

PRO32

PRO32
ENDPOINT SECURITY

Руководство администратора

Оглавление

О консоли администрирования	5
Что нового	5
Информационная панель	5
Установка PRO32 Endpoint Security	5
Подготовка к удаленной установке PRO32 Endpoint Client	6
Удаленная установка PRO32 Endpoint Client	7
Статус удаленной установки	8
Экспорт результатов установки на клиентские компьютеры	9
Отправьте запрос в службу поддержки из веб-консоли	10
Политики	11
Политика по умолчанию	11
Как создать новую политику	11
Редактирование политики	12
Удаление политики	13
Копирование существующей политики для создания новой	13
Включение AMSI-защиты в политике	13
Группы	14
Создание группы	14
Редактирование группы	15
Удаление группы	15
Изменение группы по умолчанию	16
Управление клиентами	16
Столбец IP-адресов в списке клиентов и отчетах	18
Просмотр событий изменения статуса антивируса и брандмауэра	20
Добавление дополнительных полей на страницу «Управление клиентами»	21
Смена группы	22
Управление задачами	23
Добавление новой задачи	24
Статусы задач	24

Удаление задачи	24
Обновление статусов задач	24
Переопределяющая политика	24
Включение AMSI-защиты в переопределяющей политике	26
Карантин	27
Управление приложениями	28
Просмотр списка приложений	28
Заблокировать приложения со страницы списка приложений	29
Правила блокировки приложений	29
Настройки	30
Уведомления	30
Псевдоним отправителя электронного письма	31
Тестирование получения уведомлений по электронной почте	31
Настройка получения по электронной почте уведомлений о событиях	31
Уведомления о не зарегистрированных устройствах	32
Обнаружение местоположения	34
Настройки прокси	34
Обновления	35
Управление данными	35
Добавление дополнительных полей на страницу «Настройки клиента»	35
Веб-категории	36
Лицензии	36
Администрирование	36
Роли	36
Пользователи	37
Создание пользователя	38
Суперадминистратор	38
Администратор группы	39
Настройки сеанса	39

Настройка параметров пароля для входа в консоль	39
Настройка параметров пароля	40
Вход	40
Сводка по событиям на информационной панели	41
Меню в заголовке главной страницы	41
Изменение логотипа	42
Отчеты	42
Краткий отчет	42
Создание кратких отчетов по сканированию	43
Создание краткого отчета: тип отчета – сканирование	43
Подробный отчет	45
Создание подробных отчетов по сканированию	46
Создание отчетов по журналу изменений состава аппаратных средств	47
Экспорт полного отчета по аппаратным средствам в различных форматах	49
Шаблон отчета	49
Экспорт всех видов отчетов в различных форматах	50

О консоли 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.

Что нового

Добавлена функция «Интерфейс сканирования для защиты от вредоносного ПО» (AMSI) для защиты конечных точек от бесфайловых угроз. Эта функция применима для конечных точек с операционными системами Windows 10, Windows Server 2016 или более поздними.

Информационная панель

Информационная панель – это главная консоль, 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.

Установка PRO32 Endpoint Security

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

Начальная страница → Управление клиентами

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.

Подготовка к удаленной установке PRO32 Endpoint Client

Развертывание PRO32 Endpoint Client на клиентских компьютерах – несложный процесс благодаря мастеру удаленной установки. Для удаленной установки PRO32 Endpoint Client у вас должны быть 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.

Удаленная установка PRO32 Endpoint Client

После выполнения указанных выше подготовительных шагов развертывание PRO32 Endpoint Client 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.

Install Protection

To install K7 Protection, select the installation method from below

Specific Computer Using Active Directory Using Workgroup Using IP Range

Computer Name / IP Address

Enter Computer name or IP Address

Attention!

Microsoft Windows is configured to block all the remote access by default.

For a successful remote installation, you have to change the Windows Firewall and File Sharing settings on the target computers.

[View Instructions](#)

Cancel Next

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

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

Install Protection

Enter Administrator Credentials

Domain

Username

Password

Select Group

Group

Choose Installation Options

When Reboot required Reboot Automatically Prompt User

Back Cancel Finish

5. Укажите группу, которую вы хотите применить к выбранным компьютерам, и способ перезагрузки компьютера при установке.

6. Нажмите «Готово».

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**):

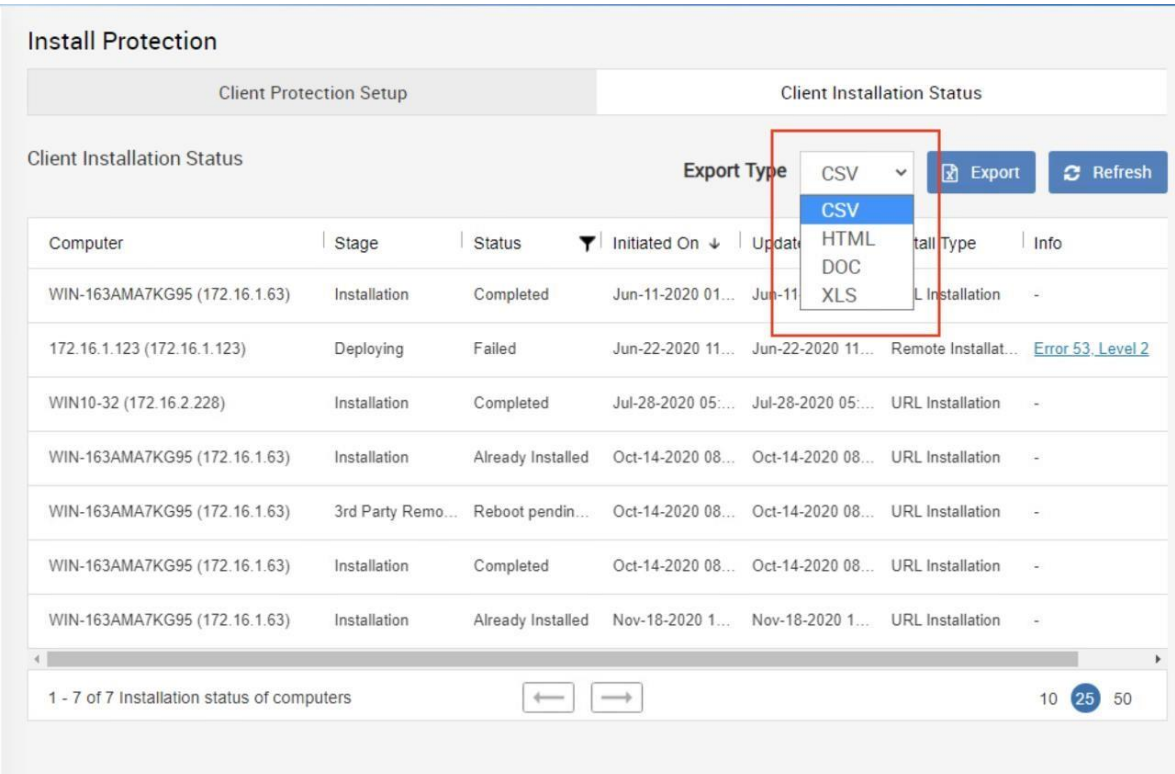
- Имя / IP-адрес компьютера
- Этап установки (удаленная push-установка, установка, удаление сторонних продуктов, уже установлено и т. д.)
- Статус установки (распределена, инициализирована, сбой, успешно начата, ожидание перезагрузки пользователем, успешно завершена и т. д.)
- Дата и время инициализации
- 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).

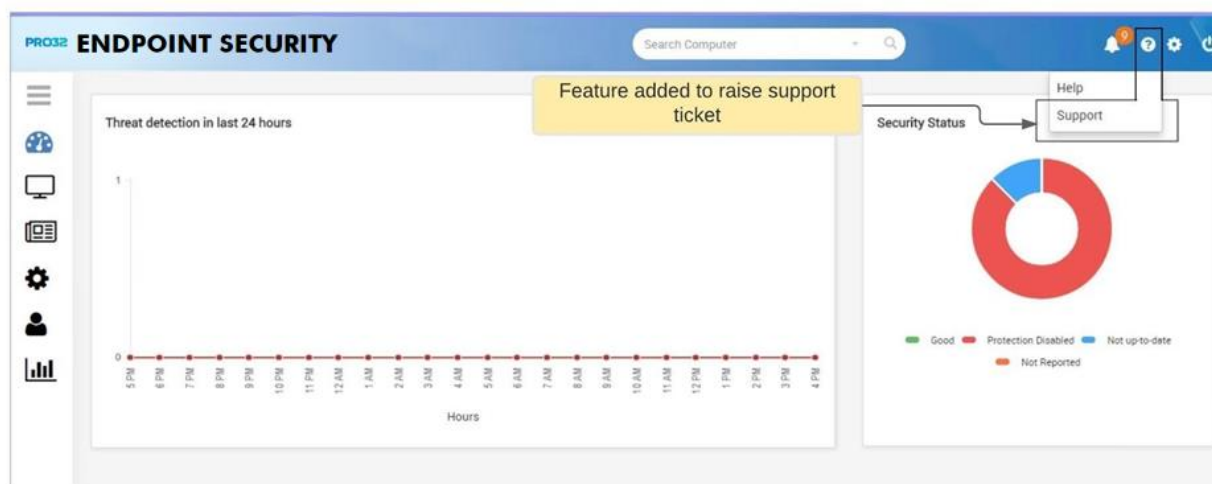


The screenshot displays the 'Install Protection' interface with the 'Client Installation Status' tab selected. An 'Export Type' dropdown menu is open, showing options: CSV (selected), HTML, DOC, and XLS. Below the menu is a table with columns: Computer, Stage, Status, Initiated On, Updated, and Installation Type. The table contains 7 rows of data. At the bottom, there is a pagination bar showing '1 - 7 of 7 Installation status of computers' and a page number '25' out of '50'.

