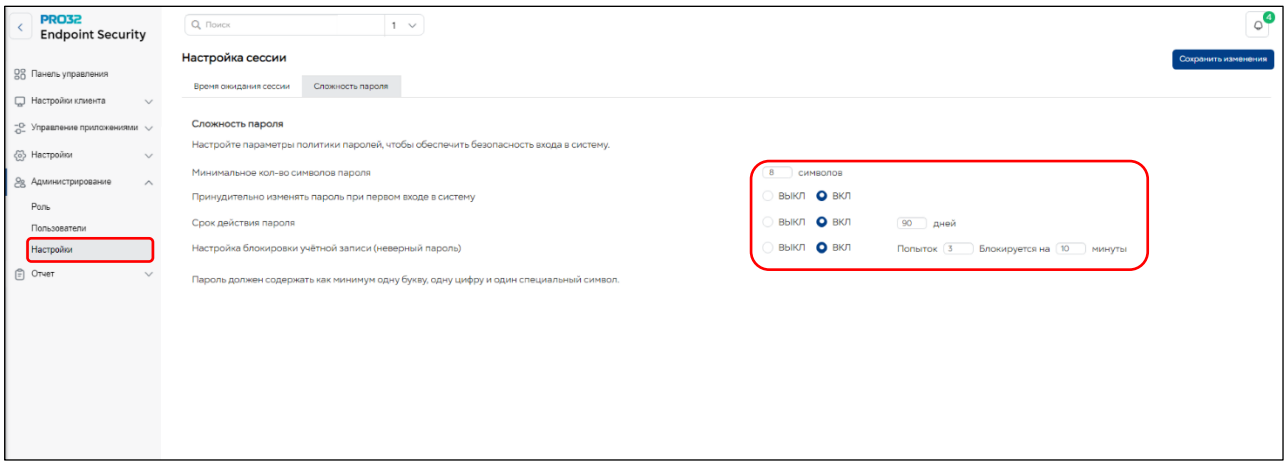
- **Минимальная длина пароля** – минимально допустимое количество символов в пароле. Значение по умолчанию – 8 символов. Администратор может установить желаемое значение в диапазоне от 8 до 50 символов. Пароль должен содержать как минимум один буквенный символ, одну цифру и один специальный символ.
- **Принудительная смена пароля** – при первом входе пользователя в систему потребовать сменить пароль. По умолчанию этот параметр отключен.
- **Срок действия пароля** – количество дней, по истечении которых пароль перестанет быть действительным, и при следующем входе система запросит сменить пароль. Если параметр включен, срок действия пароля по умолчанию составляет 90 дней. Его можно изменить в интервале от 1 до 365 дней. По умолчанию этот параметр отключен.
- **Блокировка учетной записи при попытке ввода неверного пароля** – обеспечивает блокировку входа пользователя в систему в течение указанного периода, если количество неудачных попыток ввода превышает указанное пороговое значение. Во время блокировки администратор может сменить пароль, если пользователю требуется войти в систему. По умолчанию этот параметр отключен. Если параметр включен, значение по умолчанию для допустимого порогового количества – 3 попытки, а значение по умолчанию для продолжительности блокировки – 10 минут. Администратор может установить первый параметр в диапазоне от 1 до 10 попыток и второй параметр – от 1 до 60 минут.

Откройте раздел **«Администрирование».** Слева, в ниспадающем меню выберите **«Настройки».** Нажмите вкладку **«Сложность пароля».**

Ниже показан экран настроек, когда все параметры имеют значения по умолчанию.



А так выглядит экран настроек, когда все параметры включены.



31. Отчеты

Эта функция помогает пользователям создавать отчеты о событиях различных типов, по группам клиентских компьютеров и за нужный период. Предусмотрены гибкие возможности для формирования сводных и подробных отчетов.

Для создания сводного отчета необходимо указать следующие параметры:

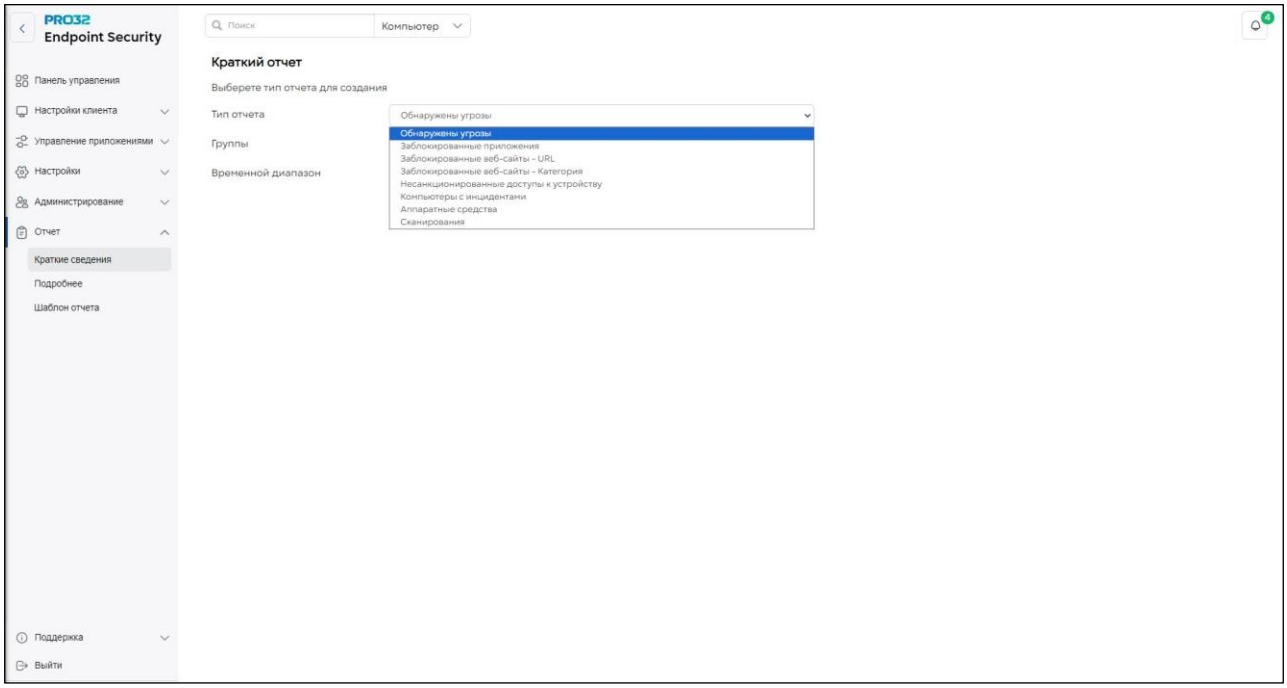
- Тип отчета
- Обнаруженные угрозы
- Заблокированное приложение
- Заблокированный веб-сайт – URL-адрес
- Заблокированный веб-сайт – категория
- Сводка о нарушениях правил доступа к устройствам
- Компьютер с инцидентами
- Аппаратные средства
- Группа
- Какая группа
- Временной интервал
- Последние 24 часа
- Последняя неделя
- Последний месяц
- Последний год
- Определенный временной интервал

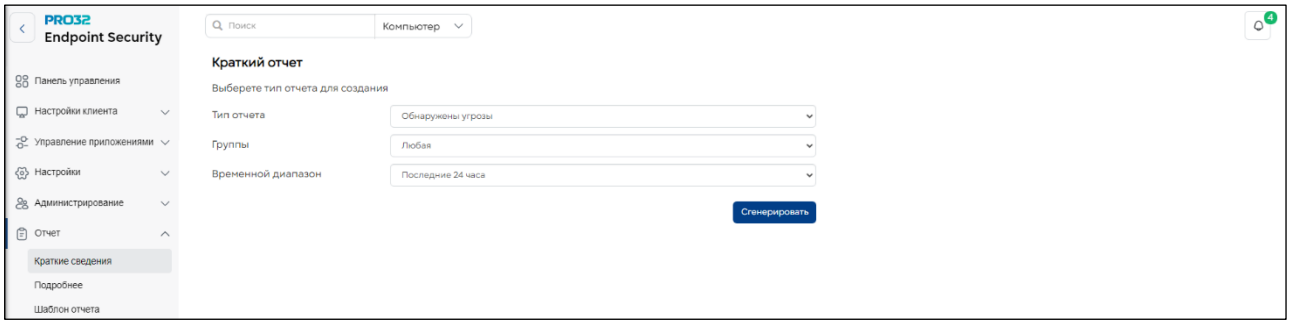
31.1 Краткий отчёт

Функция формирования отчетности была расширена – добавлены возможности создания и просмотра коротких и подробных отчетов по сканированию на основе различных параметров.
Краткий отчет может быть создан для любого из перечисленных ниже типов сканирования:

- Запланированное сканирование
- Сканирование для выявления вредоносного ПО
- Сканирование по запросу

Нажмите кнопку **«Сгенерировать»**, чтобы сформировать отчет с выбранными параметрами.





31.2 Подробный отчет

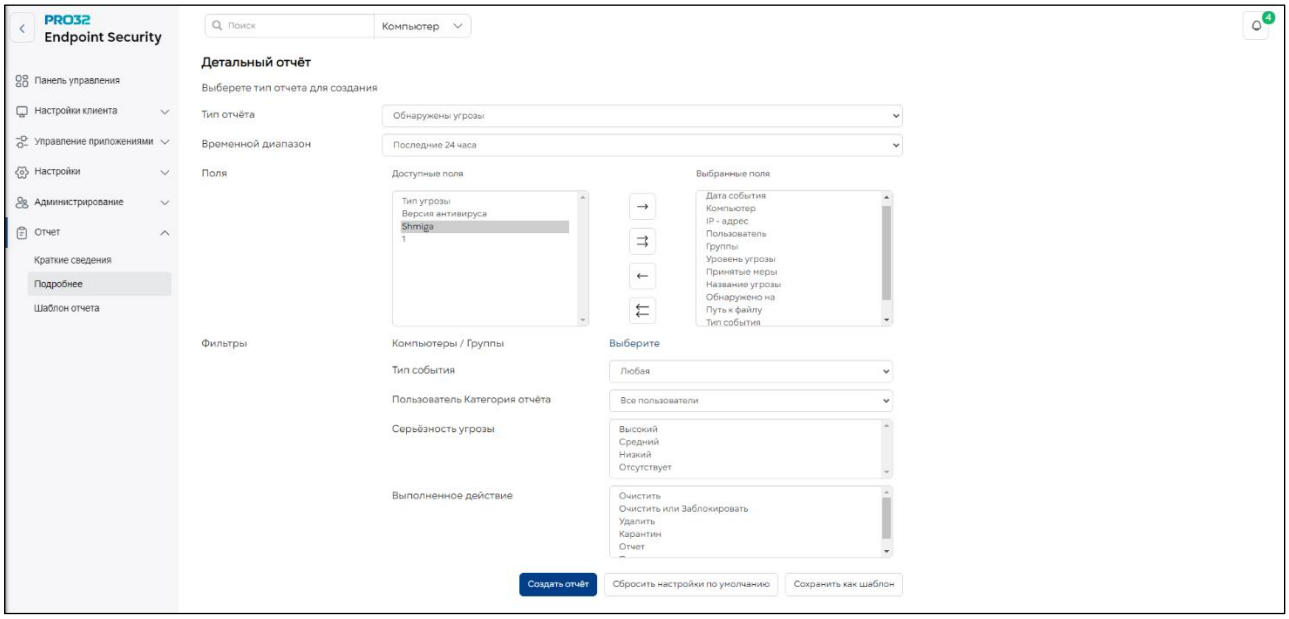
Подробные отчеты по сканированию могут содержать события следующих типов:

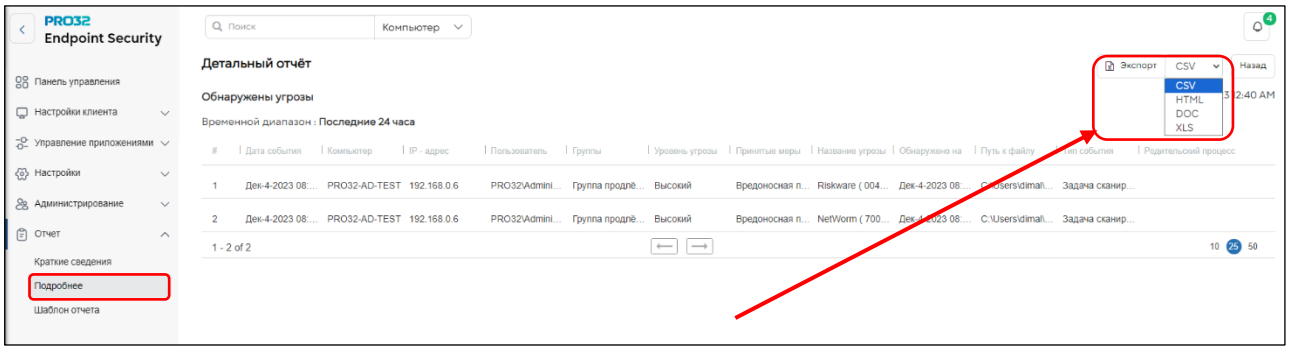
- Любое
- Запланированное сканирование
- Сканирование по запросу, инициированное задачей
- Сканирование по запросу, инициированное пользователем
- Сканирование при доступе
- Защита на основе анализа поведения
- Защита от эксплойтов
- Сканирование электронной почты

Создание подробного отчета: тип отчета – обнаруженные угрозы

1. Откройте раздел **«Отчёты».** Слева, в ниспадающем меню выберите **«Подробнее».**
2. Выберите в качестве типа отчета «Обнаруженные угрозы».
3. Укажите период.
4. Используйте клавиши со стрелками перенесите нужные поля из доступных в выбранные.
5. При необходимости установите нужные фильтры.
6. Нажмите кнопку «Сгенерировать» – отчет будет отображен в консоли.

