

Что нового в KES 11.1 и KSC 11. Краткий обзор



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

Проверка зашифрованного трафика

Защита от MAC Spoofing

Role Based Access Control for KES

Kaspersky Security Center 11: операционные системы и сервера баз данных

- **Операционные системы:**
 - Windows 10 RS5 (October 2018 Update)
 - Windows Server 2019
- **Сервера баз данных:**
 - Microsoft SQL Server 2017
 - Amazon RDS (MS SQL)
 - Microsoft Azure SQL DB



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

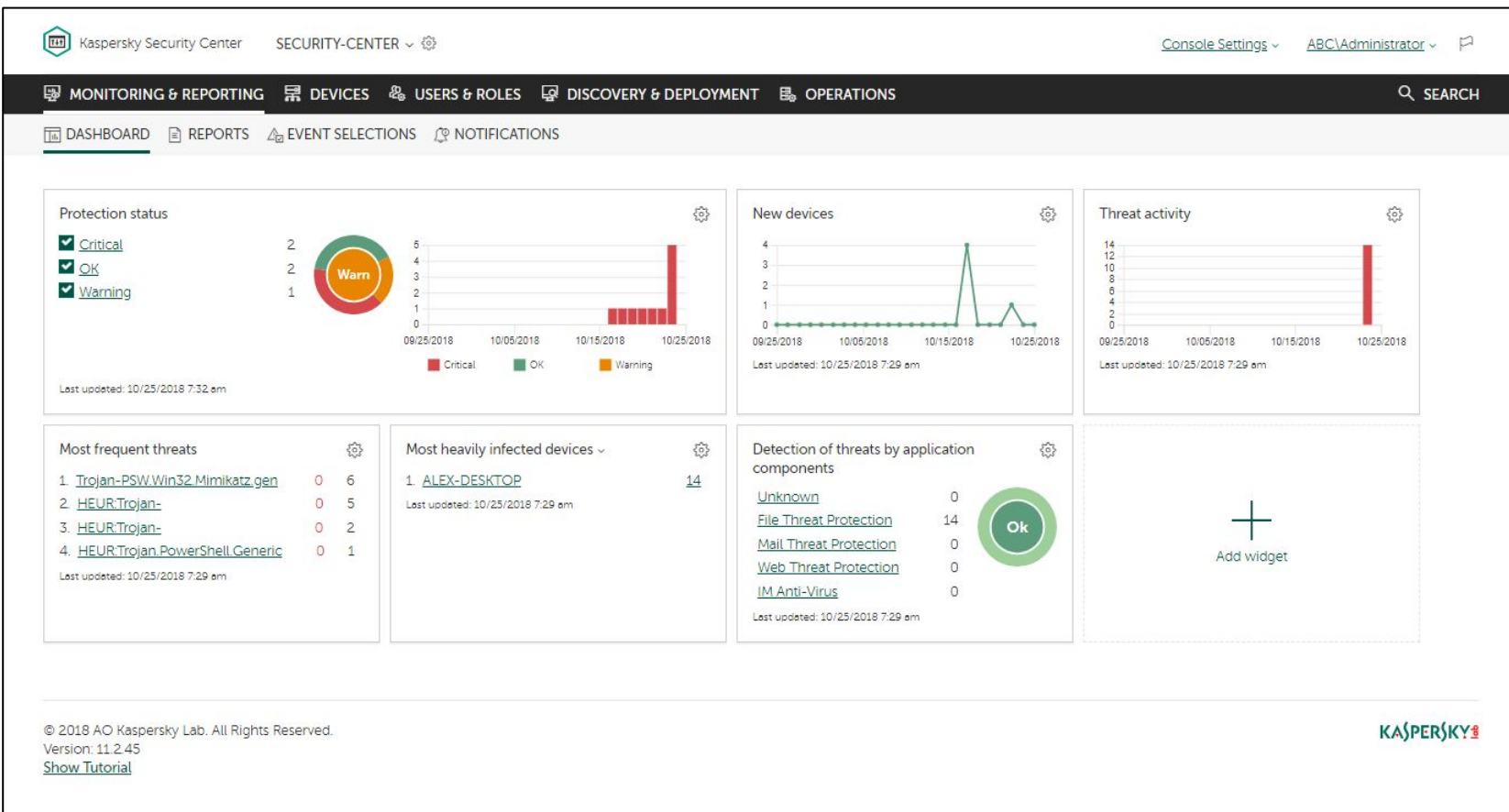
Проверка зашифрованного трафика

Защита от MAC Spoofing

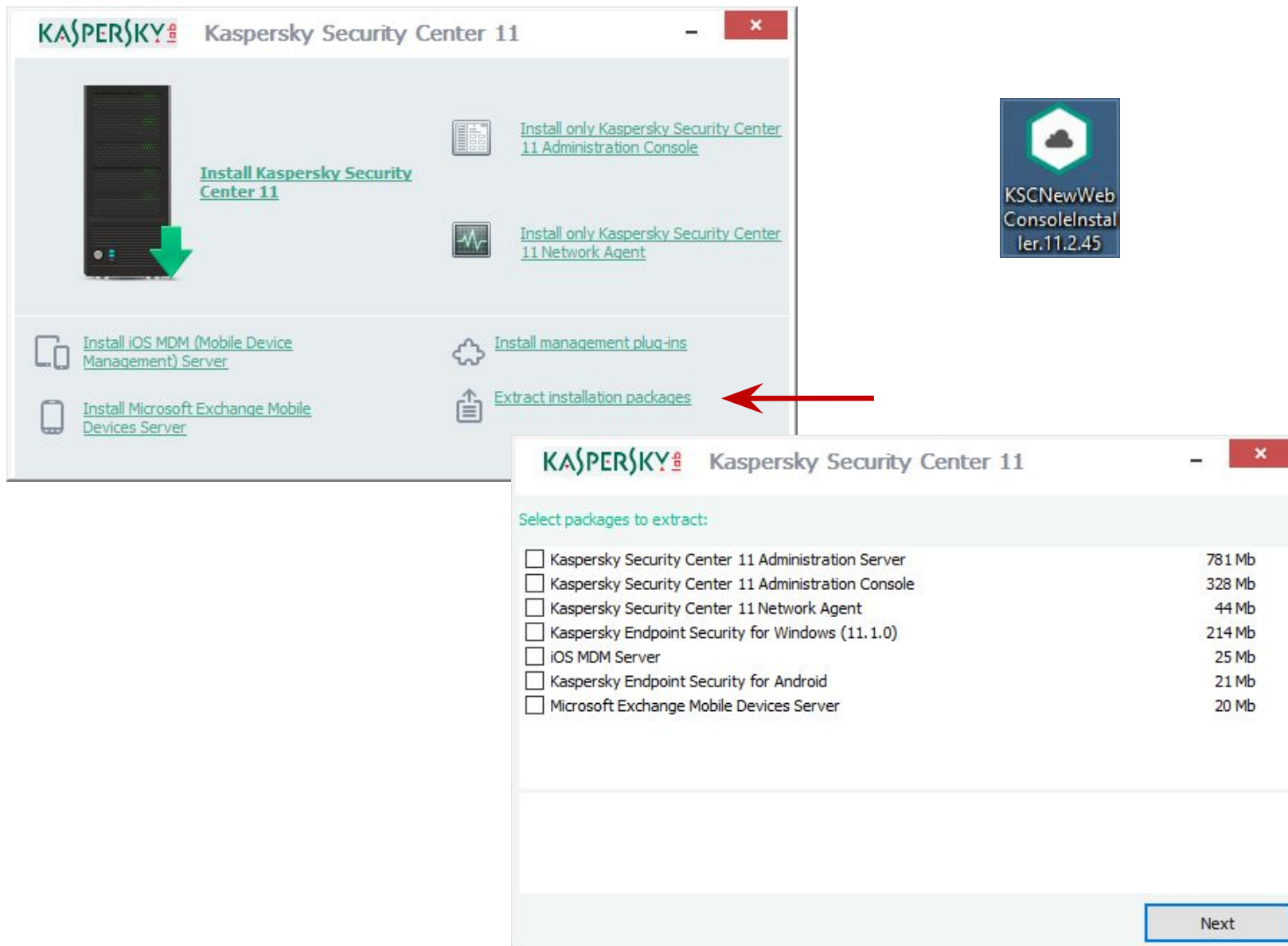
Role Based Access Control for KES

Web Console vs. MMC Console