Computer	Stage	Status	Initiated On	Updated	Installation Type	Info
WIN-163AMA7KG95 (172.16.1.63)	Installation	Completed	Jun-11-2020 01:...	Jun-11-2020 01:...	URL Installation	-
172.16.1.123 (172.16.1.123)	Deploying	Failed	Jun-22-2020 11:...	Jun-22-2020 11:...	Remote Installat...	Error 53, Level 2
WIN10-32 (172.16.2.228)	Installation	Completed	Jul-28-2020 05:...	Jul-28-2020 05:...	URL Installation	-
WIN-163AMA7KG95 (172.16.1.63)	Installation	Already Installed	Oct-14-2020 08:...	Oct-14-2020 08:...	URL Installation	-
WIN-163AMA7KG95 (172.16.1.63)	3rd Party Remo...	Reboot pendin...	Oct-14-2020 08:...	Oct-14-2020 08:...	URL Installation	-
WIN-163AMA7KG95 (172.16.1.63)	Installation	Completed	Oct-14-2020 08:...	Oct-14-2020 08:...	URL Installation	-
WIN-163AMA7KG95 (172.16.1.63)	Installation	Already Installed	Nov-18-2020 1:...	Nov-18-2020 1:...	URL Installation	-

Отправьте запрос в службу поддержки из вебконсоли

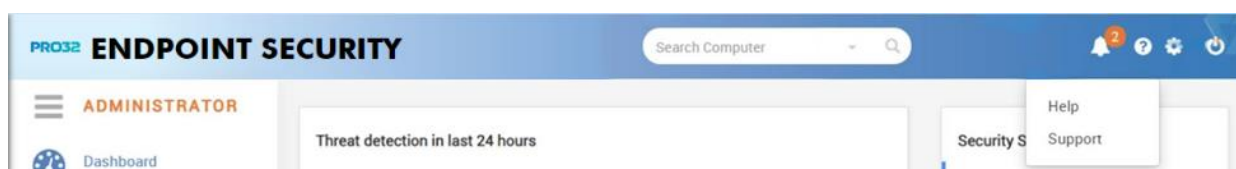
Когда администратор сталкивается с какой-либо проблемой в продукте, пользователь может создать запрос относительно проблемы, нажав на ссылку, указанную на панели мониторинга продукта.



Шаги по созданию заявки на любую проблему

Шаг 1: Перейти к Панели мониторинга

Шаг 2: Выберите значок "Справка" и выберите "Поддержка" в правом верхнем углу



Шаг 3: Выбрав вкладку "Поддержка", вы попадаете на веб-сайт k7, чтобы отправить заявку напрямую

Шаг 4: Введите необходимую информацию для создания заявки имя, фамилию, адрес электронной почты, Приоритет, Тип проблемы, категорию, тему и сообщение

Шаг 5: Прикрепите файл, если это необходимо для предоставления дополнительной информации о созданной заявке

Шаг 6: И нажмите кнопку "Отправить", чтобы отправить запрос.

Политики

Политики — это настраиваемые параметры безопасности для управления компьютерами, находящимися в сети. 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
- Недавно измененные за период

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.

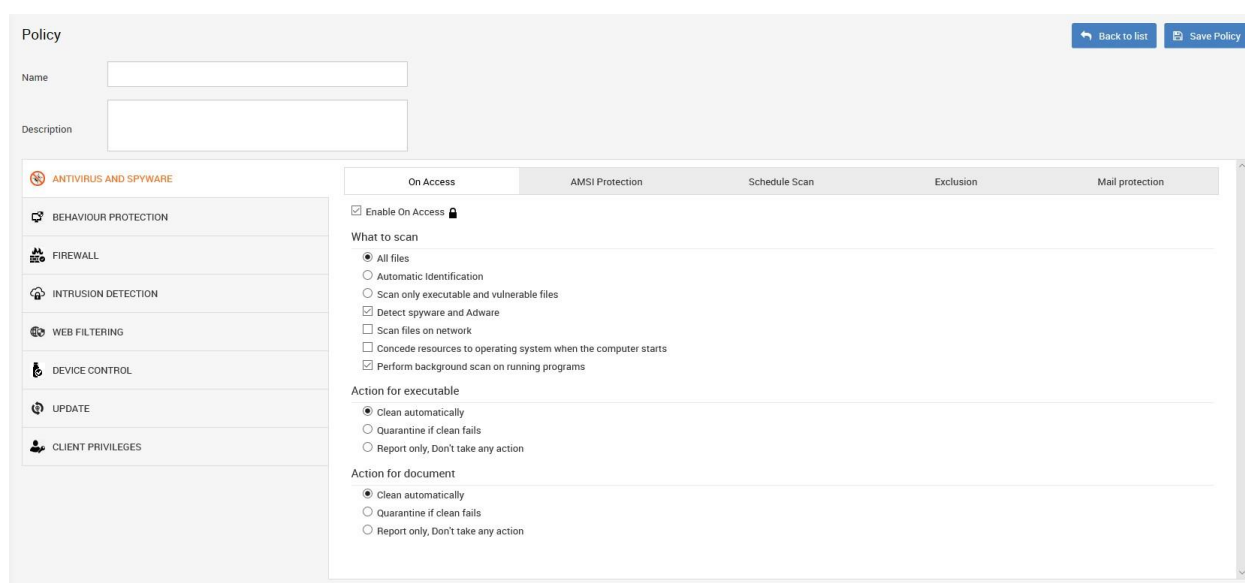
Политика по умолчанию

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.

Как создать новую политику

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.

1. Выберите вкладку «Настройки клиента» в консоли администратора и выберите "Политики" на левой панели.
2. Нажмите **кнопку Создать политику**. На левой панели отображаются различные разделы, такие как Обзор, антивирусные и шпионские программы и т.д. Введите подходящее имя и описание политики перед ее сохранением.

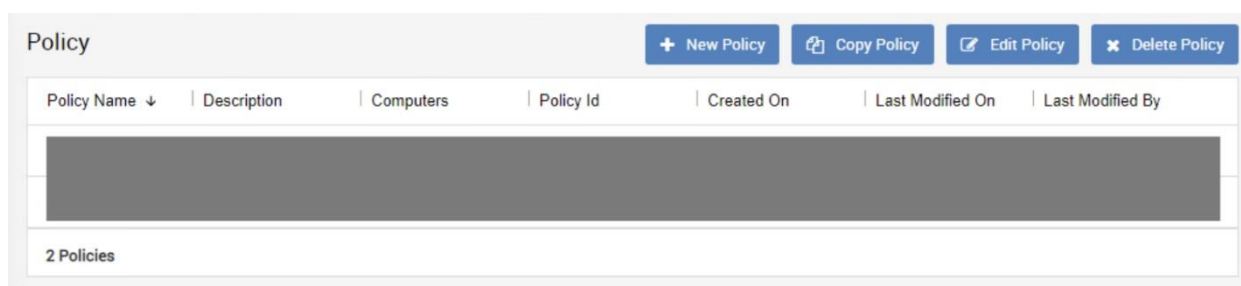


3. На левой панели откройте раздел **Антивирус и антишпионское ПО** и укажите требуемые параметры на пяти вкладках, которые отображаются на главной панели.
4. Откройте раздел **Поведенческий анализ** и укажите требуемые параметры.
5. Откройте раздел **Брандмауэр** и укажите требуемые параметры в группах **В офисе** и **Вне офиса**.
6. Откройте раздел **Веб-фильтрация** и укажите требуемые параметры на трех вкладках главной панели: **Фильтр**, **Часы работы** и **Исключения**.
7. Откройте раздел **Управление устройствами** и укажите требуемые параметры.
8. Откройте раздел **Обновления** и укажите требуемые параметры для управления обновлениями конечных точек.
9. Откройте раздел **Права клиента** и укажите требуемые параметры.
10. Нажмите **Сохранить** и затем **ОК** в появившемся диалоговом окне с сообщением о добавлении новой политики.

Редактирование политики

Вы можете изменять существующие политики на странице «Политика».

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 изменить, и нажмите кнопку **Редактировать**. (Обратите внимание, что нельзя редактировать стандартную политику.)



3. Внесите необходимые изменения в различные разделы, такие как **Антивирус и антишпионское ПО, Защита на основе анализа поведения** и т. д., которые отображаются на левой панели.

4. По окончании нажмите **Сохранить** и затем **ОК** в появившемся диалоговом окне, сообщающем об обновлении политики.

Удаление политики

Вы можете удалять существующие политики на странице «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 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 стандартную политику.

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 **Скопировать политику**.

3. Укажите подходящее имя и описание новой политики и внесите необходимые добавления/изменения к политике, выбирая различные разделы на левой панели, такие как **Антивирус и антишпионское ПО, Поведенческий анализ** и т. д.

4. Нажмите **Сохранить**, чтобы сохранить новую политику.

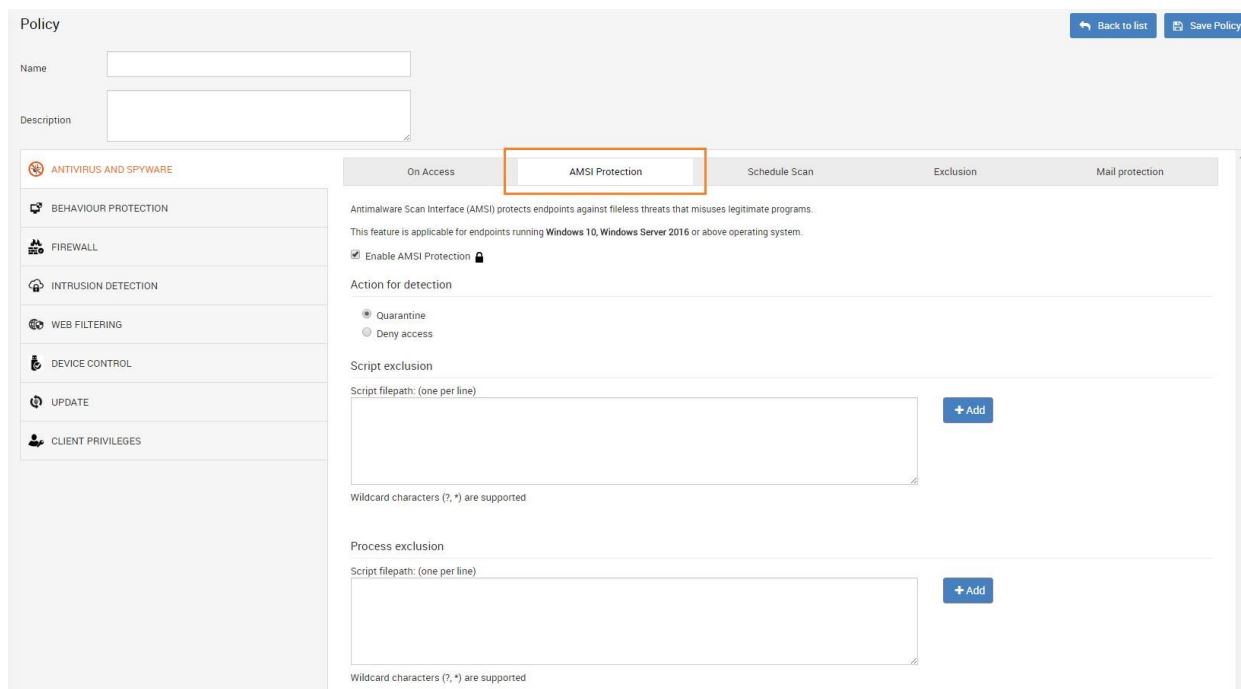
Включение AMSI-защиты в политике

Для включения в политике параметра «AMSI-защита» воспользуйтесь меню страницы **Политики**.