Отчет можно экспортировать в любом из поддерживаемых форматов файлов.





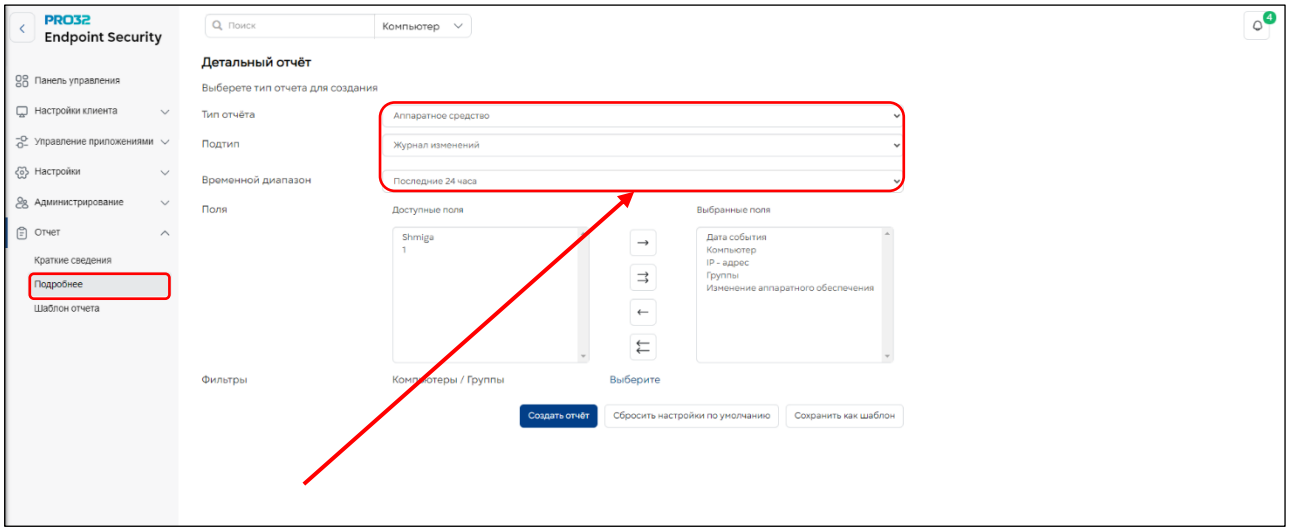
Создание отчетов по журналу изменений состава аппаратных средств

Теперь пользователь может создать отчет об изменении состава аппаратных средств для заданного набора компьютеров. Как и с любым другим отчетом, пользователь может либо просмотреть его в консоли, либо экспортировать в поддерживаемый формат.

1. Откройте раздел **«Отчёты».** Слева, в ниспадающем меню выберите **«Подробнее».**

2. Выберите в качества типа отчета **«Аппаратные средства».**

3: Выберите “Журнал изменений” в подтипе



4. Выберите необходимые поля для включения в отчет.

5. Выберите один или несколько компьютеров или групп.

6. Нажмите кнопку «Сгенерировать», чтобы сформировать отчет.

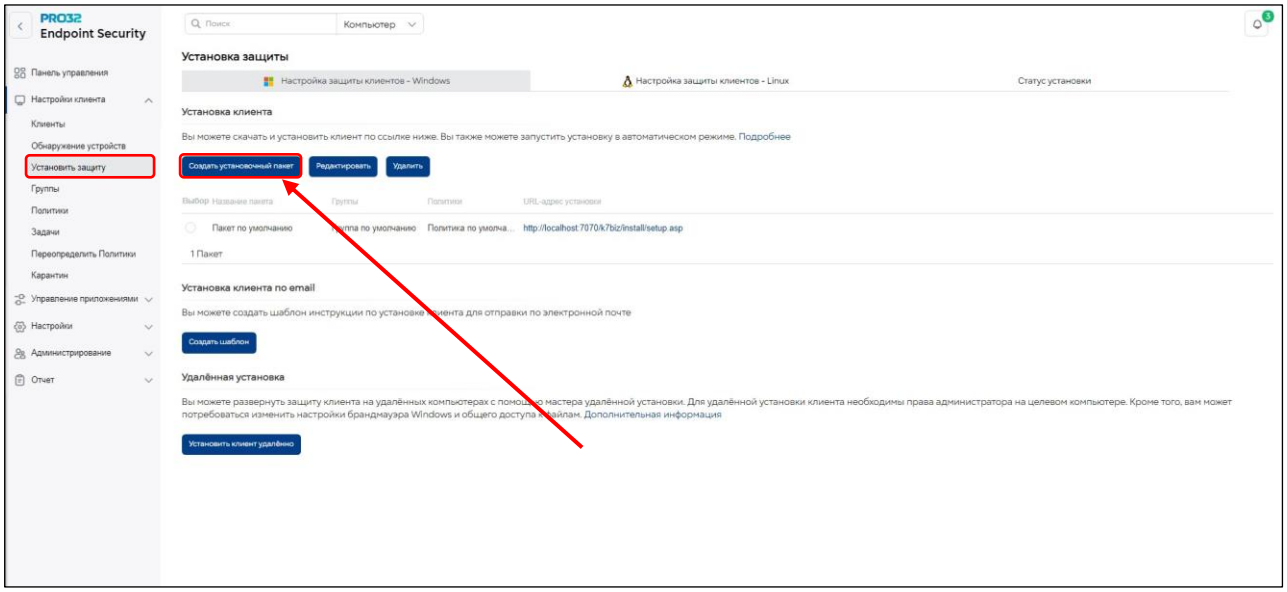
7. Просмотрите отчет об изменении состава аппаратных средств, который будет содержать информацию о времени изменения, имени компьютера, IP-адресе и группе.

31.3 Экспорт полного отчета по аппаратным средствам в различных форматах

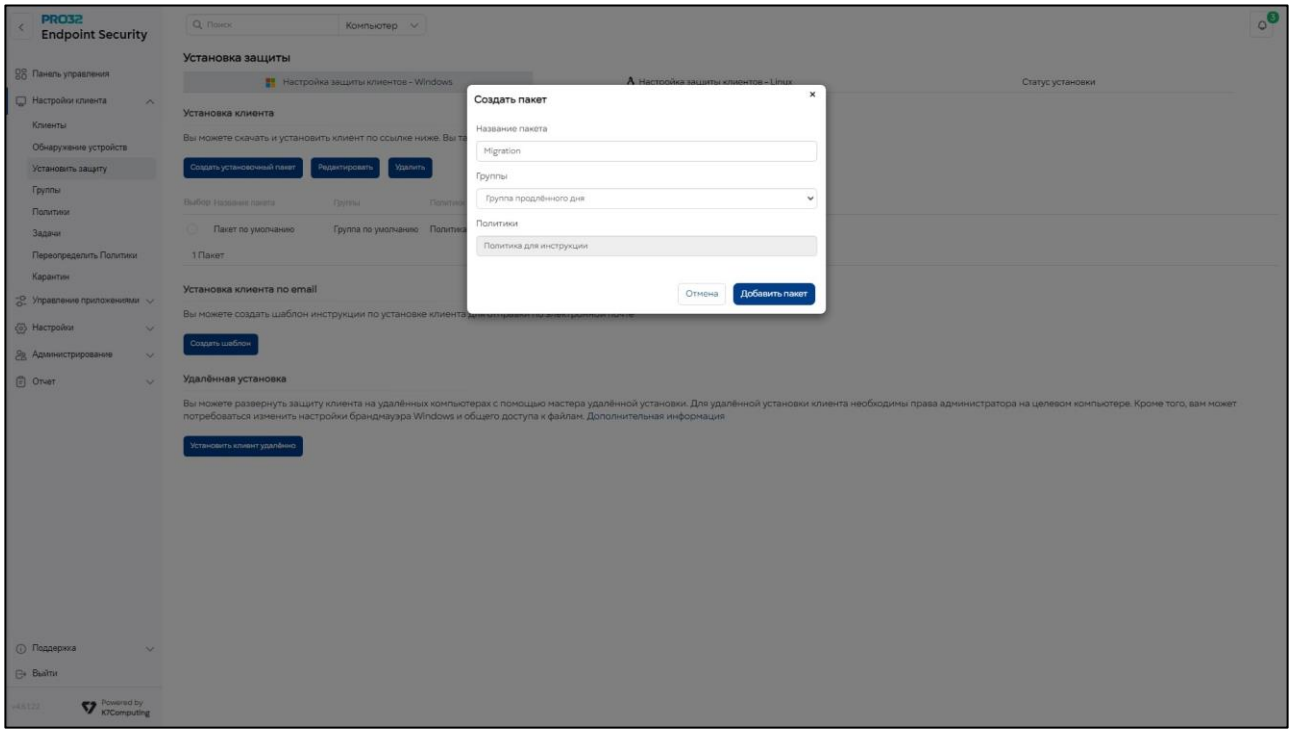
Полный отчет об аппаратных средствах можно экспортировать в различных форматах – текстовом, CSV, HTML, DOC и XLS.

32. Миграция на PRO32 Endpoint Security с ESET (средствами консоли ESET Protect)