- Не требует установки на стороне клиента
- Нет привязки к операционной системе
- Поддерживает работу с сенсорным экраном
- Не требует поддержки браузерами Java / ActiveX / Flash
- В текущей версии не поддерживается управление:
 - шифрованием
 - мобильными устройствами
 - уязвимостями и обновлениями

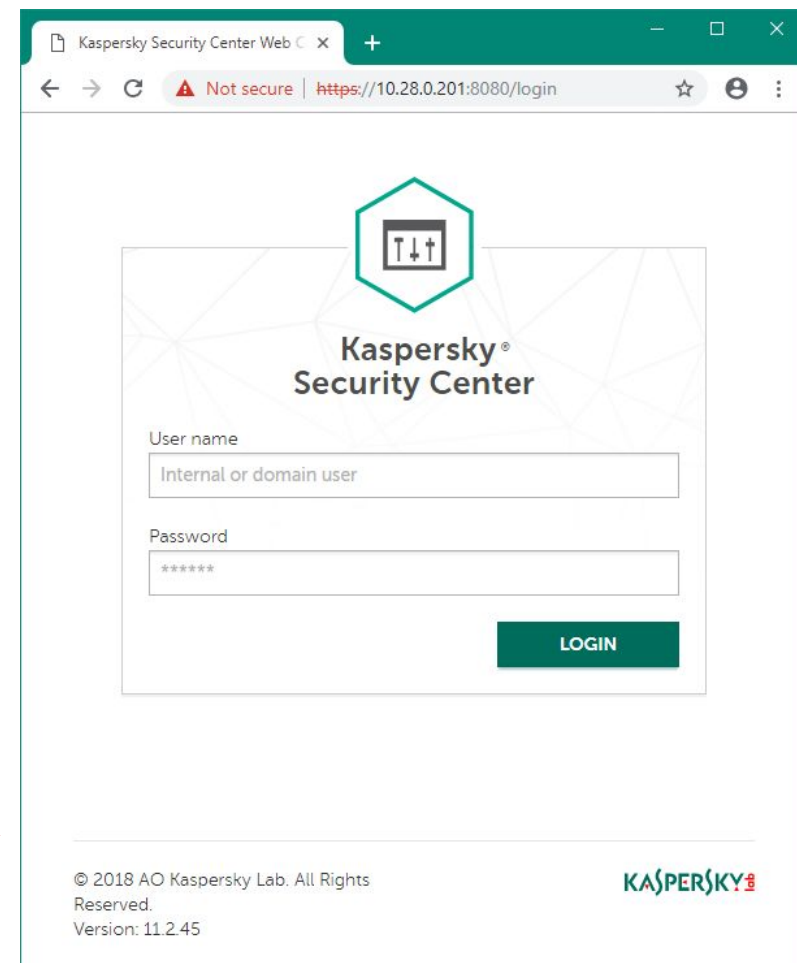
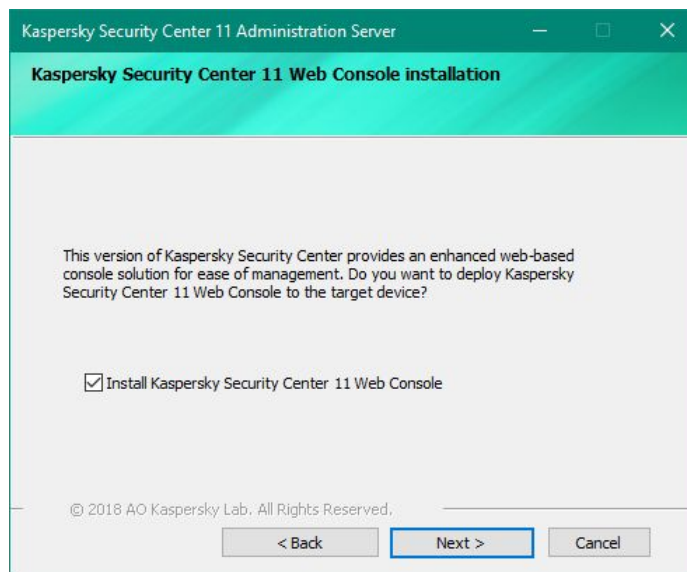