1. Нажмите **Создать политику**. На левой панели отображаются различные разделы, такие как **Обзор, Антивирус и антишпионское ПО** и т. д.

2. Откройте раздел **Антивирус и антишпионское ПО** и установите необходимые параметры на пяти вкладках главной панели.

3. Установите флажок **AMSI-защита** и задайте необходимые параметры.



4. Нажмите **кнопку Сохранить** и нажмите **кнопку ОК** в появившемся диалоговом окне с сообщением о добавлении новой политики.

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 получают 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.

Создание группы

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

1. В консоли администрирования перейдите на вкладку **Настройки клиента** и на панели слева откройте страницу **Группы**.
2. Нажмите **Создать группу** и введите имя и описание новой группы.



3. Список существующих политик отображается в раскрывающемся списке «Выбор политики».

Выберите политику, которую вы хотите применить к новой группе, и нажмите **Добавить**.

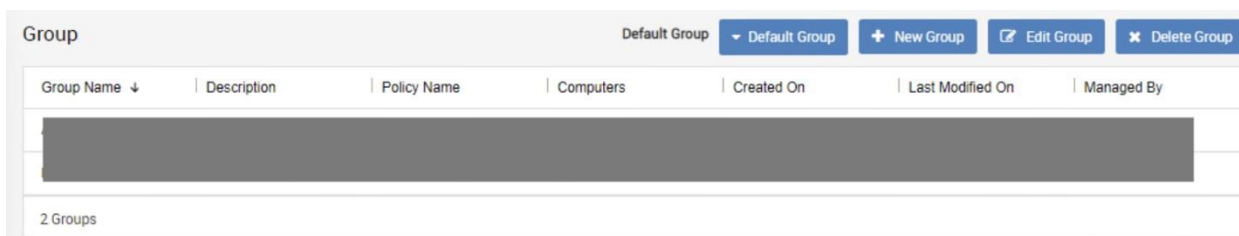
4. Нажмите **ОК** в диалоговом окне для подтверждения добавления новой группы.

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

Редактирование группы

Вы можете изменить имя группы и назначить группе другую политику.

1. В консоли администрирования перейдите на вкладку **Настройки клиента** и на панели 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.

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 на вкладку **Настройки клиента** и на панели 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.

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.

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
- Компьютеры, которые не сканируются
- Компьютеры, которые не подключены к серверу
- 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
- Последнее подключение

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

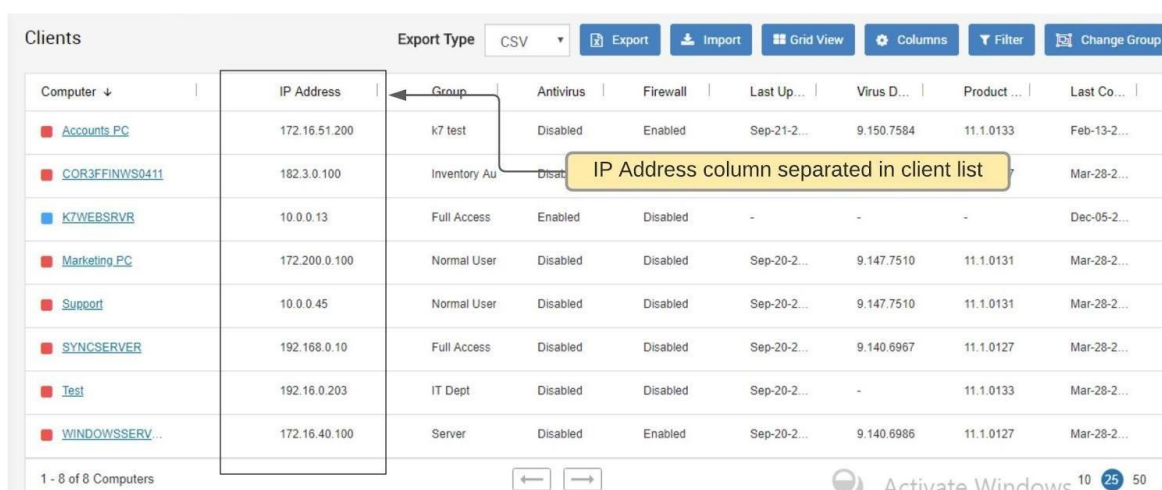
Экспортируются только те столбцы, которые выбраны видимыми в таблице. Можно выбрать следующие столбцы: ◦ Домен ◦ Антивирус ◦ Последнее обновление ◦ Версия продукта ◦ Последний контакт ◦ Операционная система ◦ Последнее сканирование

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

Столбец IP-адресов в списке клиентов и отчетах

В списке клиентов и в отчетах IP-адреса клиентских компьютеров отображаются в отдельном столбце рядом со столбцом имени компьютера.



Computer ↓	IP Address	Group	Antivirus	Firewall	Last Up...	Virus D...	Product ...	Last Co...
Accounts_PC	172.16.51.200	k7 test	Disabled	Enabled	Sep-21-2...	9.150.7584	11.1.0133	Feb-13-2...
COR3FFINWS0411	182.3.0.100	Inventory Au	Disat					Mar-28-2...
K7WEBSRVR	10.0.0.13	Full Access	Enabled	Disabled	-	-	-	Dec-05-2...
Marketing_PC	172.200.0.100	Normal User	Disabled	Disabled	Sep-20-2...	9.147.7510	11.1.0131	Mar-28-2...
Support	10.0.0.45	Normal User	Disabled	Disabled	Sep-20-2...	9.147.7510	11.1.0131	Mar-28-2...
SYNCSERVER	192.168.0.10	Full Access	Disabled	Disabled	Sep-20-2...	9.140.6967	11.1.0127	Mar-28-2...
Test	192.16.0.203	IT Dept	Disabled	Disabled	Sep-20-2...	-	11.1.0133	Mar-28-2...
WINDOWSSERV...	172.16.40.100	Server	Disabled	Enabled	Sep-20-2...	9.140.6966	11.1.0127	Mar-28-2...

Точно так же IP-адреса отображаются в отдельном столбце в приведенных ниже сводных отчетах.

- Сводный отчет по компьютерам с инцидентами

Summary Report Print Back
05 Dec 2020 4:51 PM

Computers with incidents
Incident : Threat Detected Time Range: Past month

Computer	IP Address	Incidents
Accounts PC	172.16.51.200	5
WINDOWSSERVER	172.16.40.100	2
COR3FFINWS0411	182.3.0.100	2
Marketing PC	172.200.0.100	2
Support	10.0.0.45	2
SYNCSERVER	192.168.0.10	1
K7WEBSRVR	10.0.0.13	1

1 - 7 of 7 Activate Windows 10 25 50

Note: A yellow callout box points to the IP Address column with the text "IP Address displayed as separated column".

- Сводный отчет по сканированию

Summary Report Export Type CSV Export Print Back
05 Dec 2020 4:57 PM

Scans
Event Type: Scheduled Scan Group: Any Time Range: Past month

Computer Name	IP Address	Group	Scan Type	Reported On	Files Scanned	Files Infected	Files Cleaned	Boot Sectors Scanned	Boot Sectors Infected
K7WEBSRVR	10.0.0.13	Full Access	Quick Scan	Dec-04-2020 09:16 PM	144	0	0	0	0
Marketing PC	172.200.0.100	Normal Users	Custom Scan	Nov-19-2020 08:23 PM	2428	2	0	2	0
WINDOWSSERVER	172.16.40.100	Server	Custom Scan	Nov-19-2020 08:21 PM	2428	2	0	2	0
Accounts PC	172.16.51.200	k7 test	Custom Scan	Nov-19-2020 08:19 PM	2428	2	0	2	0

1 - 4 of 4 10 25 50

Note: A yellow callout box points to the IP Address column with the text "IP Address displayed as separated column".

Во всех подробных отчетах IP-адрес отображается в виде отдельного столбца в результатах отчета и в фильтре полей, как показано ниже.

Detailed Report

Select the type of report you would like to create

Report type: Applications

Time Range: Past 24 hours

Fields:

Available fields: Publisher, Custom Field Branch

Selected fields: Application Name, Last Reported On, Action, Blocked On, Computer, IP Address, Group

Filters:

Computers / Groups: Select

Application Type: Any

Action: Any

Buttons: Generate, Reset, Save

IP Address displayed as separate column in report fields filter

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.