1. Перейдите в **«Настройки клиента» → «Установить защиту»**

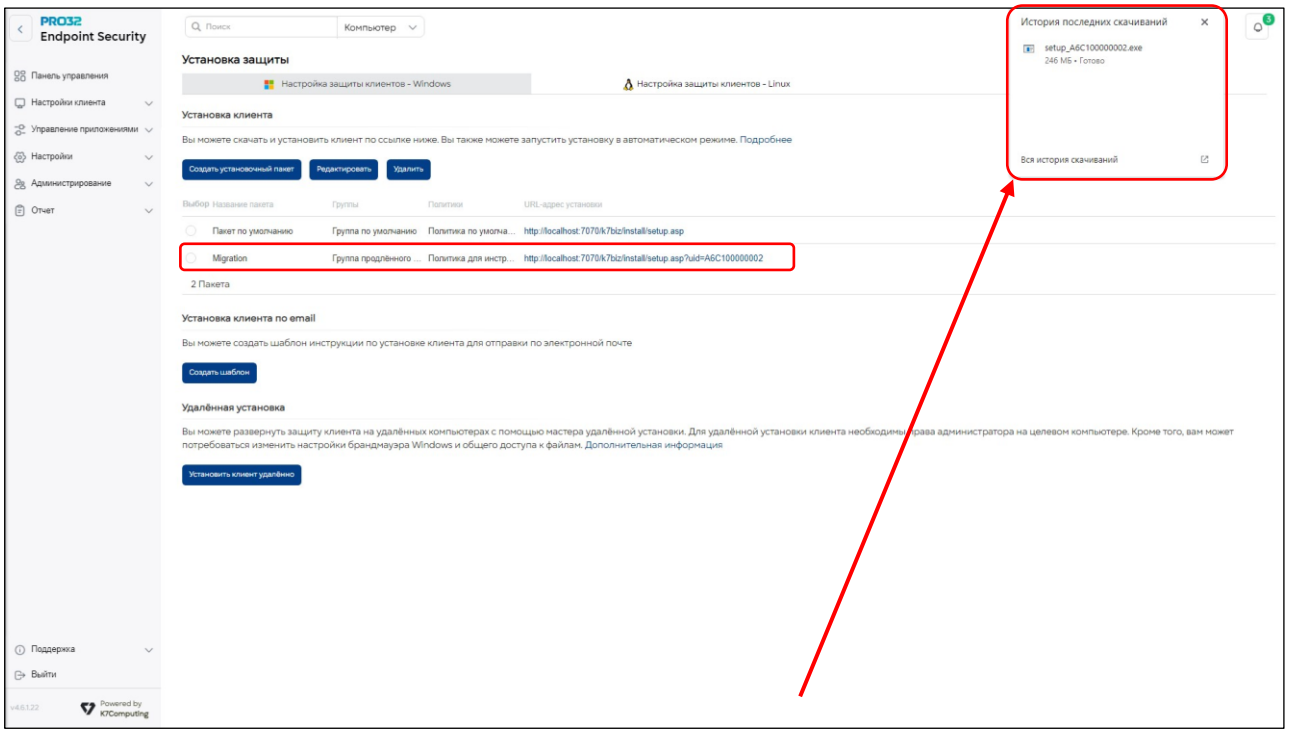


2. Нажмите **«Создать установочный пакет»**

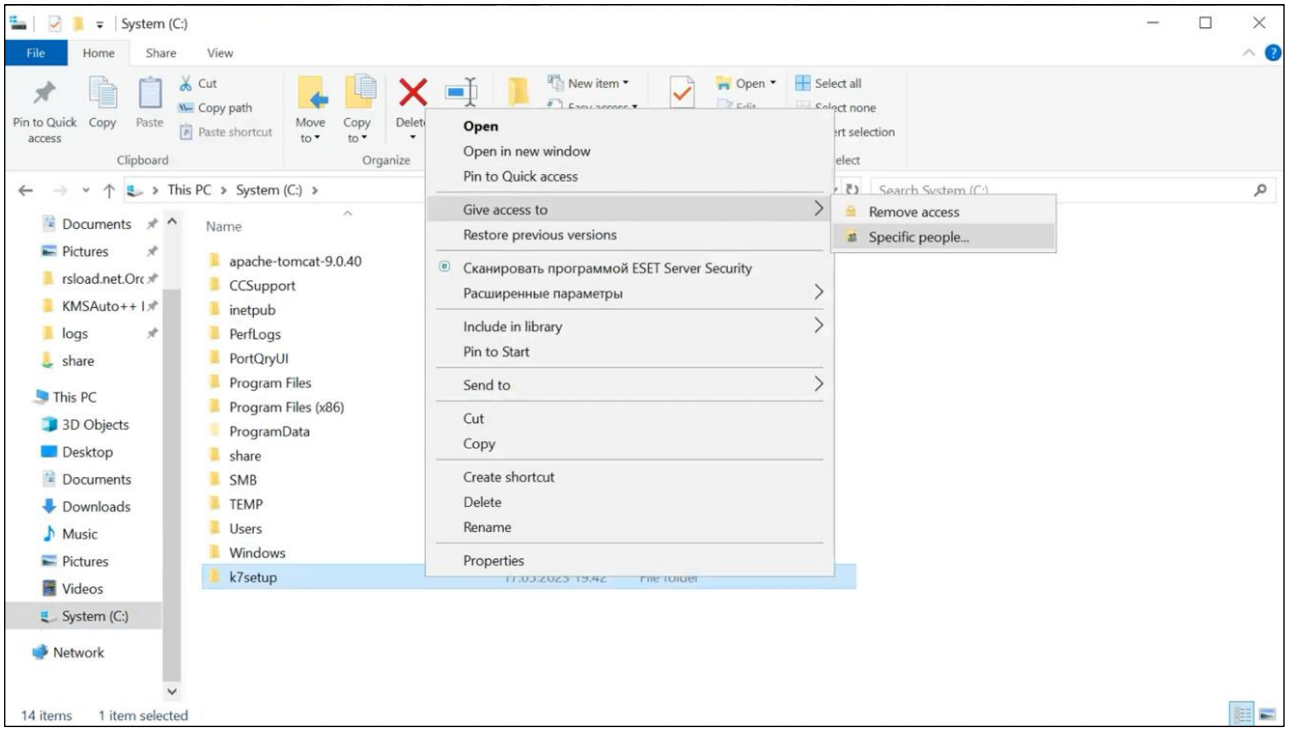


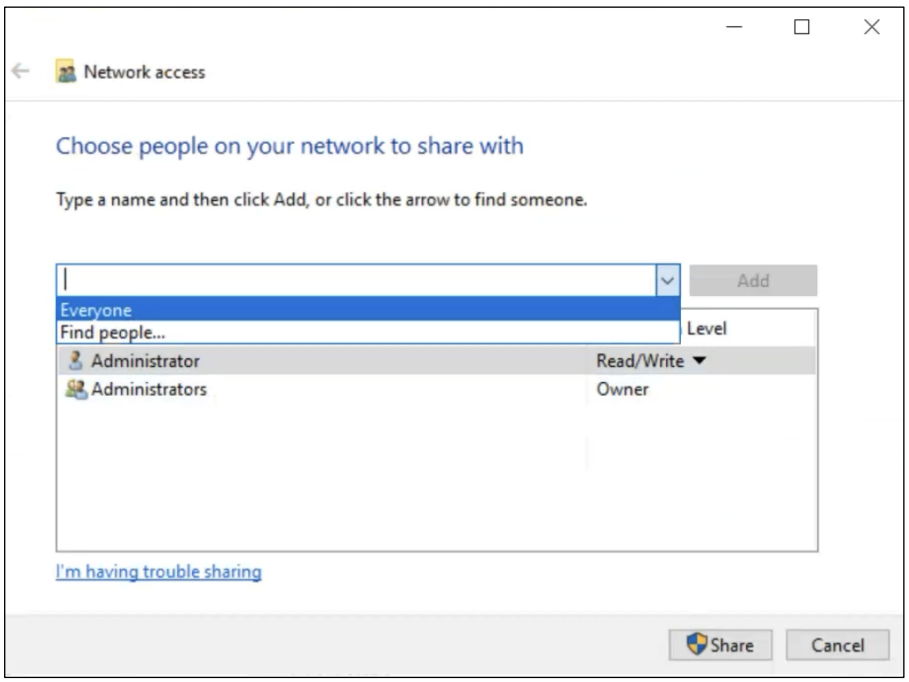
3. Укажите название пакета, группу и применяемую политику

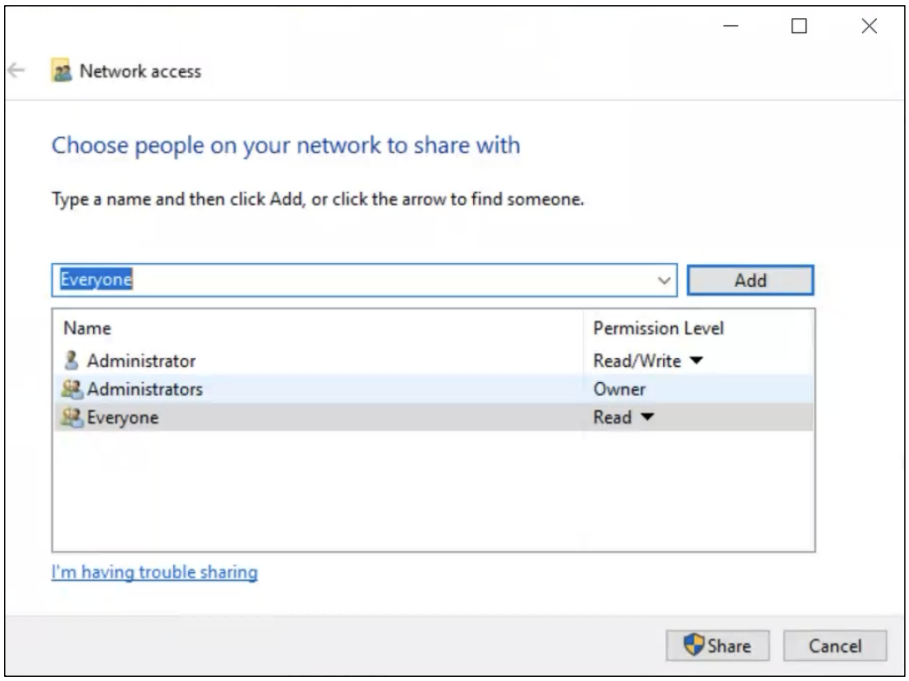
4. Скачайте установочный пакет по ссылке:

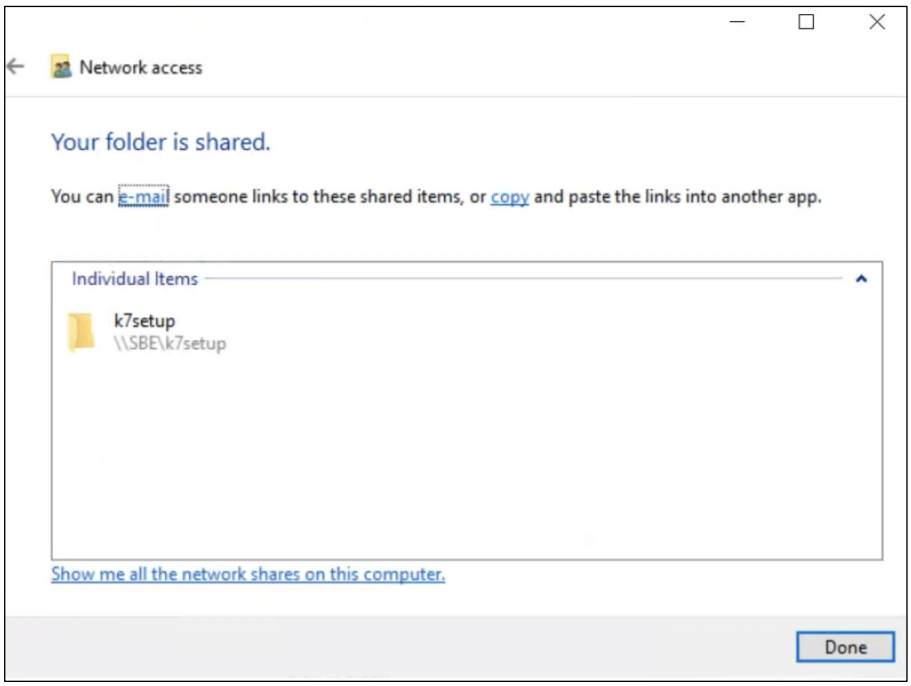


5. Создайте сетевой ресурс

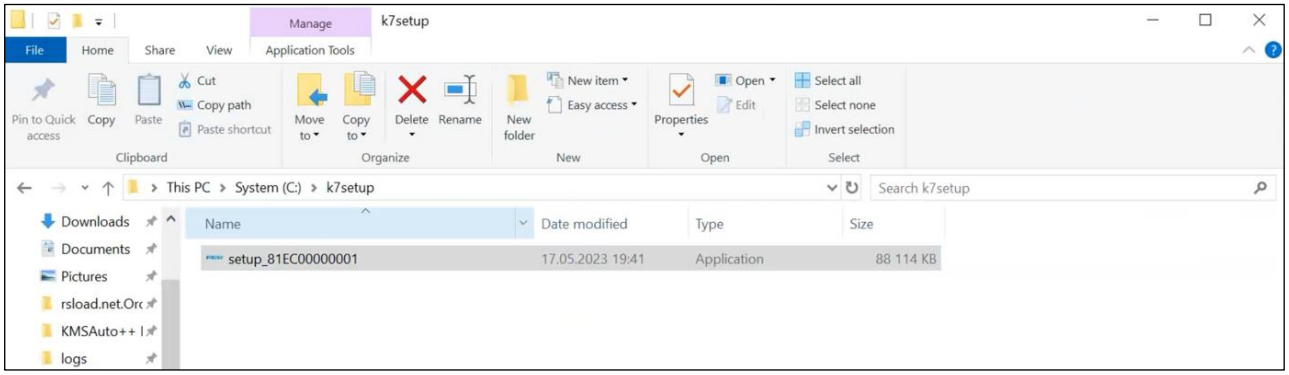



Network access
Choose people on your network to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Everyone
Find people...
Level
Administrator
Read/Write
Administrators
Owner
I'm having trouble sharing
Share
Cancel