Дистрибутив: KSC 11 Web Console



- Дистрибутив KSC 11 Web Console:
 - является частью дистрибутива KSC
 - Существует в виде отдельного дистрибутива
- Извлечь дистрибутив KSC 11 Web Console в виде отдельного инсталляционного пакета нельзя
- Может быть установлена на отдельный компьютер

Web Console: Мастер установки KSC



- При первом запуске Kaspersky Security Center 11 Web Console подключается к локальному Серверу администрирования <https://localhost:8080/>
- Подключение с удаленной машины <https://<IP-address>:8080/>

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. Задайте учетные записи
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

Установка Web Console



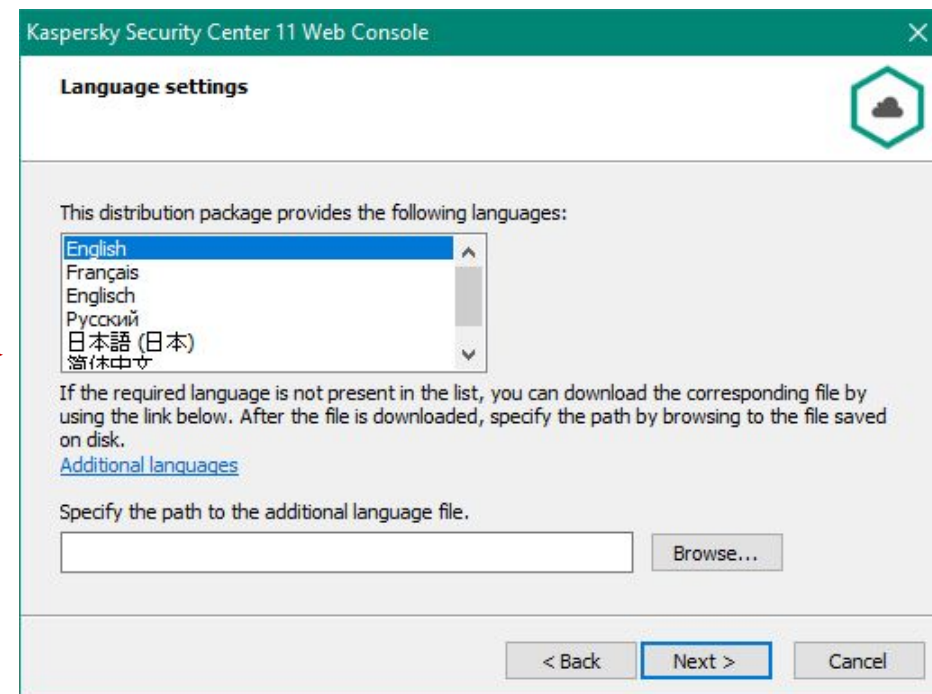
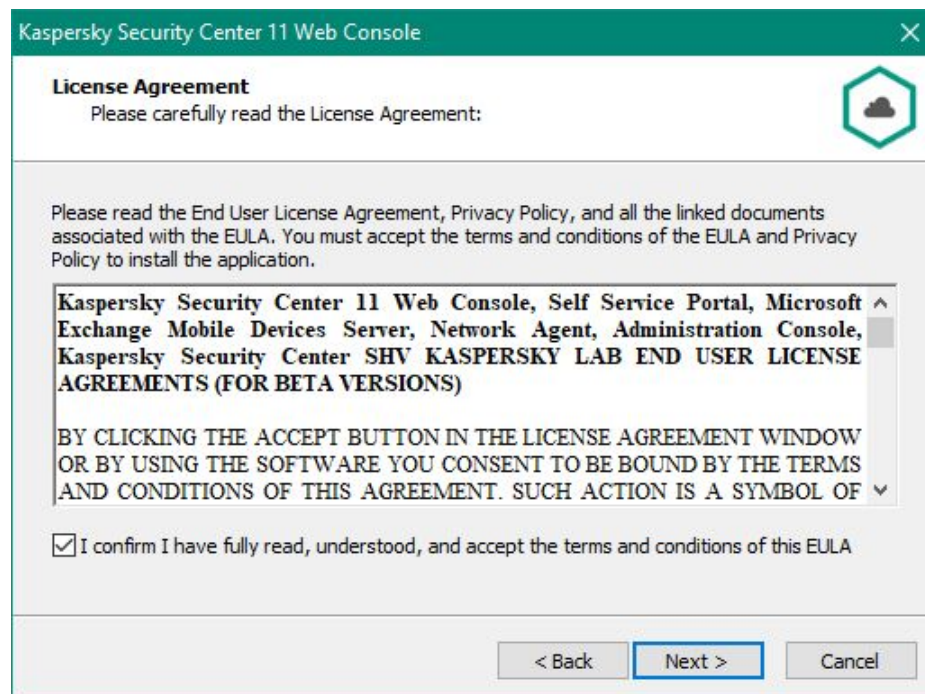
Web Console – это отдельный дистрибутив, который можно установить как вместе с Kaspersky Security Center, так и на отдельный компьютер

На первом шаг необходимо выбрать язык мастера установки, доступно 6 языков

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. Задайте учетные записи
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

Установка Web Console



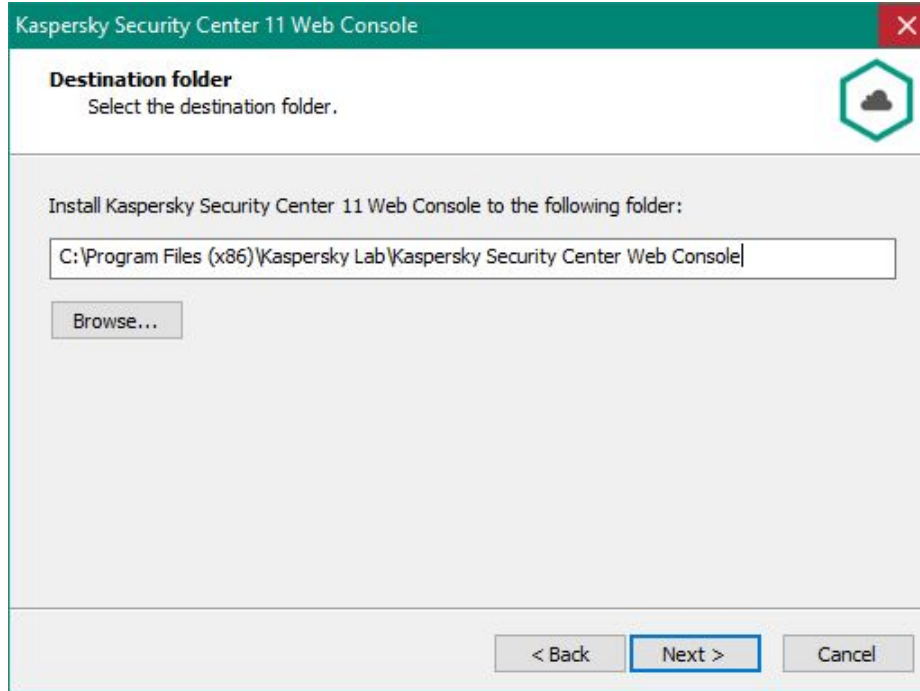
На следующем шаге необходимо принять лицензионное соглашение