K7WEBSRVR (10.0.0.13)
Windows Server 2012

Overview Applications Threats Quarantine Tasks Events Hardware Asset

Activity Type: All | Security Change | Scan Completion | Endpoint Update

Export Type: CSV | Export

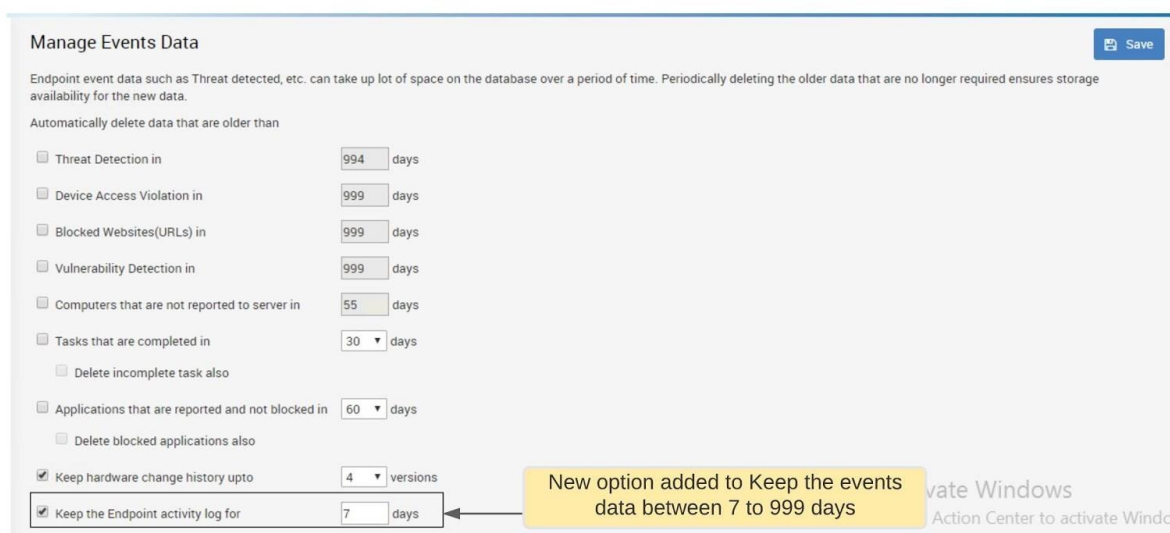
Date	Activities
Nov-24-2020 09:05 PM	Antivirus Enabled by Admin
Nov-24-2020 09:05 PM	Antivirus Disabled by Admin
Nov-24-2020 09:05 PM	Antivirus Enabled by User
Nov-24-2020 09:05 PM	Antivirus Disabled by User
Nov-19-2020 08:56 PM	Antivirus Enabled by Admin
Nov-19-2020 08:56 PM	Antivirus Disabled by Admin
Nov-19-2020 08:56 PM	Antivirus Enabled by Admin
Nov-19-2020 08:56 PM	Antivirus Disabled by Admin
Sep-04-2020 11:10 AM	Firewall Disabled by Admin
Sep-04-2020 11:10 AM	Antivirus Disabled by Product

Antivirus/Firewall Enabled/disabled events triggered by admin

Export feature added

Many Events

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.



Добавление дополнительных полей на страницу «Управление клиентами»

Введение

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.

Create Custom Field

Field Label	<input type="text"/>
Type	<input type="text" value="Text"/>
Add in Quick Search	<input checked="" type="checkbox"/>
Restrict duplicate data	<input type="checkbox"/>
Disable this field	<input type="checkbox"/>

Смена группы

Вы можете сменить группу для одного или нескольких компьютеров. Чтобы сменить группу для компьютеров:

- В разделе Настройки клиента → Клиенты нажмите кнопку «Сменить группу» – появится диалоговое окно «Смена группы».

Clients

Computer selection > Group >

Search Computer

Group:

Computers	Selected Computers
<input type="checkbox"/> Select all the Computers from this Group	

- Выберите группу из выпадающего списка и нажмите кнопку Показать, чтобы просмотреть компьютеры, связанные с выбранной группой
- Выберите компьютеры из списка, которые вы хотите переместить в другую группу, и нажмите кнопку Добавить
- Нажмите кнопку Готово

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

The screenshot shows the 'New Task' configuration interface. It features a breadcrumb trail with 'Task Type' and 'Computer selection'. The 'Type' dropdown is set to 'Quick Scan'. The 'Name' field is empty. There are two sections for actions: 'Action for executable' and 'Action for document', both with 'Clean automatically' selected. The 'cancel' and 'Next' buttons are at the bottom right.

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

Добавление новой задачи

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.

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

Удаление задачи

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

Обновление статусов задач

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

Переопределяющая политика

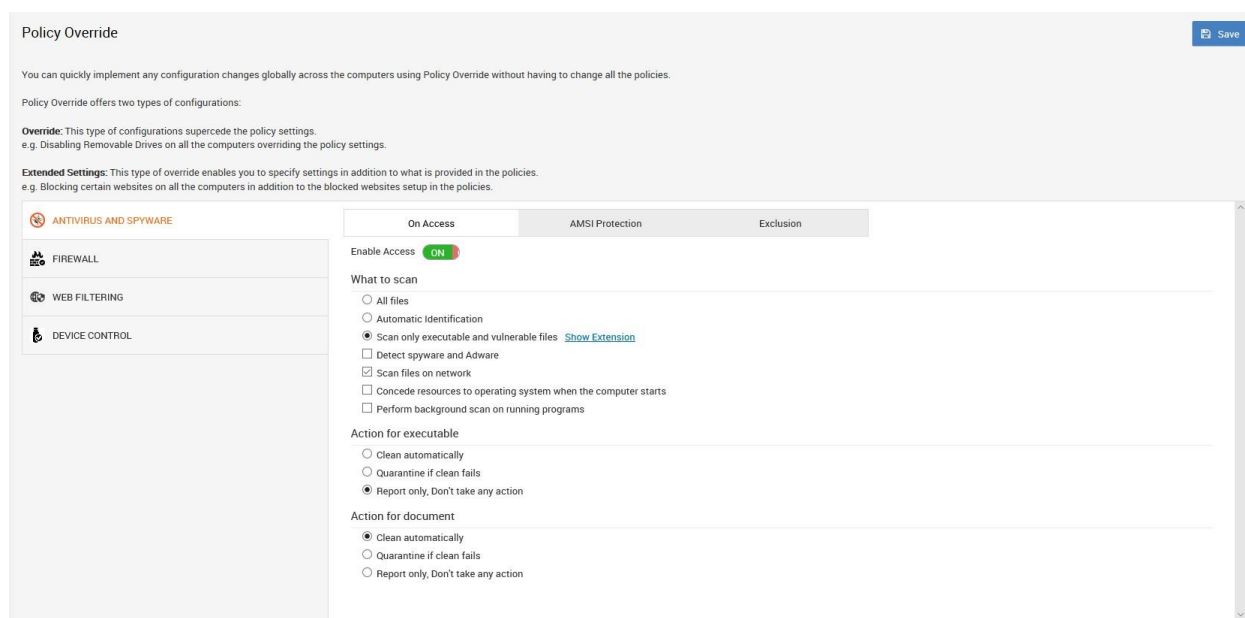
Если требуется применить какой-либо набор параметров сразу на нескольких компьютерах, это можно сделать без изменения их политик с помощью функции «Переопределяющая политика».

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.



В частности, 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
 - Действие для обнаружения
 - Исклучение сценариев
 - Исклучение процессов
 - Исклучение
 - Исклучить определенный файл или папку из сканирования
- Брандмауэр
 - В офисе
 - Уровень безопасности: включить / отключить

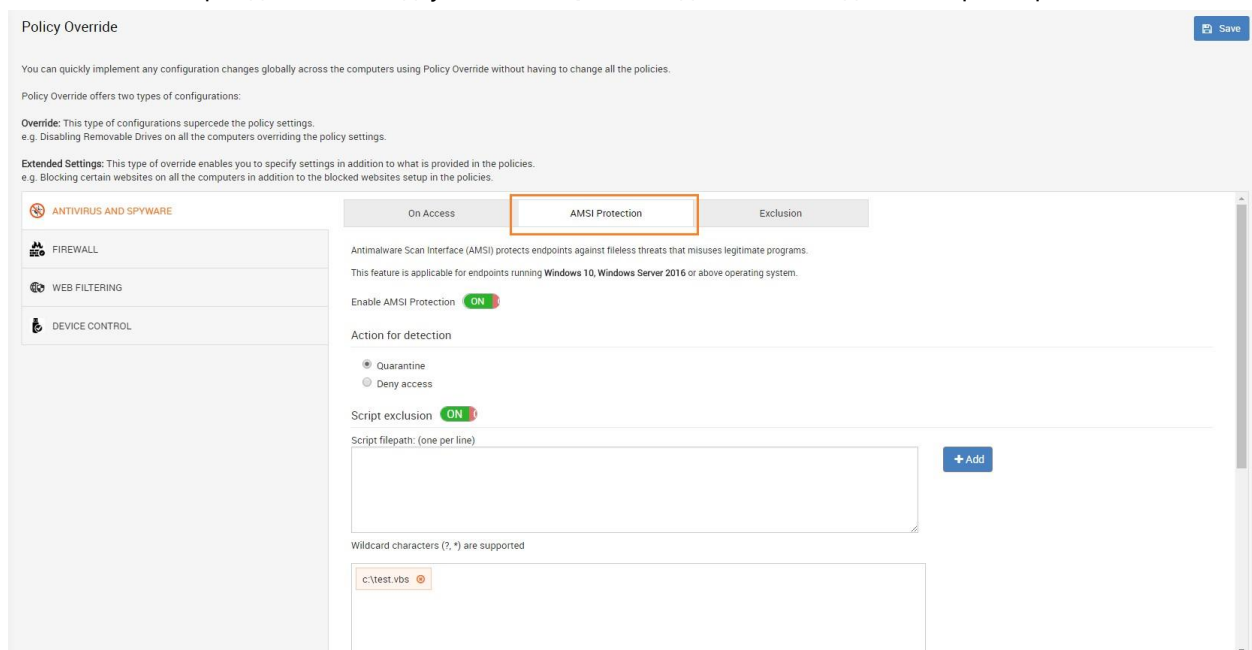
- Дополнительные правила брандмауэра
- Вне офиса
- Уровень безопасности: блокировать всё / доверенные/ недоверенные / запрос
- Дополнительные правила брандмауэра
- Веб-фильтрация
 - Список разрешенных веб-сайтов
 - Список заблокированных веб-сайтов
- Управление устройствами
 - Доступ к устройствам хранения
 - Съёмный носитель
 - CD-привод
 - Дискковод 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».

Включение AMSI-защиты в переопределяющей политике

Можно включить AMSI-защиту в переопределяющей политике.

1. На левой панели щелкните **Настройки клиента**.
2. Откройте страницу **Переопределить политики**.
3. Перейдите на вкладку **AMSI-защита** и задайте необходимые параметры.



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

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.