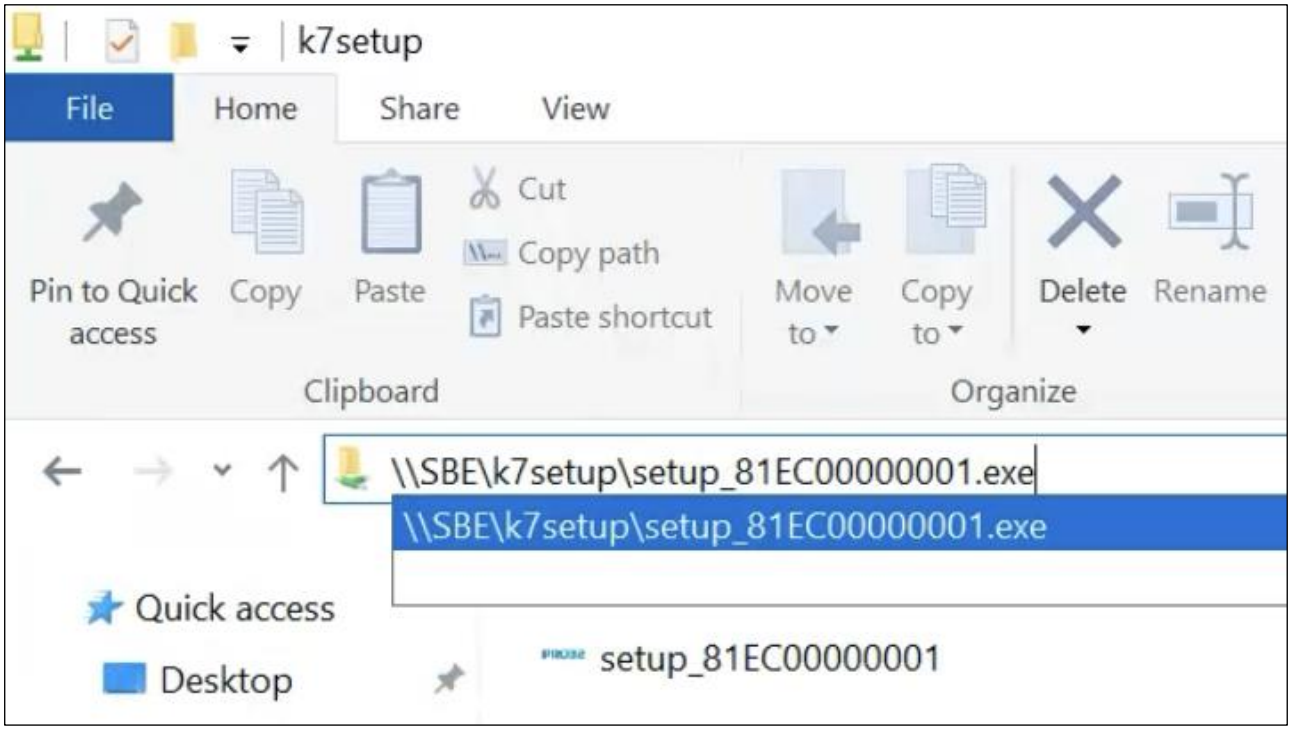

Network access
Choose people on your network to share with
Type a name and then click Add, or click the arrow to find someone.
Everyone
Add
Name
Permission Level
Administrator
Read/Write
Administrators
Owner
Everyone
Read
I'm having trouble sharing
Share
Cancel


Network access
Your folder is shared.
You can e-mail someone links to these shared items, or copy and paste the links into another app.
Individual Items
k7setup
\\SBE\k7setup
Show me all the network shares on this computer.
Done

6. Поместите в сетевой ресурс загруженный ранее *exe файл установочного пакета

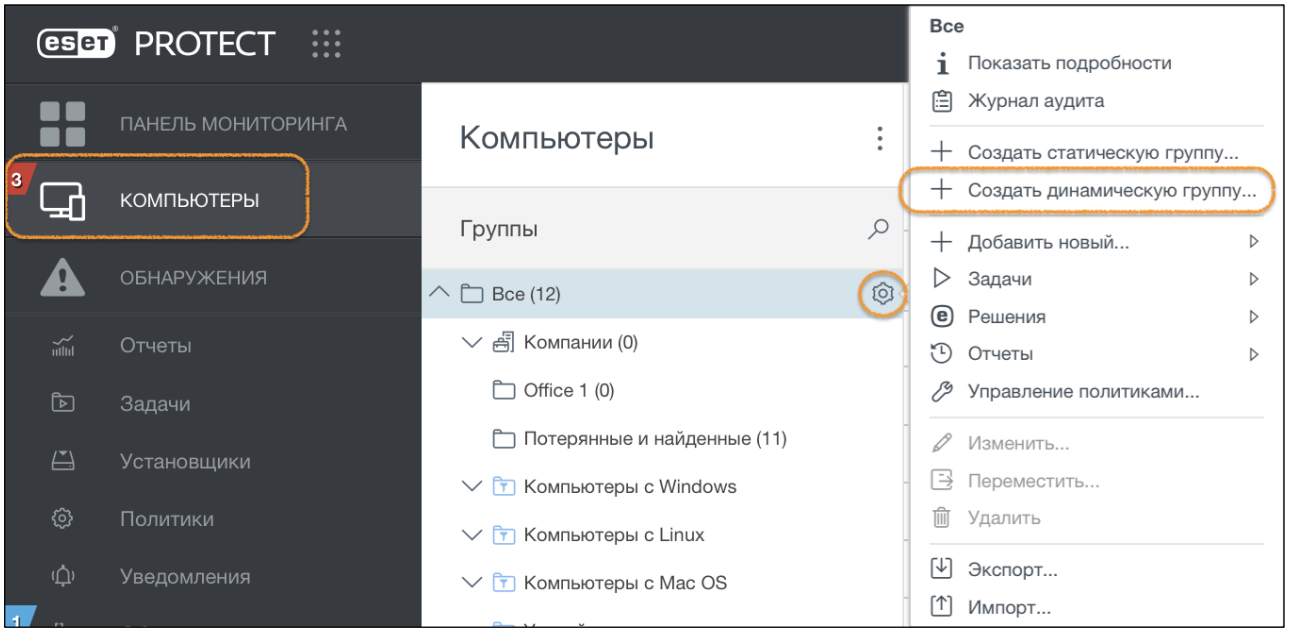


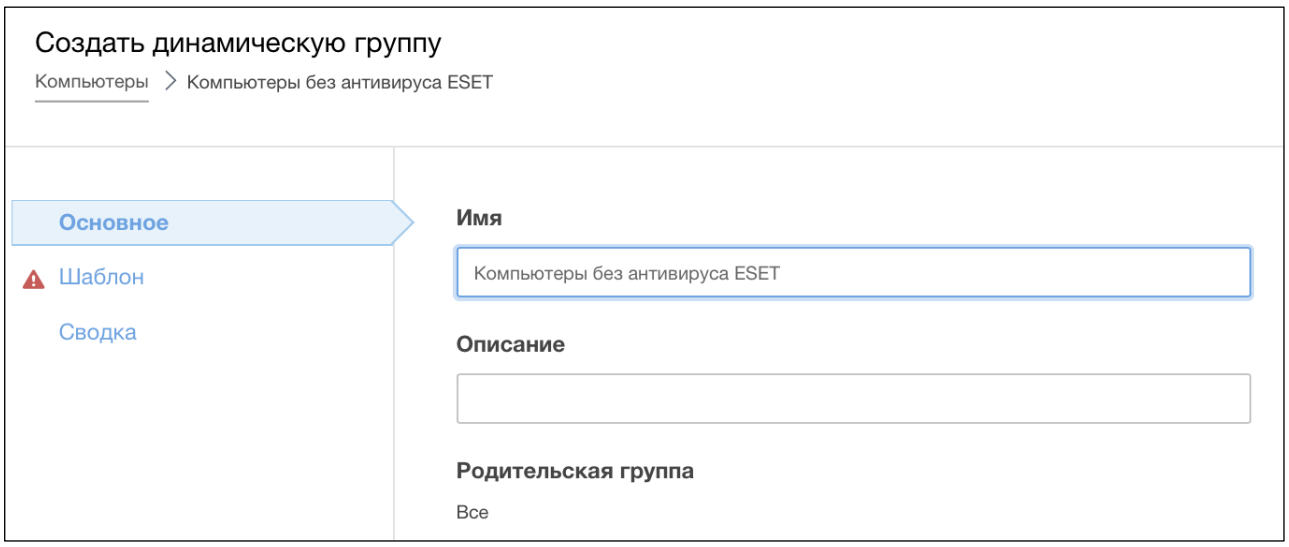
7. Проверьте доступность сетевого ресурса и скопируйте полный адрес до исполняемого файла, он будет необходим далее.



8. Перейдите в консоль ESET Protect, создаейте новую динамическую группу.

В качестве альтернативы динамической группе + задаче, можно вручную запустить задачу установки PRO32 с ручной выборкой устройств или групп, а не с автоматической по шаблону (в случае динамической группы + задачи). В этом случае не создаем динамическую группу.

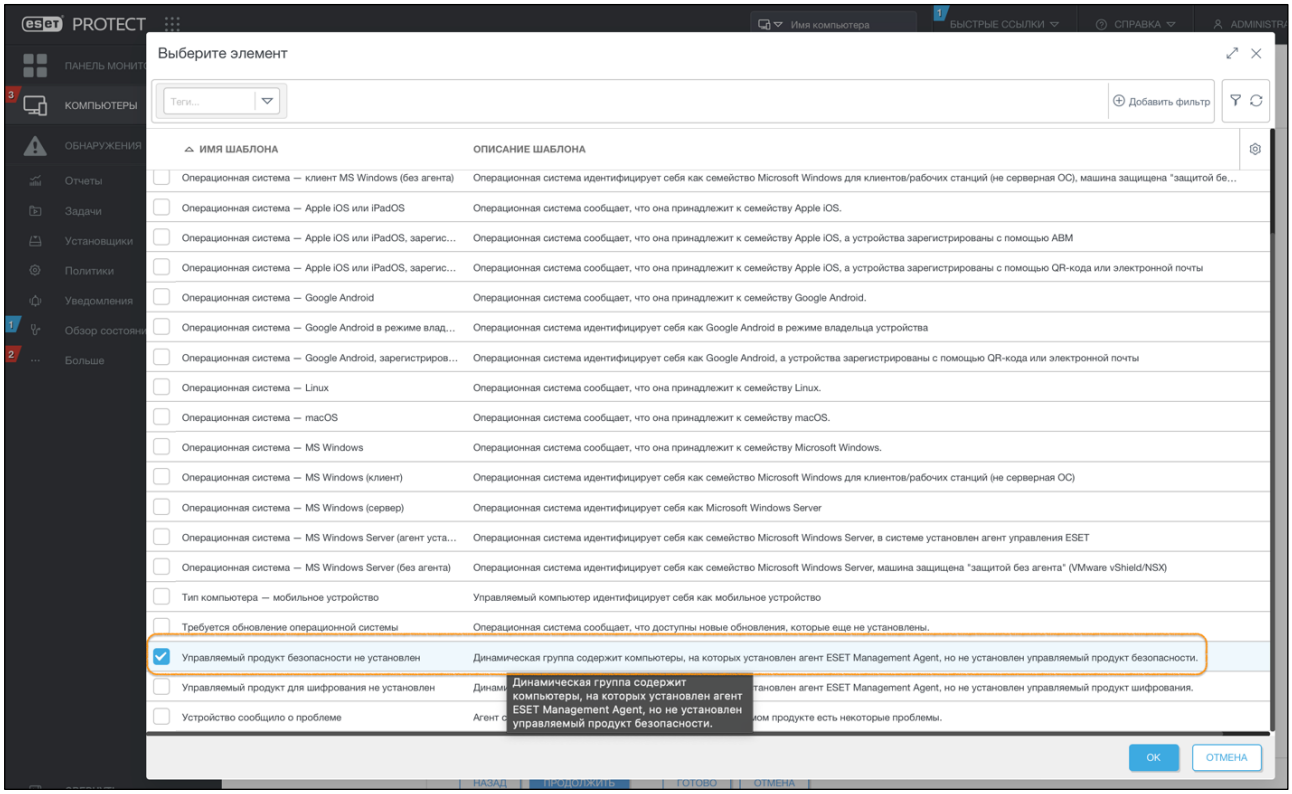




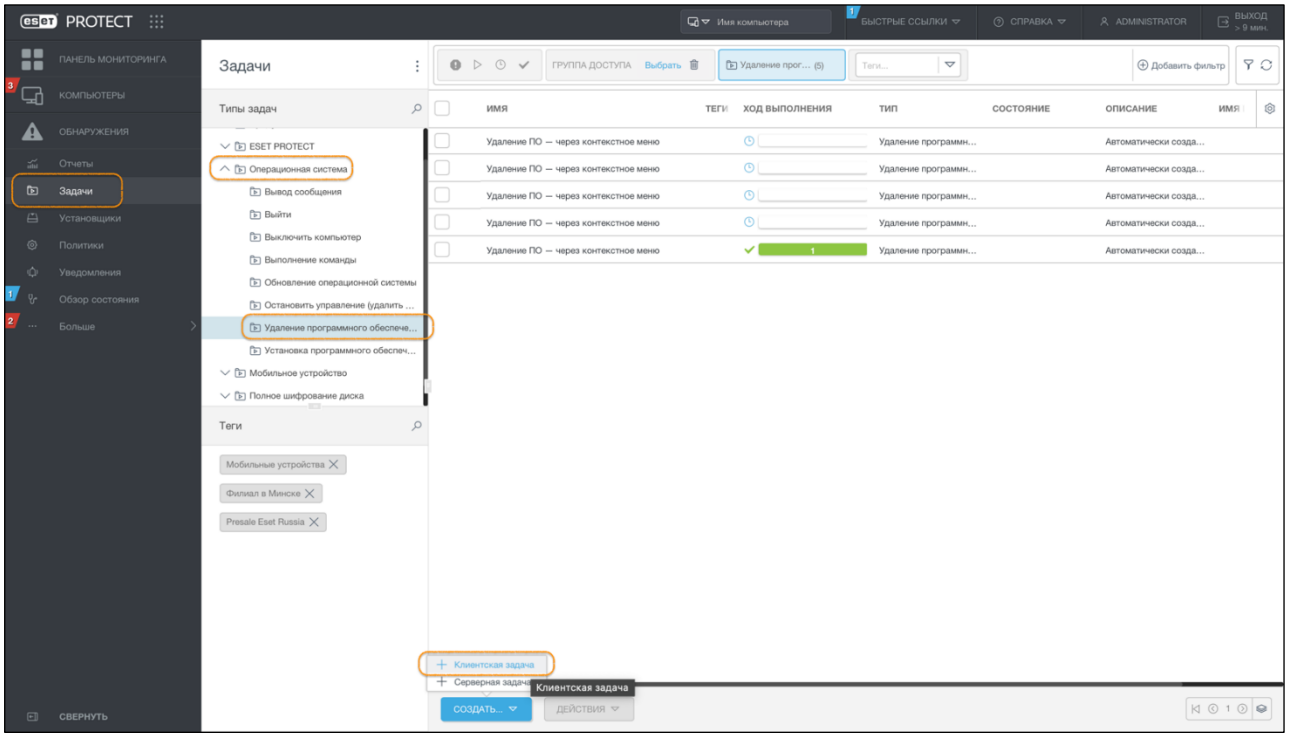
9. В качестве шаблона выбираем **«Управляемый продукт безопасности не установлен»**