Затем смотрим какие языки локализации Web Console доступны в инсталляторе, также можно подготовить и подгрузить любой язык в JSON-формате.

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. Задайте учетные записи
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

Установка Web Console



Kaspersky Security Center 11 Web Console

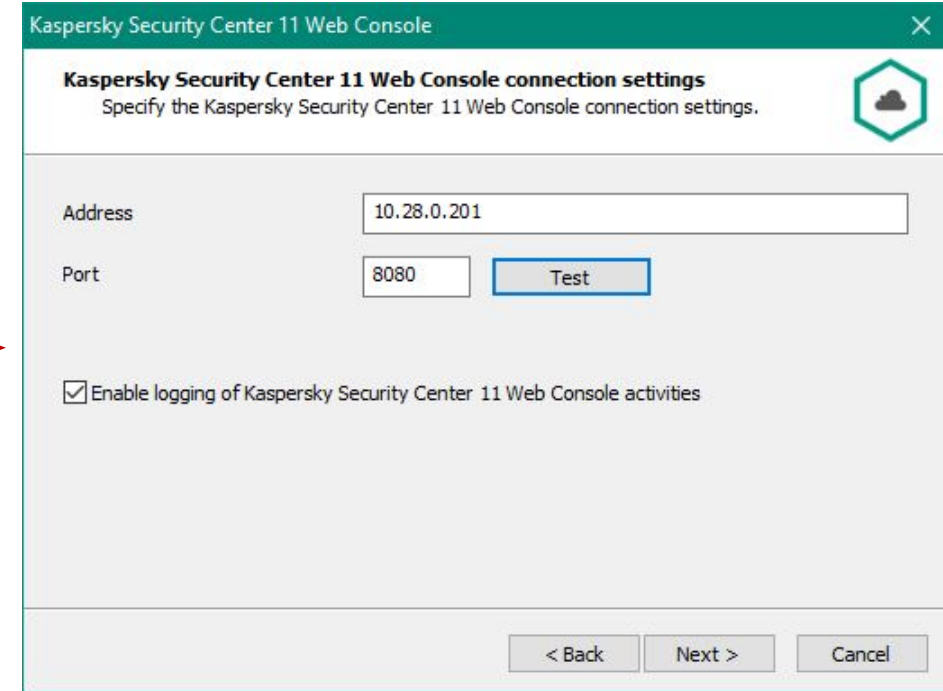
Destination folder
Select the destination folder.

Install Kaspersky Security Center 11 Web Console to the following folder:

C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center Web Console

Browse...

< Back Next > Cancel



Kaspersky Security Center 11 Web Console

Kaspersky Security Center 11 Web Console connection settings
Specify the Kaspersky Security Center 11 Web Console connection settings.

Address 10.28.0.201

Port 8080 Test

☒ Enable logging of Kaspersky Security Center 11 Web Console activities

< Back Next > Cancel

Далее необходимо указать путь установки, рекомендуется оставить по умолчанию

Затем надо указать адрес и порт, которые будут использоваться для подключения к Web Console

Говорят, что к релизу порт 8080 должен будет измениться на 443.

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. **Задайте учетные записи**
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

Установка Web Console

Kaspersky Security Center 11 Web Console

Account settings
Specify the Kaspersky Security Center 11 Web Console account settings.