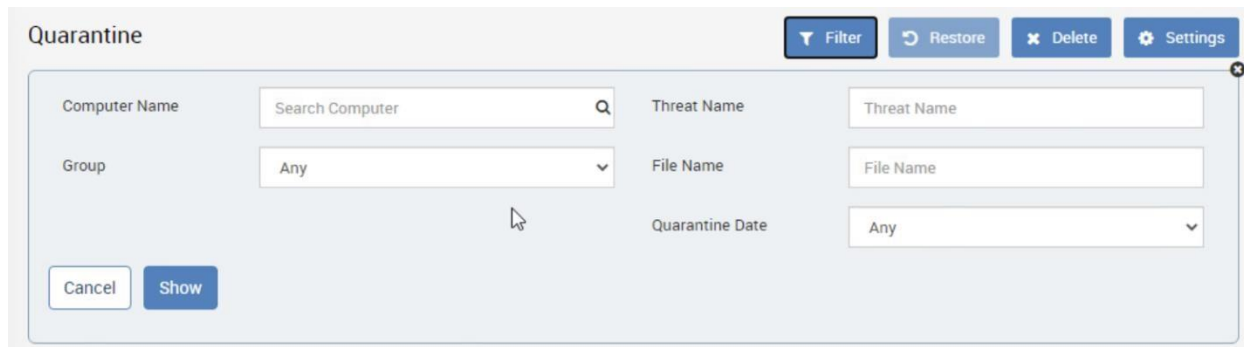
Всякий раз, когда PRO32 Endpoint Security определяет файл как зараженный, программа перемещает его в карантин и запускает очистку или удаление файла. Файлы, перемещенные в карантин, могут содержать вирус или вредоносную программу. Файлы на карантине можно просмотреть по пути **Настройки клиента** → **Карантин** и удалить их, 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, перейдя по пути **Настройки клиента** → **Клиенты** → **Выберите нужное вам Имя компьютера** → вкладка **Карантин**.

Для просмотра файлов в карантине доступны следующие параметры фильтрации:



- 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.

Quarantine Settings ✕

Quarantine Location

Store quarantined files on the server and on the local computer

Store quarantined files on the local computer

Store quarantined files on the server

Purge Files

Purge the quarantined files which are older than days

Управление приложениями

Контроль 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

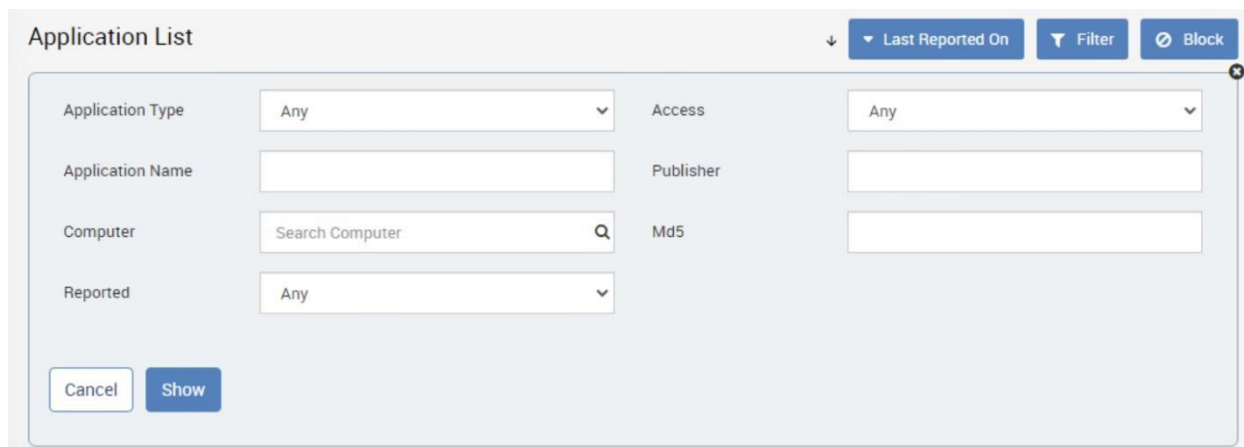
Просмотр списка приложений

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



Заблокировать приложения со страницы списка приложений

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.

Правила блокировки приложений

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. Ограничение доступа возможно в следующих вариантах:

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

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».

New Rule Back to list

Rule > Computer selection > Block access

Rule Name:

File Type: File Path File Hash(MD5)

Folder:

[Show me the list of enviormoment variables](#)

File Name:

This file may be found anywhere under the folder

Нажмите «Далее» и укажите, к каким компьютерам или группам вы хотите применить это правило.

Затем укажите тип блокировки:

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

Чтобы изменить правило, выберите его из списка и нажмите кнопку «Редактировать правило».

Для удаления правила выберите его из списка и нажмите кнопку «Удалить правило».

Настройки

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

Чтобы открыть страницу настроек, перейдите по пути **Главное меню** → **Настройки**.

Можно настроить следующие параметры:

- Уведомления
- Обнаружение местоположения
- Настройки прокси
- Обновления
- Управление данными
- Управление настраиваемыми полями
- Веб-категории
- Лицензия

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».

Псевдоним отправителя электронного письма

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.

Тестирование получения уведомлений по электронной почте

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

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

Notification Save

Email Settings Notifications Client Settings

Email Settings

Configure the Email settings for receiving protection and other notifications by Email.

Sender

Sender name

SMTP Settings

Server

Port

Use secure connection (ssl)

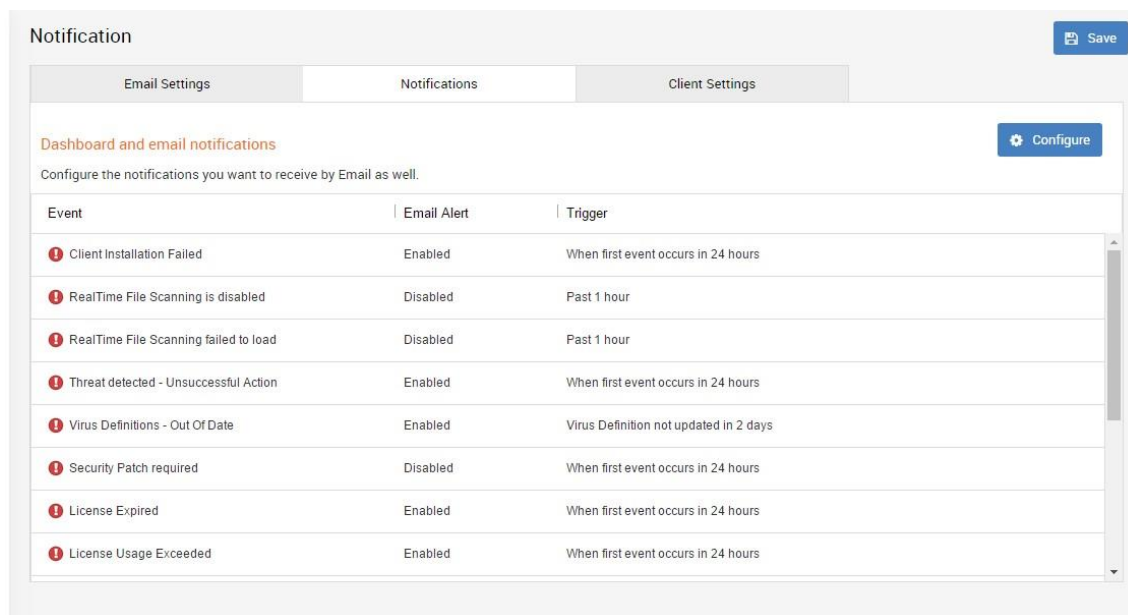
Use authentication

User name

Password [Change Password](#)

Настройка получения по электронной почте уведомлений о событиях

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.



Notification

Save

Email Settings Notifications Client Settings

Dashboard and email notifications

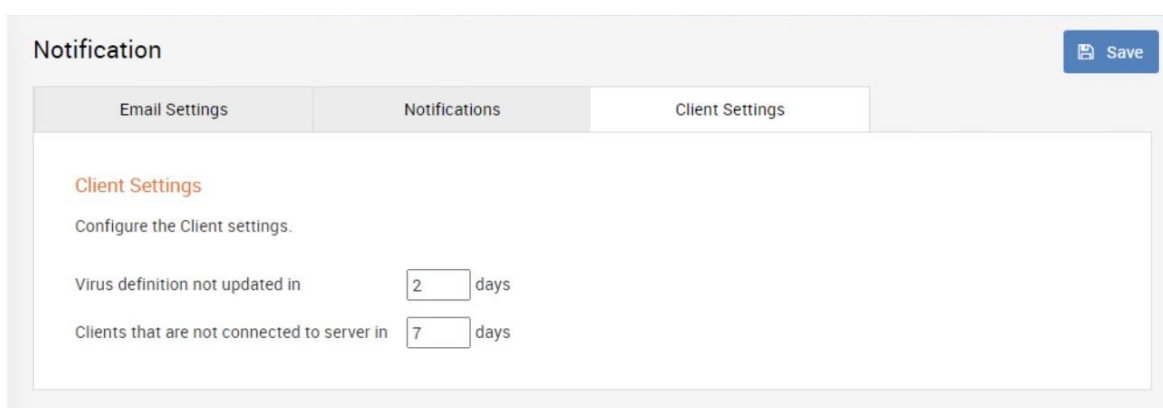
Configure the notifications you want to receive by Email as well.

Configure

Event	Email Alert	Trigger
Client Installation Failed	Enabled	When first event occurs in 24 hours
RealTime File Scanning is disabled	Disabled	Past 1 hour
RealTime File Scanning failed to load	Disabled	Past 1 hour
Threat detected - Unsuccessful Action	Enabled	When first event occurs in 24 hours
Virus Definitions - Out Of Date	Enabled	Virus Definition not updated in 2 days
Security Patch required	Disabled	When first event occurs in 24 hours
License Expired	Enabled	When first event occurs in 24 hours
License Usage Exceeded	Enabled	When first event occurs in 24 hours

Уведомления о не зарегистрированных устройствах

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.



Notification

Save

Email Settings Notifications Client Settings

Client Settings

Configure the Client settings.

Virus definition not updated in days

Clients that are not connected to server in days

В разделе «Управление данными» 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.

Настройка уведомлений о компьютерах, не отправляющих отчеты Шаг

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

Шаг 2. Перейдите на вкладку «Уведомления».

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

Notification

Save

Email Settings Notifications Client Settings

Dashboard and email notifications Configure

Configure the notifications you want to receive by Email as well.