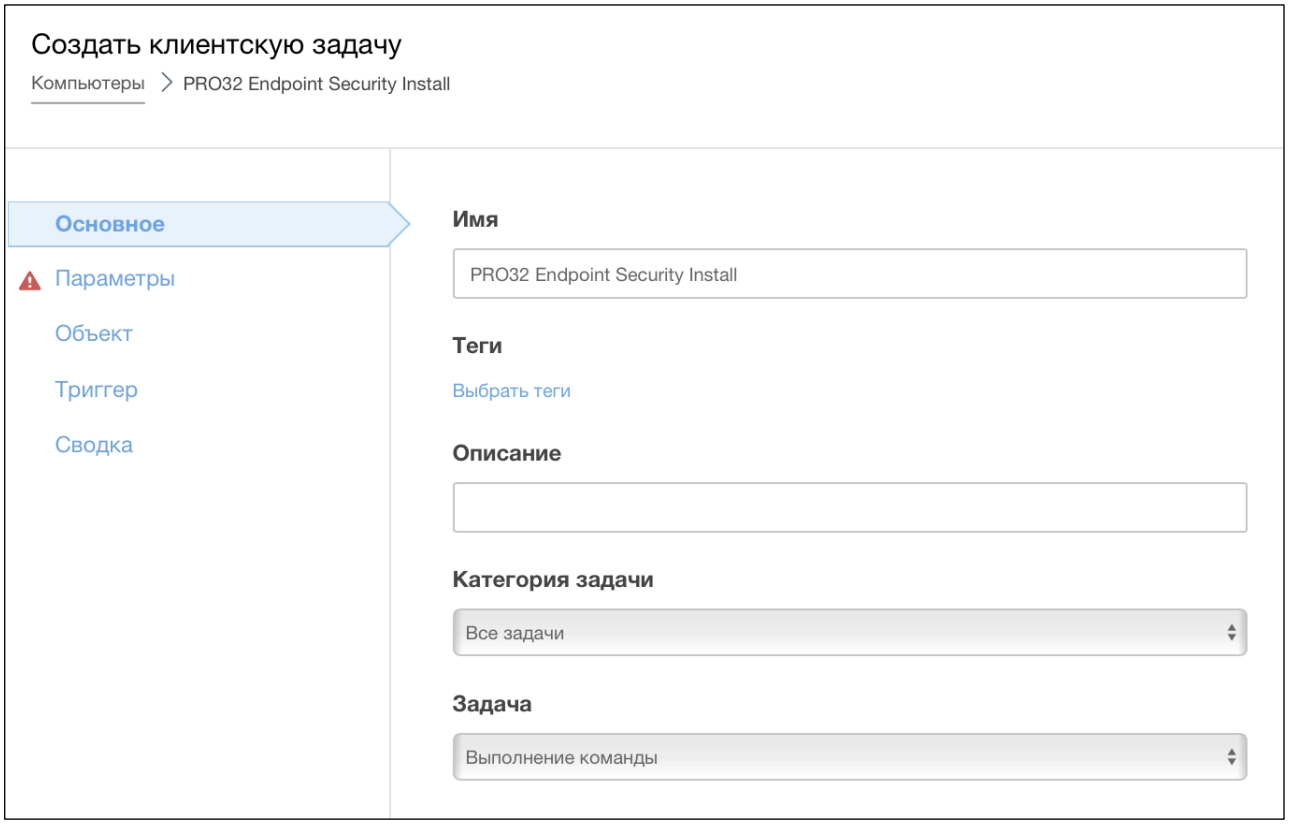
По данному шаблону в группу будут помещаться все управляемые агентом ESET Protect устройства, на которых не установлен (или удален) антивирус ESET Endpoint Antivirus, ESET Endpoint Security, ESET Server Security и другие антивирусы ESET;

ВАЖНО! Далее к динамической группе идет привязка выполнения задачи установки антивируса PRO32 Endpoint Security, если необходимо сделать какие-либо исключения компьютеров (чтобы они не попали в эту группу и не запустилась установка антивируса PRO32), в этом случае необходимо скорректировать шаблон **«Управляемый продукт безопасности не установлен»** под себя.



10. Создайте клиентскую задачу **«Выполнение команды»**





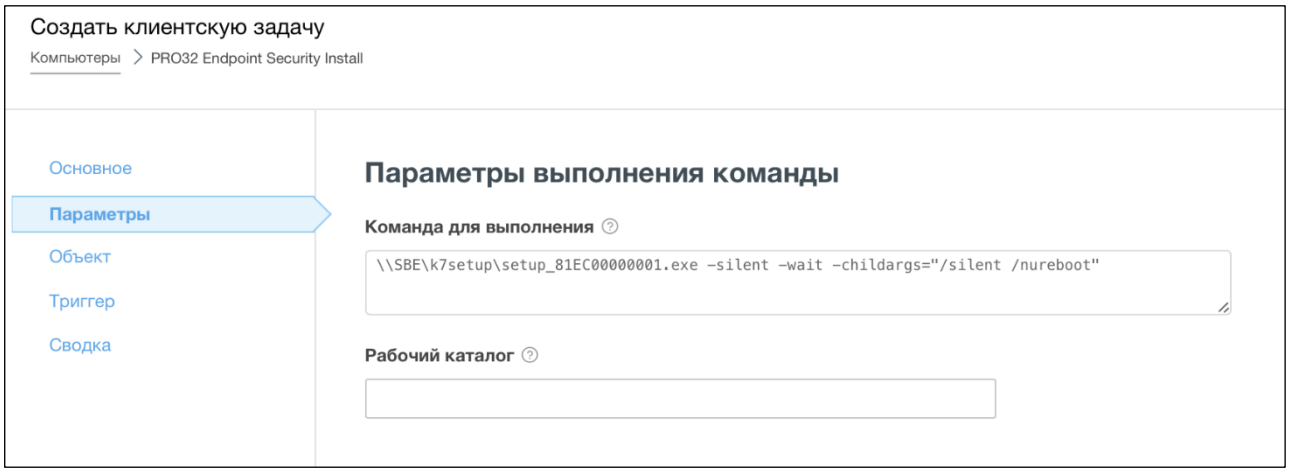
В параметрах указываем полный путь к исполняемому файлу установщика (пункт 6 инструкции):

На нашем примере: \\SBE\k7setup\setup_81EC00000001.exe

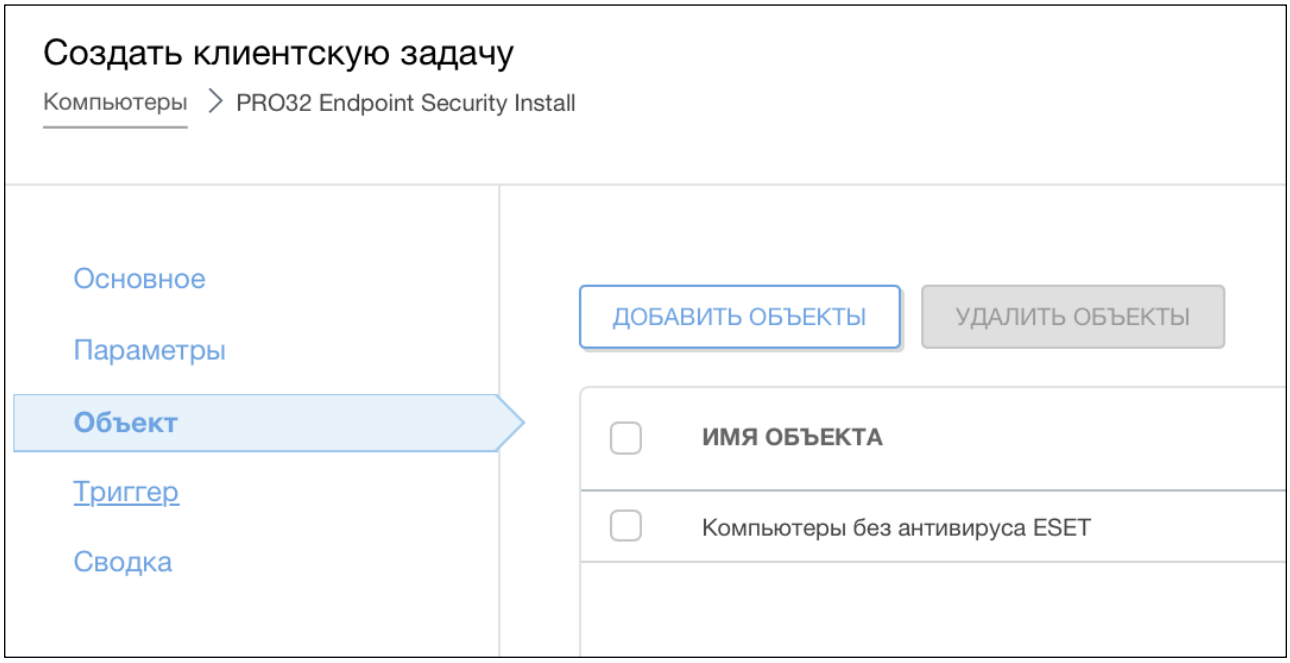
В качестве дополнительных параметров также указываем через пробел обязательные ключи установки:

-silent -wait -childargs="/silent /nureboot"

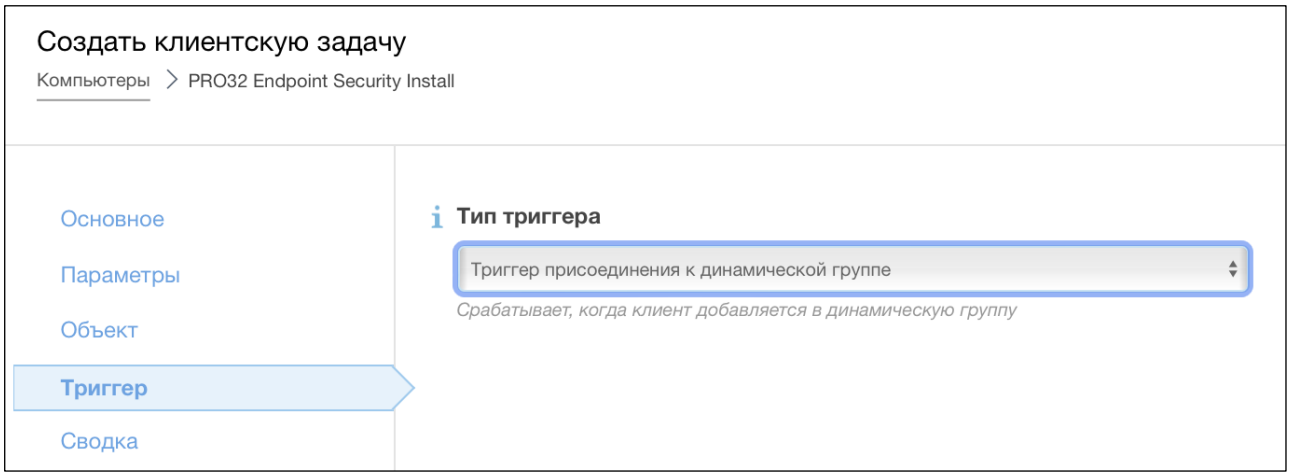
Итоговый результат:



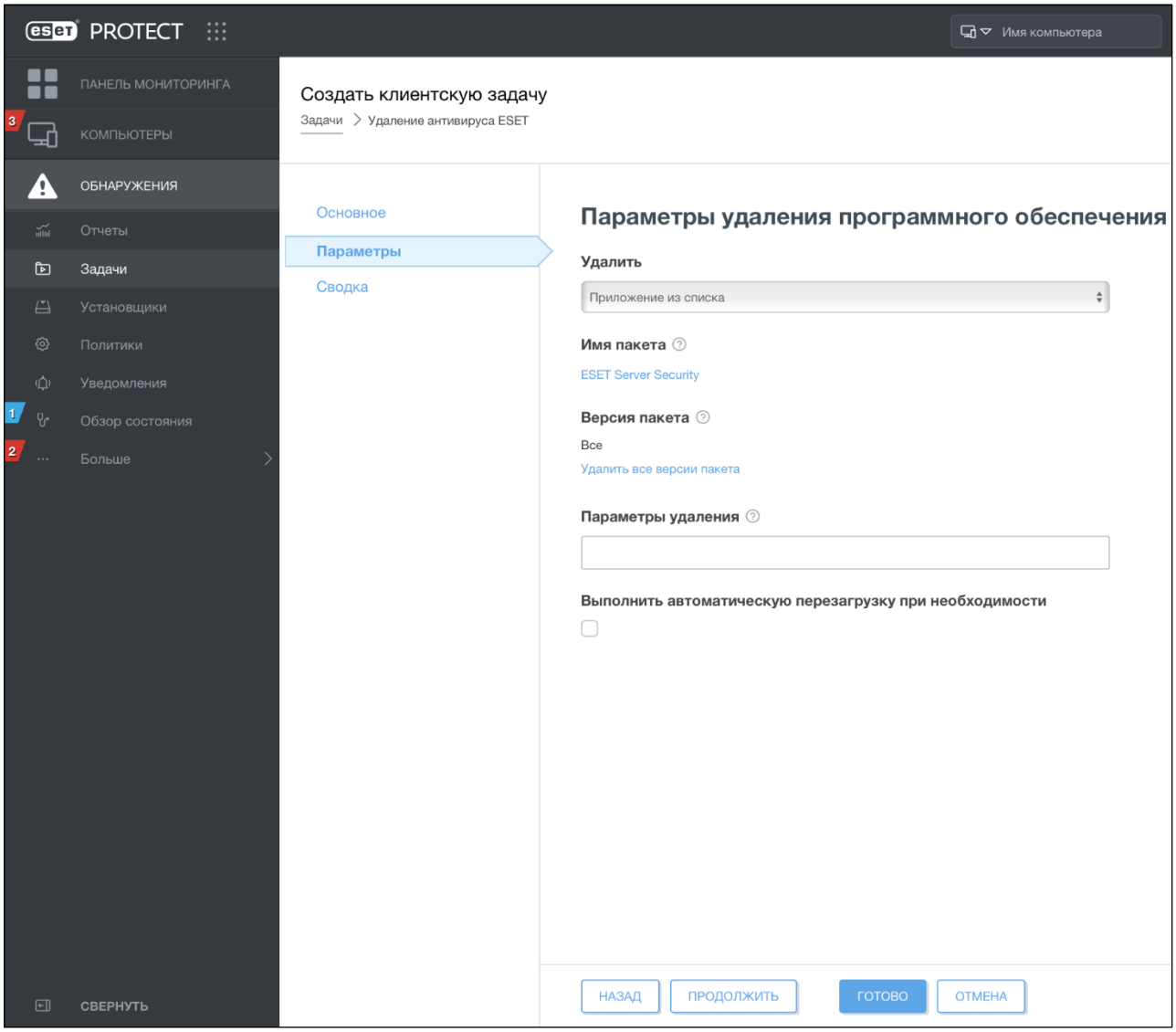
В качестве объекта указываем динамическую группу “Компьютеры без антивируса ESET”, созданную на ранее.



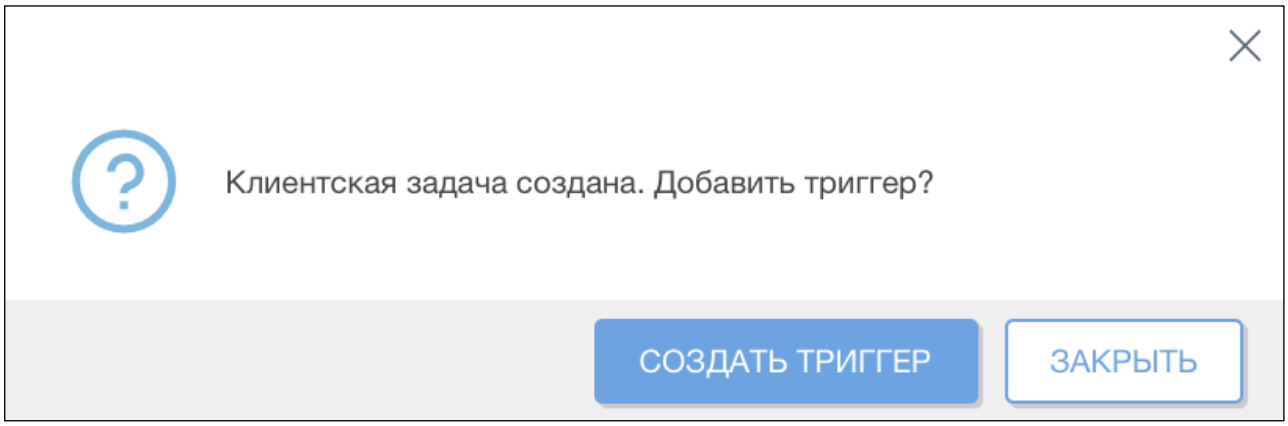
В качестве триггера (условия выполнения задачи) указываем «Триггер присоединения к динамической группе» **(задача будет выполнена на всех устройствах, находящихся в группе)**



11. Создайте клиентскую задачу **«Удаление программного обеспечения»,** в параметрах выбираем необходимые версии и приложения антивирусов ESET Endpoint Antivirus, ESET Endpoint Security, ESET Server Security и так далее, указываем все версии пакета (если на разных устройствах разные версии);



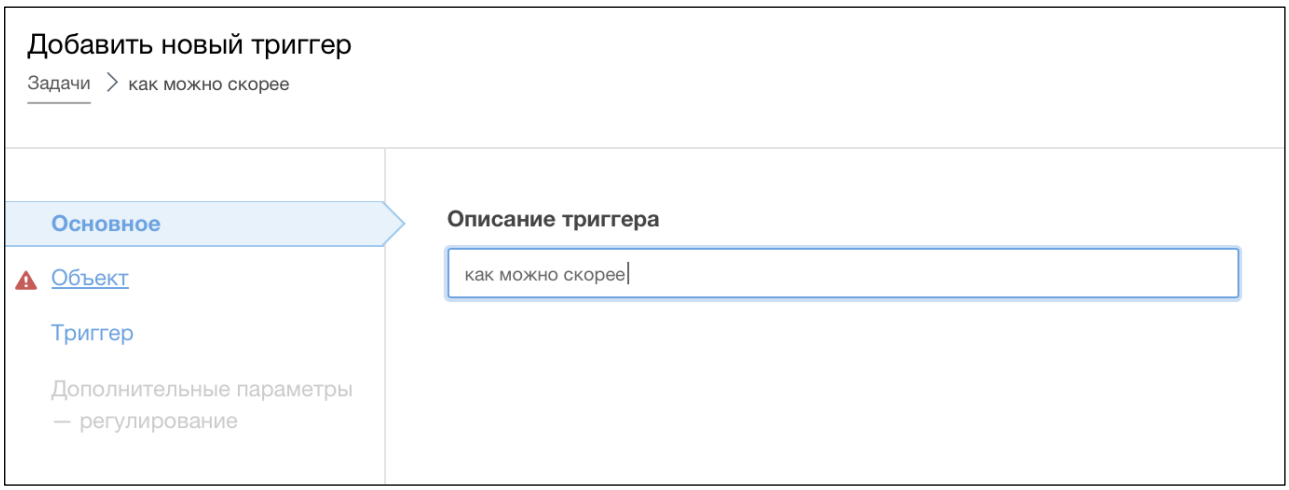
Подтвердите создание триггера старта задачи:

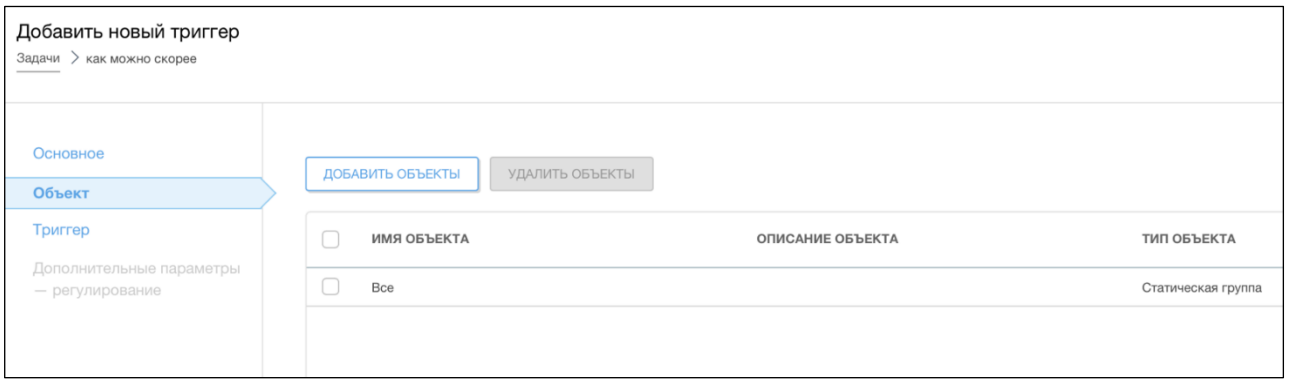


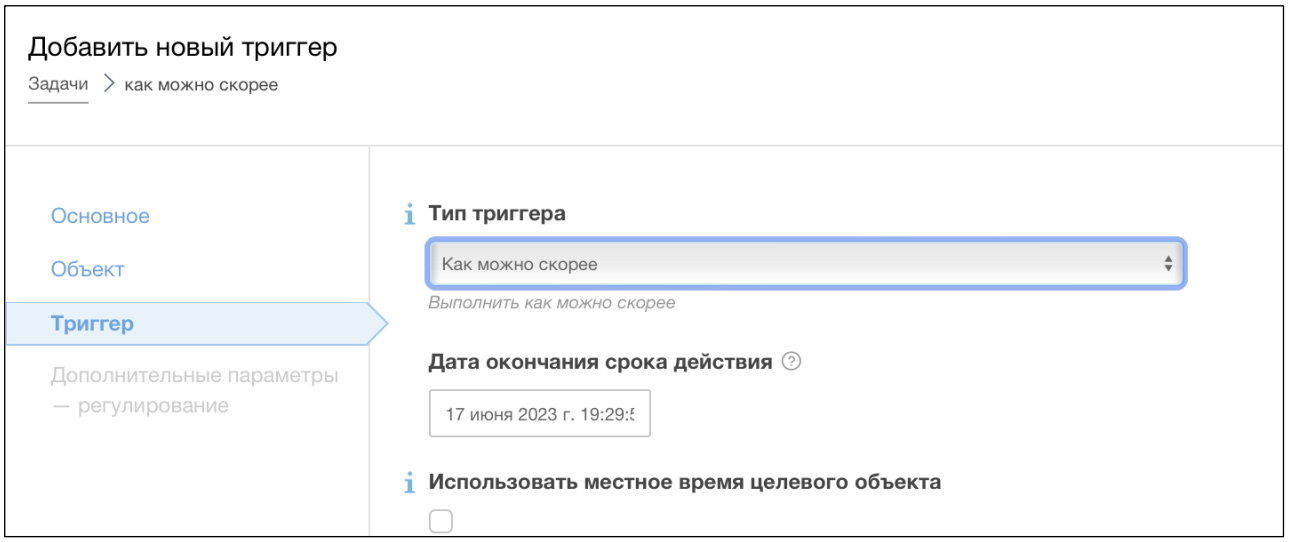
ВНИМАНИЕ: на примере ниже рассматривается запуск **«как можно скорее»,** после синхронизации задачи на агентах, она будет запущена **незамедлительно** и начнется удаление антивируса ESET.

Далее, после удаления антивируса ESET, устройства попадут в динамическую группу с шаблоном «Управляемый продукт безопасности не установлен», что активирует старт задачи «Выполнение команды», которая установит PRO32 Endpoint Security.

Рекомендуем для распределения нагрузки на устройства и на сеть предприятия, выполнять миграцию поэтапно (например, по группам устройств, начиная с тестовой группы), в нерабочие часы или дни, чтобы это не сказывалось на рабочих процессах предприятия.