Event	Email Alert	Trigger
Virus Definitions - Out Of Date	Enabled	Virus Definition not updated in 2 days
Security Patch required	Enabled	When first event occurs in 24 hours
License Expired	Enabled	When first event occurs in 24 hours
License Usage Exceeded	Enabled	When first event occurs in 24 hours
Unable to update license information	Enabled	When first event occurs in 24 hours
Subscription expiration in advance	Enabled	When first event occurs in 24 hours
Hardware change detection	Disabled	Immediate
Threat detected	Enabled	Immediate
Scan Task completed	Disabled	Immediate
Schedule Scan interrupted	Enabled	Immediate
Computer not reported	Enabled	Clients that are not connected to server in 7 days

Activate Windows
Go to Settings to activate Windows.

Шаг 4. Нажмите кнопку «Настроить». **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

Шаг 2: Выберите вкладку “Настройки клиента”

Notification Save

Email Settings Notifications Client Settings

Client Settings

Configure the Client settings.

Virus definition not updated in days

Clients that are not connected to server in days

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

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

Обнаружение местоположения

Некоторые параметры безопасности зависят от местоположения компьютера (например, брандмауэр в офисе или вне офиса). PRO32 Endpoint Security может автоматически определять местоположение и применять соответствующие политики.

Вы также можете указать IP-адрес или MAC-адрес шлюза для определения местоположения «в офисе». Сетевые подключения за пределами этих адресов будут считаться местоположением «вне офиса».

Настройки прокси

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

Proxy Settings

Use Proxy server for updates

Proxy Server

Port (Port number is optional)

Proxy Server Authentication

Username

[Set Password](#)

Обновления

Вы можете настроить периодичность проверки сервером наличия обновлений.

The screenshot shows the 'Update' settings page. At the top, it says 'Update'. Below that, it states 'Server checks for its own update automatically in every 6 hour(s)'. There is a dropdown menu showing '6' and a 'Check update now' link. Under the 'Settings' section, there are two radio buttons: 'Always connected to internet' (which is selected) and 'Custom hours'.

Управление данными

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

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

The screenshot shows the 'Manage Events Data' settings page. It has a 'Save' button in the top right corner. The page contains a paragraph explaining that endpoint event data can take up a lot of space and that periodically deleting older data ensures storage availability. Below this, there is a section titled 'Automatically delete data that are older than' with several rows of settings:

- Threat Detection in 120 days
- Device Access Violation in 120 days
- Blocked Websites(URLs) in 30 days
- Vulnerability Detection in 120 days
- Computers that are not reported to server in 15 days
- Tasks that are completed in 30 days
 - Delete incomplete task also
- Applications that are reported and not blocked in 60 days
 - Delete blocked applications also
- Keep hardware change history upto 2 versions

Добавление дополнительных полей на страницу «Настройки клиента»

Благодаря функции добавления настраиваемых полей администратор может вставить на страницу «Настройки клиента» необходимые ему данные строкового или числового типа. Затем эти данные

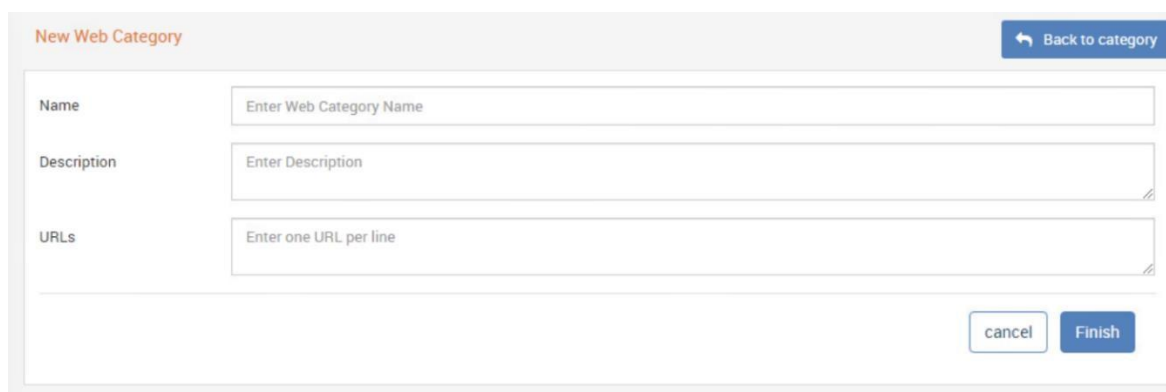
администратор может использовать при поиске клиентских компьютеров всякий раз, когда ему требуется создать отчет или назначить задачу (сканирование, обновление и т. д.) отдельному компьютеру или группе компьютеров.

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

Веб-категории

Администратор может создавать настраиваемые веб-категории и применять к ним необходимые политики. Веб-категория включает имя, описание и список URL-адресов.

Веб-категории можно редактировать и удалять.



The screenshot shows a web form titled "New Web Category". At the top right, there is a blue button with a back arrow and the text "Back to category". The form contains three input fields: "Name" with the placeholder "Enter Web Category Name", "Description" with the placeholder "Enter Description", and "URLs" with the placeholder "Enter one URL per line". At the bottom right of the form, there are two buttons: "cancel" and "Finish".

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.

Администрирование

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

Роли

Чтобы открыть эту страницу, перейдите по пути Меню → Администрирование → Роли.

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.

Для создания роли 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 выбранными разрешениями, нажмите кнопку «Создать».

Permissions	Read Only	Manage
<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Clients	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Tasks	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Groups	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Install Protection	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Policy Override	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Quarantine	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Application Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Manage Server Settings	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Manage Roles and Users	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Manage Reports	<input type="checkbox"/>	<input type="checkbox"/>

Пользователи

Чтобы открыть эту страницу, перейдите по пути Меню → Администрирование → Пользователи.

Для каждого пользователя будут указаны следующие атрибуты:

- Полное имя
- Адрес электронной почты

- Имя пользователя
- Назначенные роли
- Последний вход
- Созданный логин
- Статус активности

Создание пользователя

Чтобы создать нового пользователя, укажите следующие параметры и нажмите кнопку «Создать 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».

The screenshot shows the 'Create User' form with the following fields and options:

- Full Name:** Input field with placeholder 'Enter full name'.
- Email Address:** Input field with placeholder 'Enter email id'.
- User Name:** Input field with placeholder 'Enter User Name'.
- Password:** Input field with placeholder 'Enter Password' and a note 'Minimum 8 characters'.
- Re-type Password:** Input field with placeholder 'Re-type the password'.
- Account is Disabled:** A checkbox that is currently unchecked.
- Roles:** A dropdown menu currently showing 'Full Access'.
- Notes:** Below the roles dropdown, it states 'Full access role will have a full privileges to the admin console.'
- Buttons:** 'Cancel' and 'Create' buttons at the bottom left.

Суперадминистратор

Если в организации нужно управлять огромным количеством конечных точек, суперадминистратор может разделить свои обязанности по управлению конечными точками с несколькими администраторами групп. Однако конкретному администратору группы может быть запрещен доступ к определенным критически важным параметрам, таким как изменение политики безопасности, удаление с конечной точки антивирусного ПО и т. д.

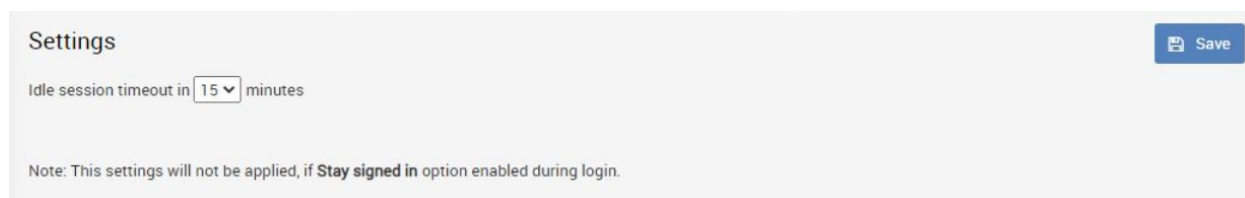
Администратор группы

Пользователи с правами администратора группы могут управлять одной или несколькими группами конечных точек, имея полные или ограниченные права. Эти администраторы групп могут выполнять такие задачи, как сканирование, обновление, удаление антивирусного ПО и т. д., но только по заданным компьютерам или группам.

Всякий раз, когда администратор группы выполняет какие-либо действия или меняет политику, эти действия будут регистрироваться в системе с уведомлением суперадминистратора, чтобы он мог предотвратить совершение любых рискованных действий в корпоративной среде.

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 «Остаться в системе».



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.

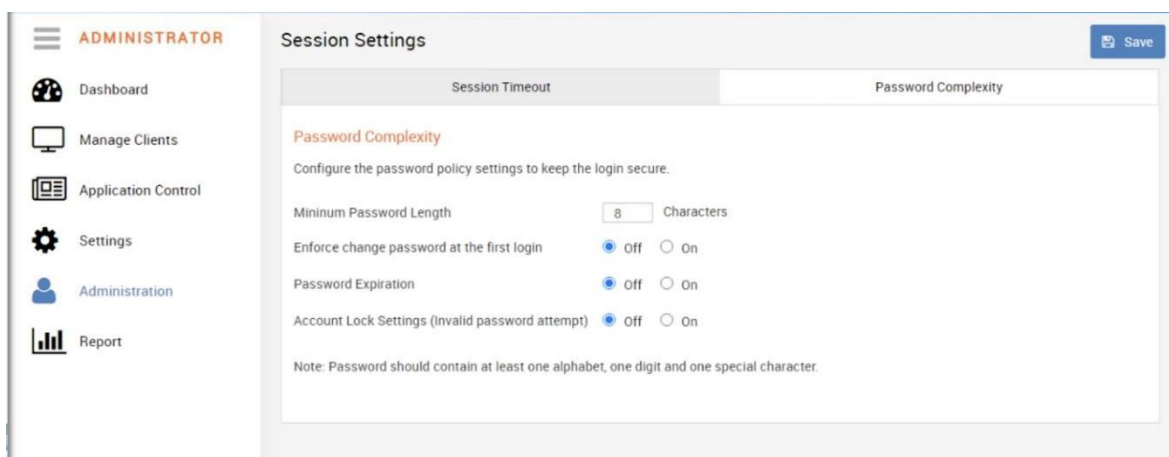
- **Блокировка учетной записи при попытке ввода неверного пароля** – обеспечивает блокировку входа пользователя в систему в течение указанного периода, если количество неудачных попыток ввода превышает указанное пороговое значение. Во время блокировки администратор может сменить пароль, если пользователю 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.

Настройка параметров пароля

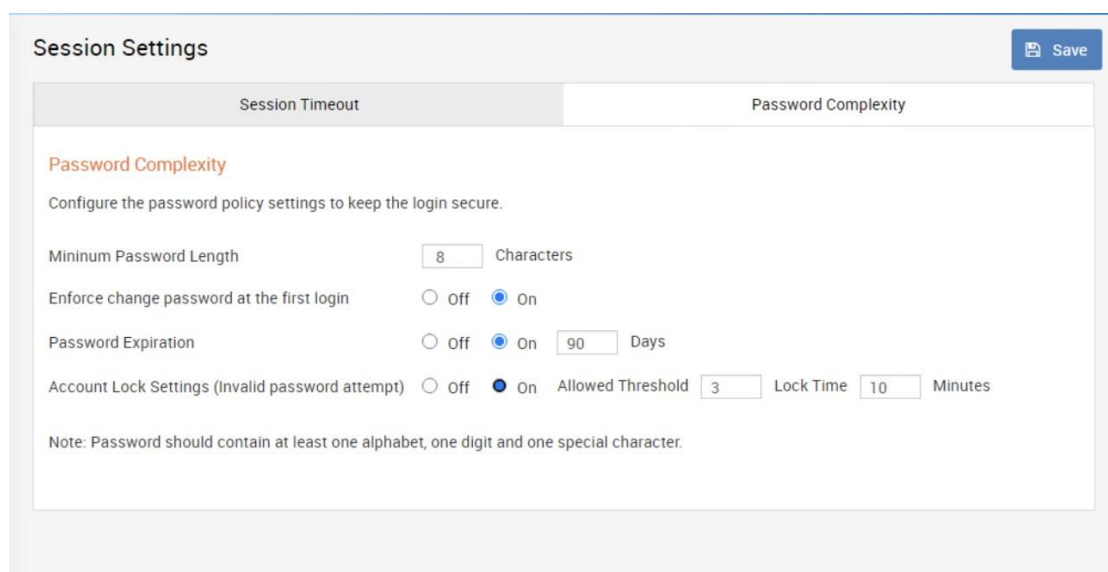
Шаг 1. Перейдите по пути Администрирование → Настройки.

Шаг 2. Откройте вкладку «Сложность пароля».

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

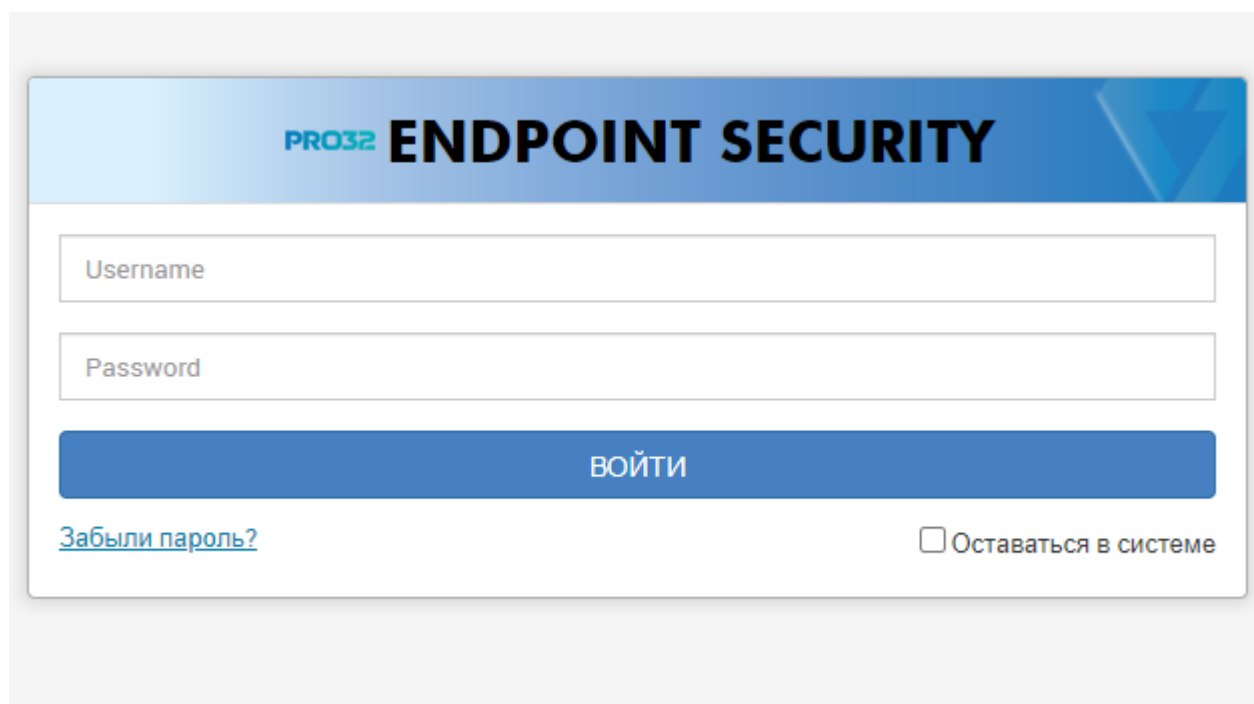


Ниже показан экран настроек, когда все параметры включены.



Вход

Флажок «Остаться в системе» на экране входа в систему по умолчанию снят, чтобы максимальная продолжительность сеанса была ограничена. При установленном флажке максимальная продолжительность сеанса составит 7 дней, если за это время пользователь не выйдет из веб-консоли.



PRO32 **ENDPOINT SECURITY**

Username

Password

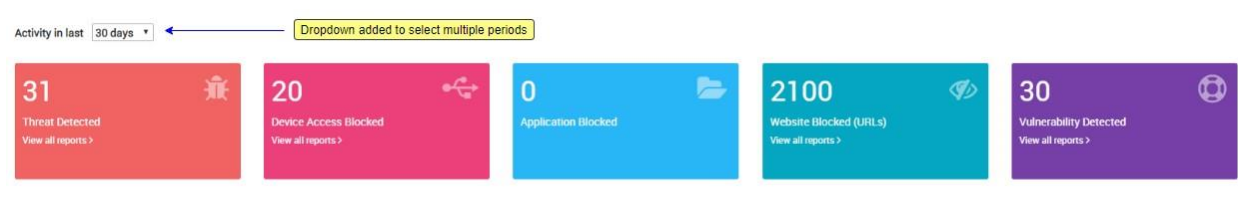
ВОЙТИ

[Забыли пароль?](#) Оставаться в системе

Сводка по событиям на информационной панели

Виджет «Активности» отображает количество событий за определенный период (по умолчанию – за последние 30 дней). К событиям относятся обнаружение угроз, блокировка устройств, обнаружение уязвимостей, блокировка веб-сайтов, блокировка приложений и т. д.

Теперь в качестве продолжительности периода можно указать не только 30 дней, но и 24 часа и 7 дней.



Вы можете выбрать любой из периодов и просмотреть сводный отчет по активности. Выбранный период будет автоматически сохранен, и при последующем посещении панели мониторинга даже после выхода из системы будет отображаться заданный период.

Меню в заголовке главной страницы

Это меню помогает вам получить быстрый доступ к некоторым ключевым функциям продукта. Поле «Поиск» поможет быстро найти нужные данные, а колокольчик уведомлений немедленно уведомит о важных событиях и действиях.



Функция поиска

Поле «Поиск», расположенное в заголовке главной страницы, помогает администраторам найти нужную информацию. Доступные следующие варианты поиска:

- Поиск компьютера
- Поиск группы
- Поиск по настраиваемому полю, созданному администратором
- Поиск веб-сайта
- Поиск приложения

Уведомление

Колокольчик уведомлений информирует о важных событиях и действиях. При выборе уведомления пользователь переходит в соответствующее окно.

Справка

При выборе меню «Справка» пользователь переходит к полному справочному руководству по PRO32 Endpoint Security.

Настройки

В меню настроек пользователь может изменить свой текущий пароль для входа, а также изменить логотип на консоли.

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».

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.

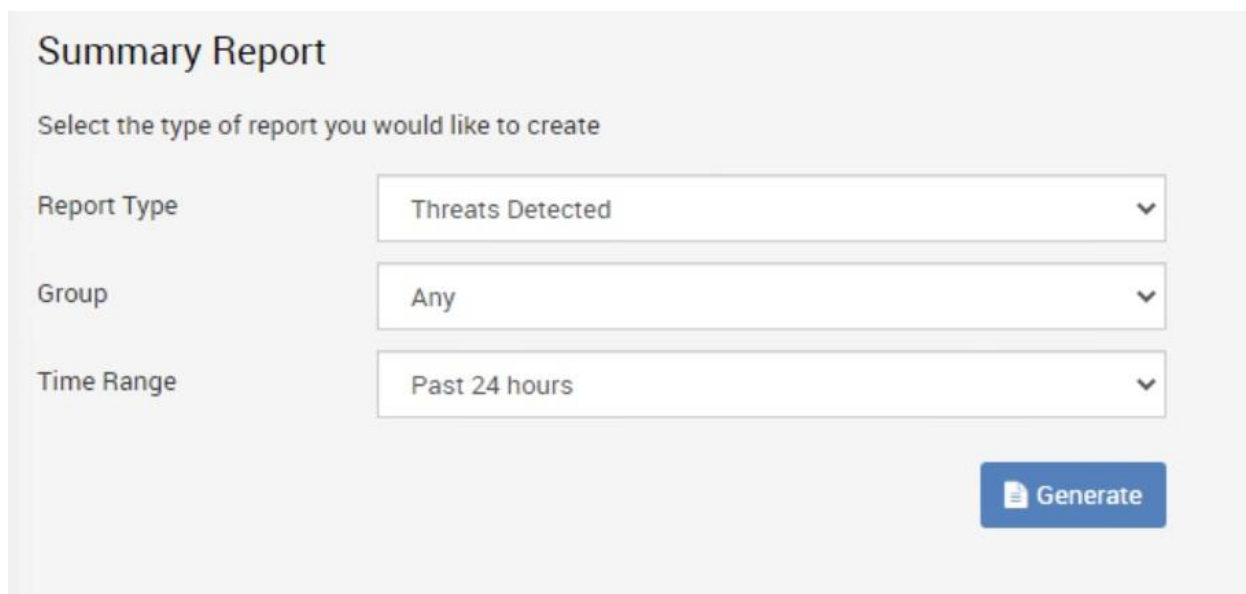
Краткий отчет

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

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



Summary Report

Select the type of report you would like to create

Report Type: Threats Detected

Group: Any

Time Range: Past 24 hours

Generate

Создание кратких отчетов по сканированию

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

Создание краткого отчета: тип отчета – сканирование

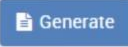
Шаг 1. Перейдите по пути Отчеты → Краткие сведения.