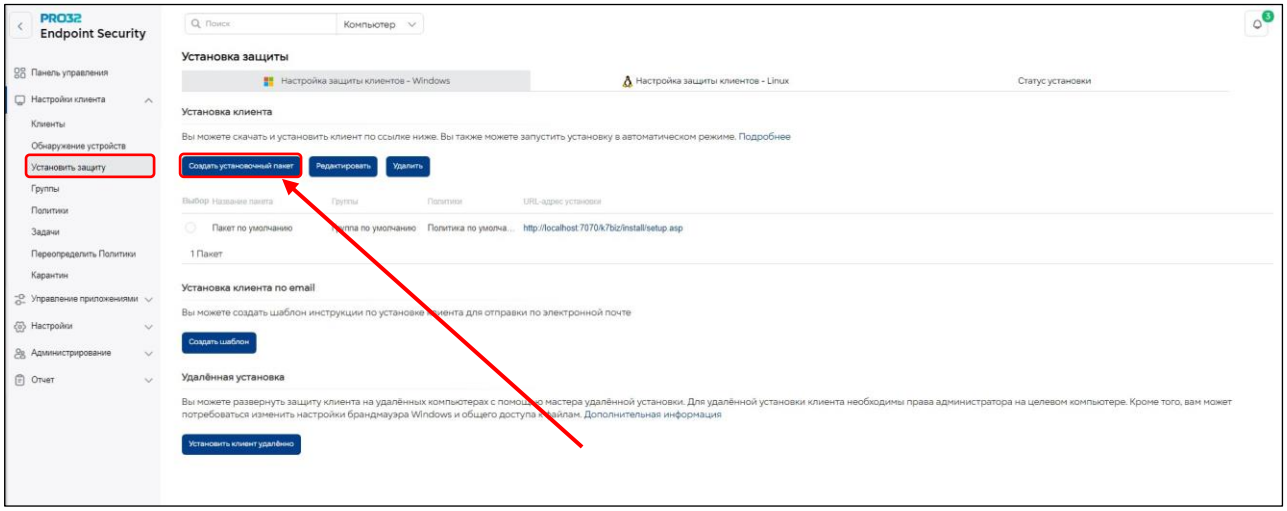

Добавить новый триггер
Задачи > как можно скорее
Основное
Объект
Триггер
Дополнительные параметры — регулирование
Описание триггера
как можно скорее


Добавить новый триггер
Задачи > как можно скорее
Основное
Объект
Триггер
Дополнительные параметры — регулирование
ДОБАВИТЬ ОБЪЕКТЫ
УДАЛИТЬ ОБЪЕКТЫ
ИМЯ ОБЪЕКТА
ОПИСАНИЕ ОБЪЕКТА
ТИП ОБЪЕКТА
Все
Статическая группа

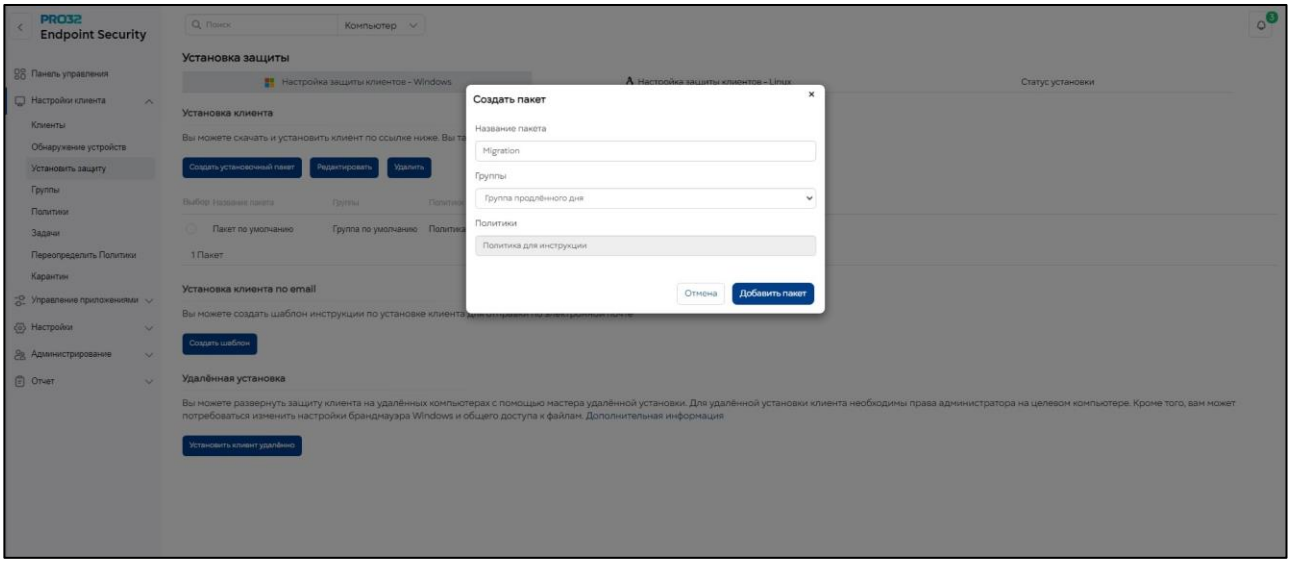

Добавить новый триггер
Задачи > как можно скорее
Основное
Объект
Триггер
Дополнительные параметры — регулирование
Тип триггера
Как можно скорее
Выполнить как можно скорее
Дата окончания срока действия
17 июня 2023 г. 19:29:
Использовать местное время целевого объекта

33. Миграция на PRO32 Endpoint Security с Kaspersky Endpoint Security

1. Перейдите в **«Настройки клиента» → «Установить защиту»**

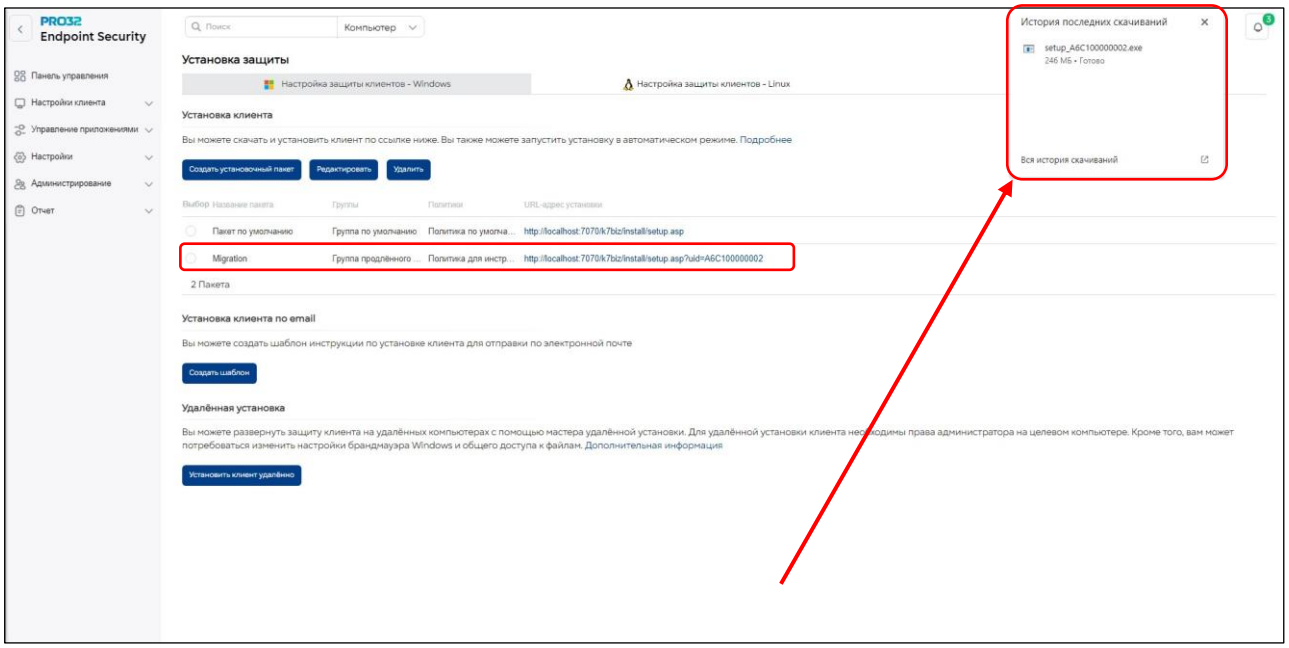


2. Нажмите **«Создать установочный пакет»**



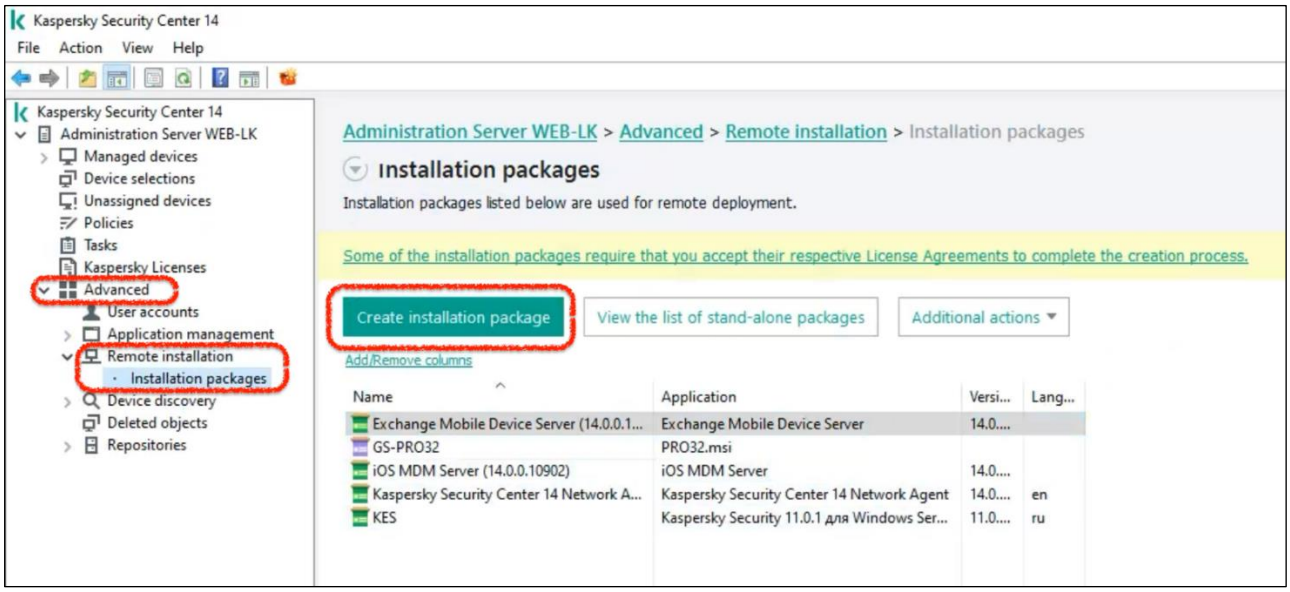
3. Укажите название пакета, группу и применяемую политику

4. Скачайте установочный пакет по ссылке:

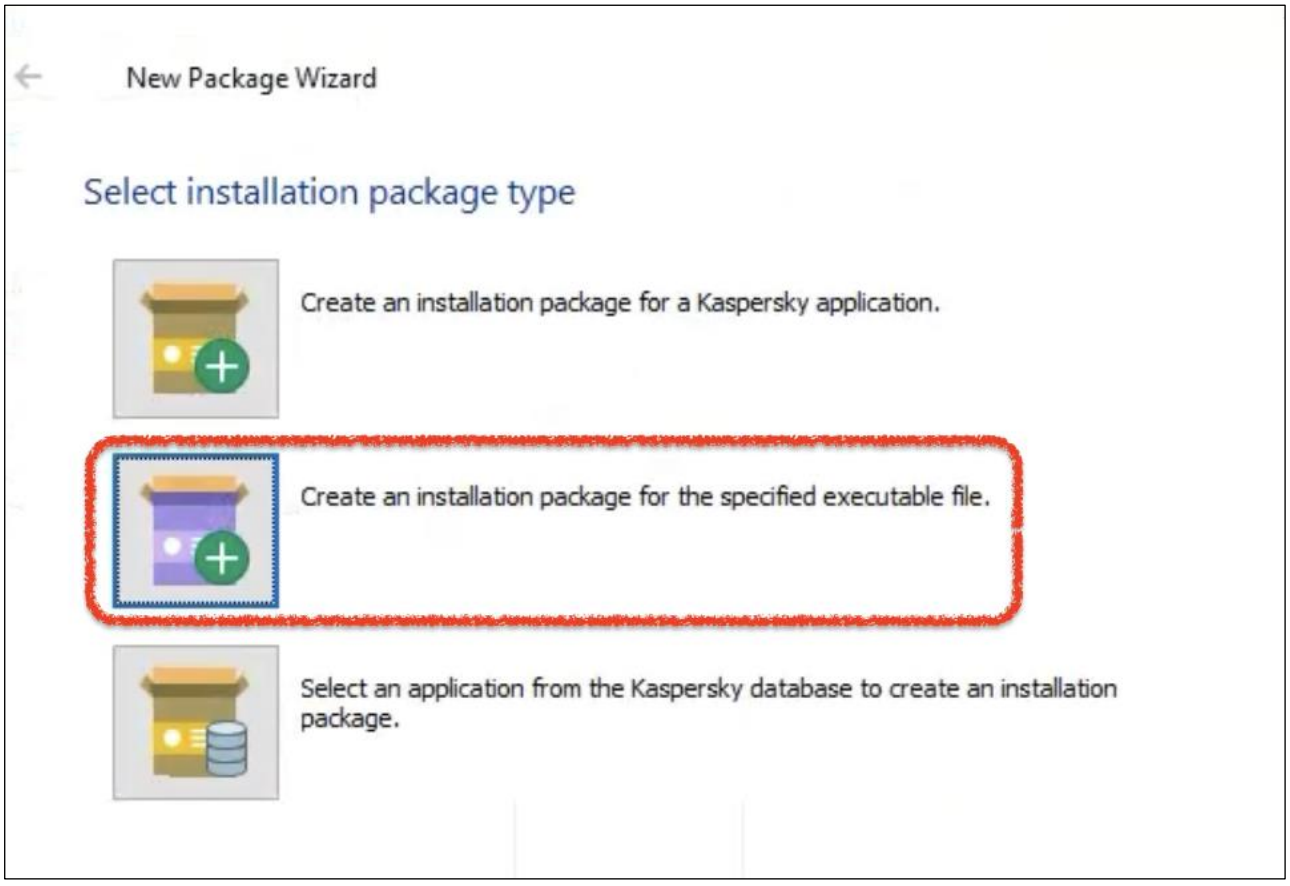


5. В консоли KSC добавляем новый инсталляционный пакет и запускаем на установку

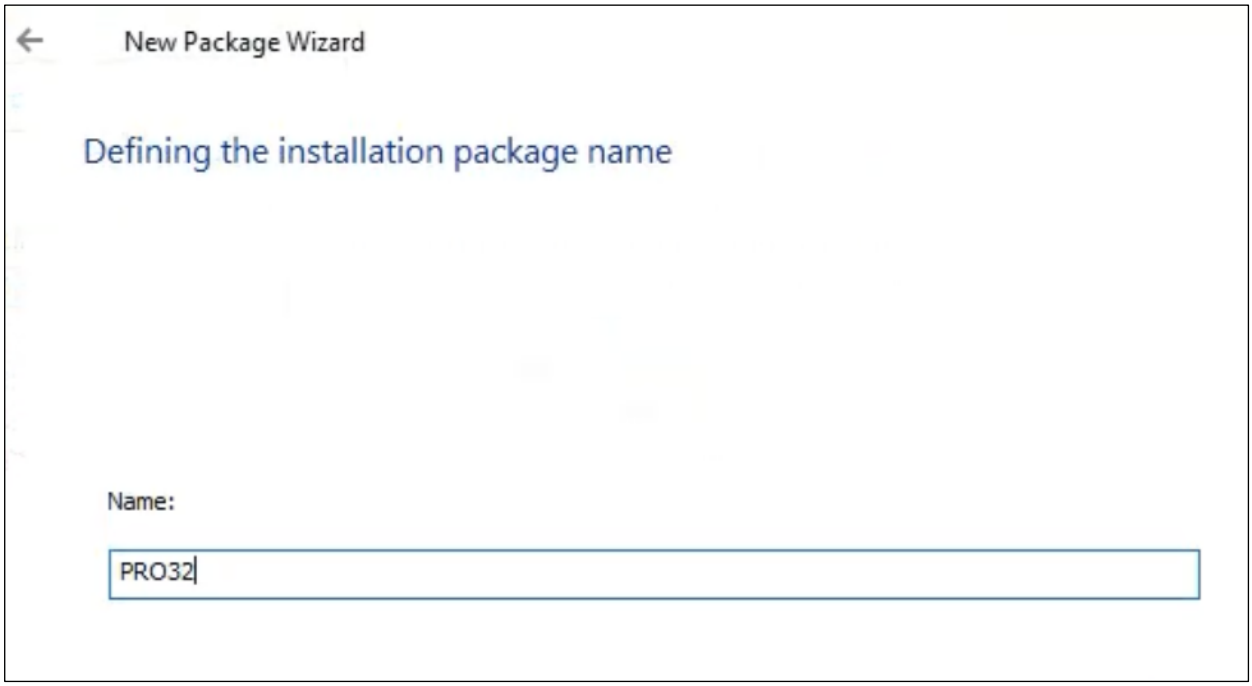
Создать установочный пакет



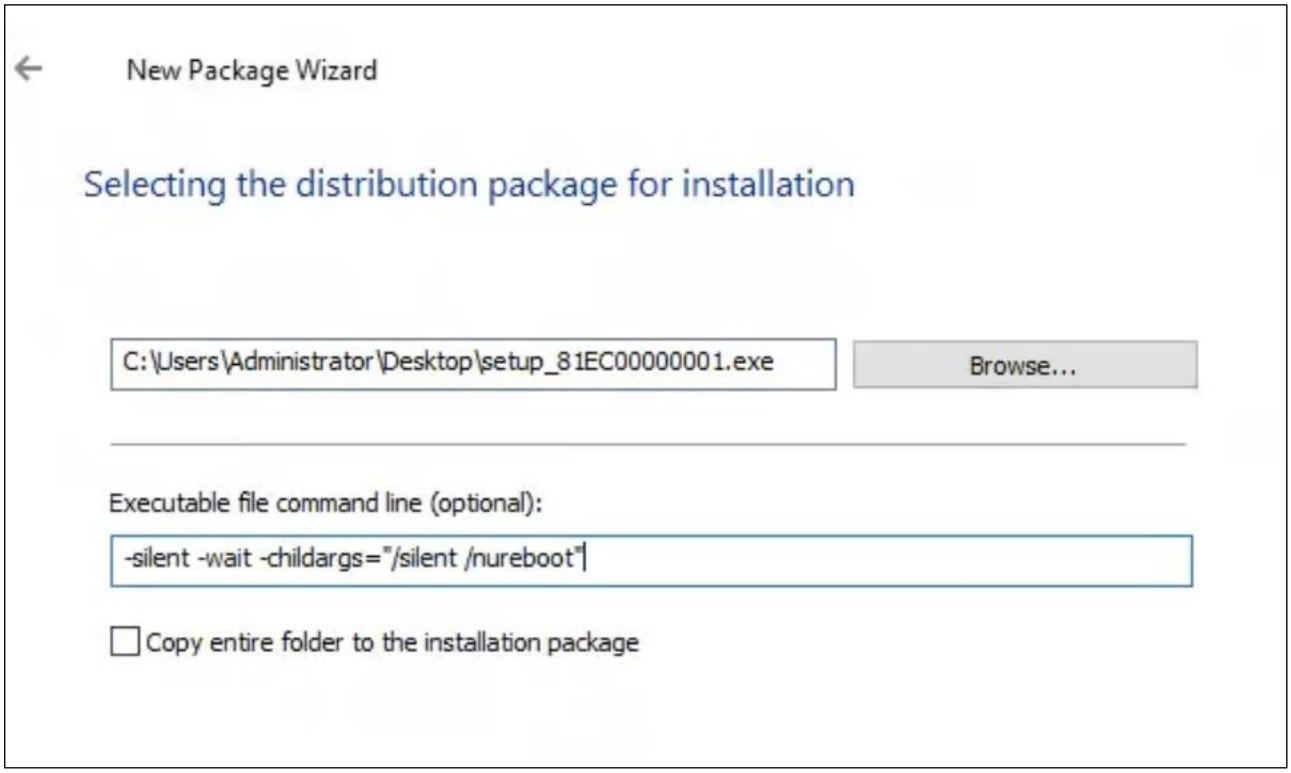
Создать пакет для определенного исполняемого файла – пункт 2



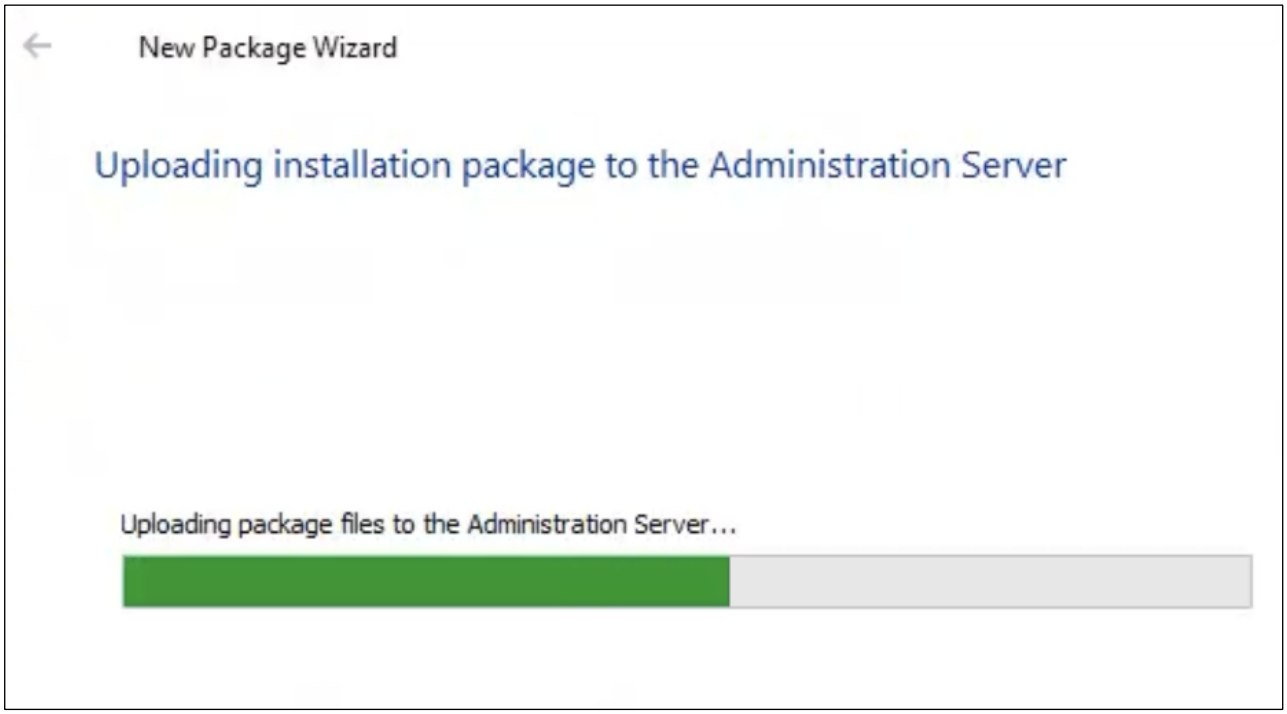
Укажите имя пакета



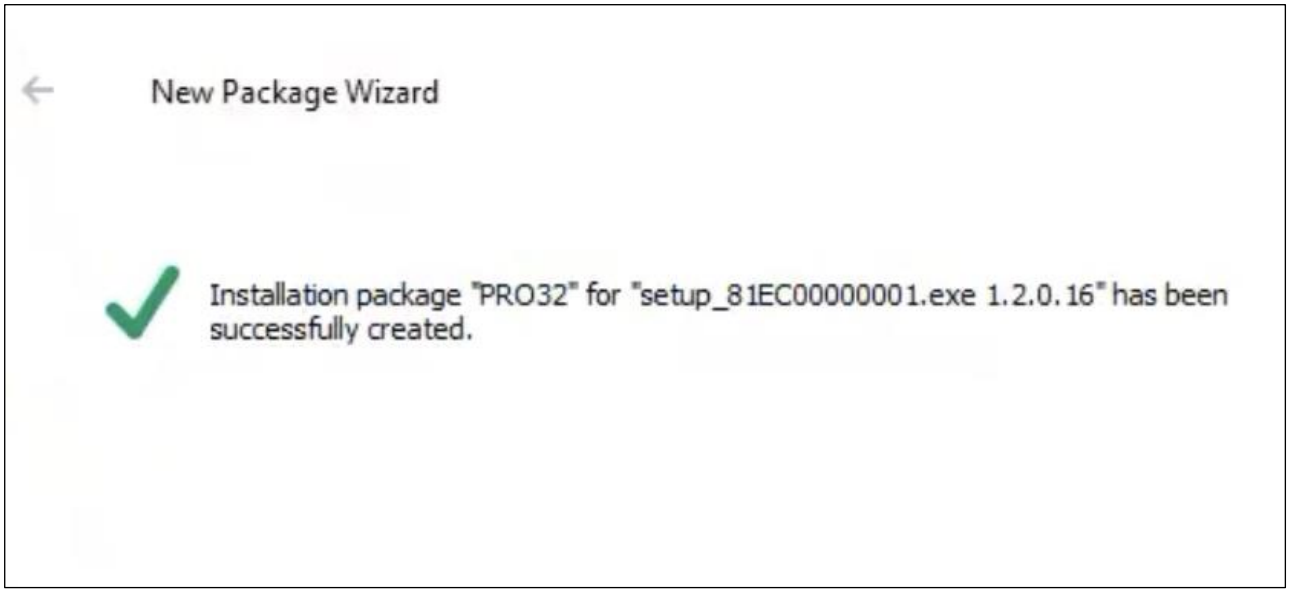
Обязательно добавьте параметры установки: **-silent -wait -childargs="/silent /nureboot"**



Дождитесь окончания загрузки пакета



Закройте окно мастера пакетов



Из списка пакетов выберите PRO32 и запустите создание задачи установки ПО