Шаг 2. В раскрывающемся списке «Тип отчета» выберите «Сканирование»

Summary Report

Select the type of report you would like to create

Report Type	Scans
Event Type	Threats Detected Applications Blocked Websites Blocked - URL Websites Blocked - Category Device Access Violation Summary Computers with incidents Hardware Assets Scans
Group	
Time Range	

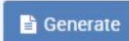


Шаг 3. Выберите нужный тип событий

Summary Report

Select the type of report you would like to create

Report Type	Scans
Event Type	Scheduled Scan Scheduled Scan Malware Scan Task On Demand Scan By User
Group	
Time Range	Past 24 hours



Шаг 4: Выберите нужную "Группу" из выпадающего списка**Шаг 5:** Выберите требуемый временной диапазон**Шаг 6:** Нажмите на кнопку Сгенерировать, чтобы просмотреть отчет в консоли. Отчёт может быть экспортирован в любой из поддерживаемых форматов файлов:

- Имя компьютера, IP - адрес
- Группы
- Сообщается о
- Файлы сканируются, файлы заражаются, файлы очищаются.
- Загрузочные сектора проверены, загрузочные сектора заражены, загрузочные сектора очищены.
- Проверенный раздел, Зараженный раздел, Очищенный раздел
- Сканировалось

Summary Report											Export Type	CSV	Export	Print	Back
Scans											05 Dec 2020 1:41 PM				
Event Type: On Demand Scan By User Group: Any Time Range: Past year															
Computer Name	IP Address	Group	Reported On	Files Scanned	Files Infected	Files Cleaned	Boot Sectors Scanned	Boot Sectors Infected	Boot Sectors Cleaned	Partition Scan					
K7WEBSRVR	10.0.0.13	Full Access	Nov-19-2020 09:20 PM	119	0	0	0	0	0	0					
SYNCSERVER	192.168.0.10	Full Access	Nov-19-2020 08:24 PM	23	23	21	2	0	0	1					
K7WEBSRVR	10.0.0.13	Full Access	Nov-19-2020 08:22 PM	23	23	21	2	0	0	1					
Accounts PC	172.16.51.200	k7 test	Nov-19-2020 08:19 PM	23	23	21	2	0	0	1					
K7WEBSRVR	10.0.0.13	Full Access	Sep-03-2020 07:44 PM	145	0	0	0	0	0	0					
K7WEBSRVR	10.0.0.13	Full Access	Sep-01-2020 12:22 PM	138	0	0	0	0	0	0					

1 - 6 of 6

Подробный отчет

Помимо информации, отображаемой в кратком отчете, в подробном отчете будут добавлены следующие поля:

- Тип угрозы
- Версия антивирусной программы
- Время отчета
- Компьютер
- Пользователь
- Группа
- Уровень угрозы
- Предпринятое действие
- Название угрозы
- Время обнаружения
- Путь к файлу
- Тип события
- Родительский процесс

Параметры фильтрации:

- Компьютер/группа
- Пользователь
- Уровень угрозы
 - Высокий
 - Средний
 - Низкий
 - Отсутствует
- Предпринятое действие
 - Очистка
 - Очистка или блокировка
 - Удаление

- o Помещено в карантин
- o Создан отчет
- o Прервано

Нажмите кнопку «Сброс», чтобы переустановить все вышеперечисленные параметры в начальное состояние.

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

Создание подробных отчетов по сканированию

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 Шаг

1. Перейдите по пути Отчет → Подробнее.

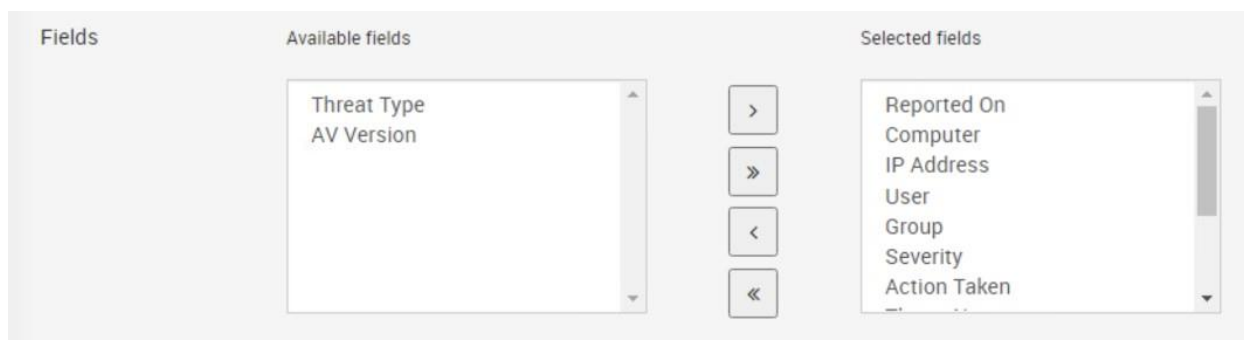
Шаг 2. Выберите в качестве типа отчета «Обнаруженные угрозы». **ar**

3. Укажите период.

Шаг 4. Используйте клавиши со стрелками перенесите нужные поля из доступных в выбранные.

Добавлены новые поля:

- Имя компьютера
- IP-адрес



Шаг 5. При необходимости установите нужные фильтры.

Detailed Report

Select the type of report you would like to create

Report type: Threats Detected

Time Range: Past 24 hours

Fields:

- Available fields: Threat Type, AV Version, custfield, test1
- Selected fields: Reported On, Computer, IP Address, User, Group, Severity, Action Taken

Filters:

- Computers / Groups: Select
- Event type: Any (selected)
- User: [empty]
- Threat Severity: [empty]
- Action Taken: [empty]

Buttons: Generate, Reset, Save

Event type filter is added to select scan types

Activate Windows
Go to Action Center to activate Windows.

Шаг 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.

Создание отчета об изменении состава аппаратных средств

Шаг 1. Перейдите по пути Отчеты → Подробнее.

Шаг 2. Выберите в качестве типа отчета «Аппаратные средства».

Detailed Report

Select the type of report you would like to create

Report type: Hardware Asset

Sub type: Threats Detected, Applications, Websites Blocked, Device Access, Vulnerability Detected, Scan Task, **Hardware Asset**

Fields: Computer, IP Address, Group, Hardware Change

Filters: Computers / Groups [Select](#)

[Generate](#) [Reset](#) [Save](#)

Шаг 3: Выберите “Журнал изменений” в подтипе

Detailed Report

Select the type of report you would like to create

Report type: Hardware Asset

Sub type: Full Report

Fields: Full Report, **Change log**, Summary, System Manufacturer, RAM, Operating System, Processor

Filters: Computers / Groups [Select](#)

[Generate](#) [Reset](#) [Save](#)

Шаг 4. Выберите необходимые поля для включения в отчет.

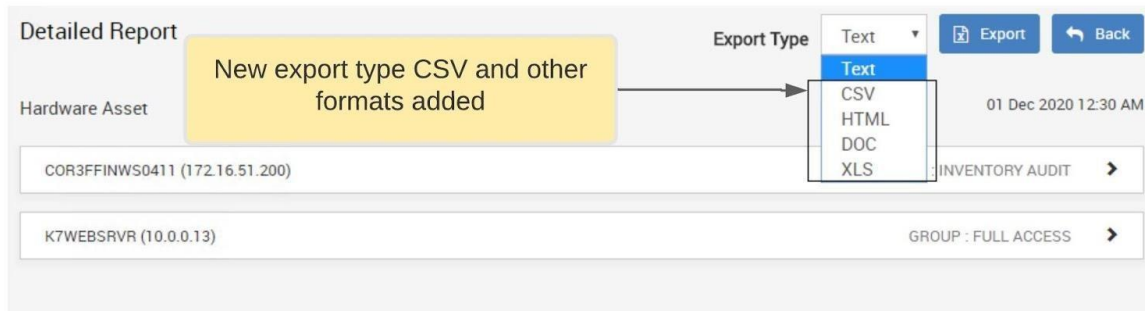
Шаг 5. Выберите один или несколько компьютеров или групп.

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

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

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.



Ниже показан пример CSV-файла.

Computer Name	IP Address	Manufacturer	System Mo	Total RAM	Processors	Caption	Cores	Logical Processors	Family	Architecture	Network Adapter Name
COR3FFINWS0411	172.16.51.	Dell Inc.	Inspiron 56	0 bytes	Pentium(R)	x64 Family	3	2	Other	x64	Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet NIC (NDI
K7WEBSRVR	10.0.0.13	Dell Inc.	Vostro 380	4 GB	Intel(R) Per	Intel64 Fam	2	2	Pentium Br	x64	Realtek PCIe GBE Family Controller

Шаблон отчета

Список доступных шаблонов отчетов содержит следующие поля:

- Имя шаблона
- Описание
- Запланированное электронное сообщение
- Время создания
- Автор

Выберите нужный шаблон отчета из списка и нажмите кнопку «Создать», чтобы создать отчет на базе этого шаблона.

Выберите нужный шаблон отчета из списка и нажмите кнопку «Редактировать», чтобы изменить этот шаблон.

Выберите нужный шаблон отчета из списка и нажмите кнопку «Удалить», чтобы удалить этот шаблон.

Экспорт всех видов отчетов в различных форматах

Подробные отчеты теперь можно экспортировать в различных форматах – CSV, HTML, DOC и XLS.

PRO32