The Node.js account and update service account are required for starting and updating Kaspersky Security Center 11 Web Console. You can use the default accounts or specify custom ones.

☒ Use default accounts
☐ Specify custom accounts

< Back Next > Cancel



Kaspersky Security Center 11 Web Console

Client certificate
Select how to specify the certificate:

☒ Generate new certificate
Make sure the below domain is trusted.
Domain: ABC

☐ Choose existing certificate
CRT certificate file: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Se Browse...
PEM certificate file: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Se Browse...
Certificate password (optional):

< Back Next > Cancel

По умолчанию, службы Web Console будут запускаться под системными учетными записями, но можно задать свои

Следующий шаг это создание сертификата веб-сервера, на котором будет крутиться Web Console. Сертификат будет генерироваться автоматически или можно подложить свой.

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. Задайте учетные записи
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

Установка Web Console

Kaspersky Security Center 11 Web Console

Trusted Administration Servers
Specify the settings of trusted Administration Servers.

You must create a list of trusted Administration Servers entitled to connect to Kaspersky Security Center 11 Web Console. After installation, Kaspersky Security Center 11 Web Console will only connect to the Administration Servers listed below. You can start the installer in Modify mode to edit the list of Administration Servers after installation.

List of trusted Administration Servers

Address	Port	Certificate
---------	------	-------------

Add
Delete
Edit

< Back Next > Cancel



Edit Administration Server

Administration Server name: SECURITY-CENTER

Administration Server address: localhost

Administration Server port: 13299

Administration Server certificate: C:\ProgramData\Kaspersky Browse

Update Cancel

На этом шаге администратор указывает с какими Kaspersky Security Center сможет взаимодействовать Web Console

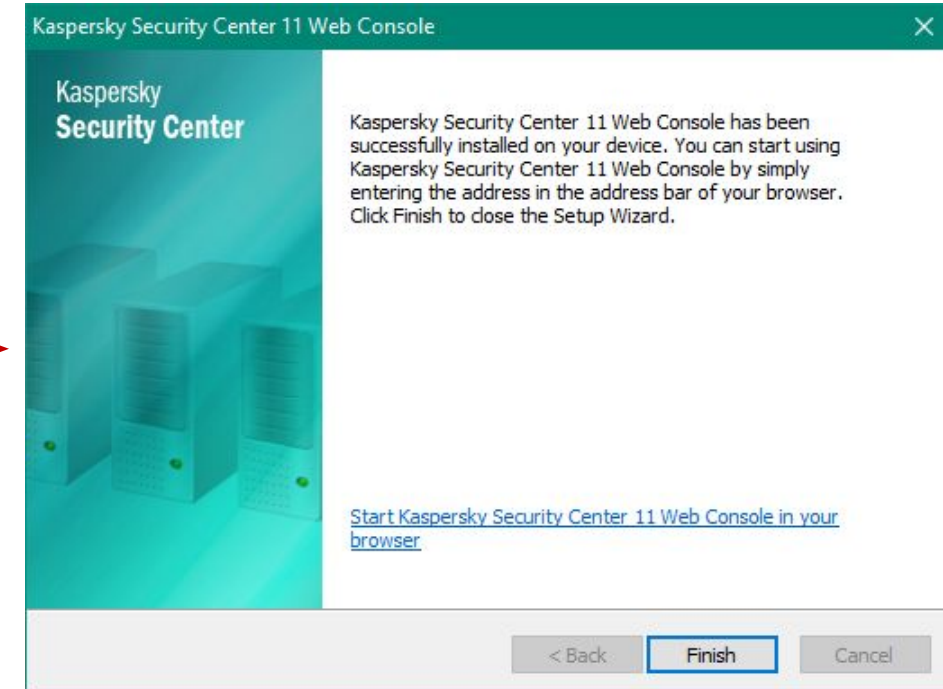
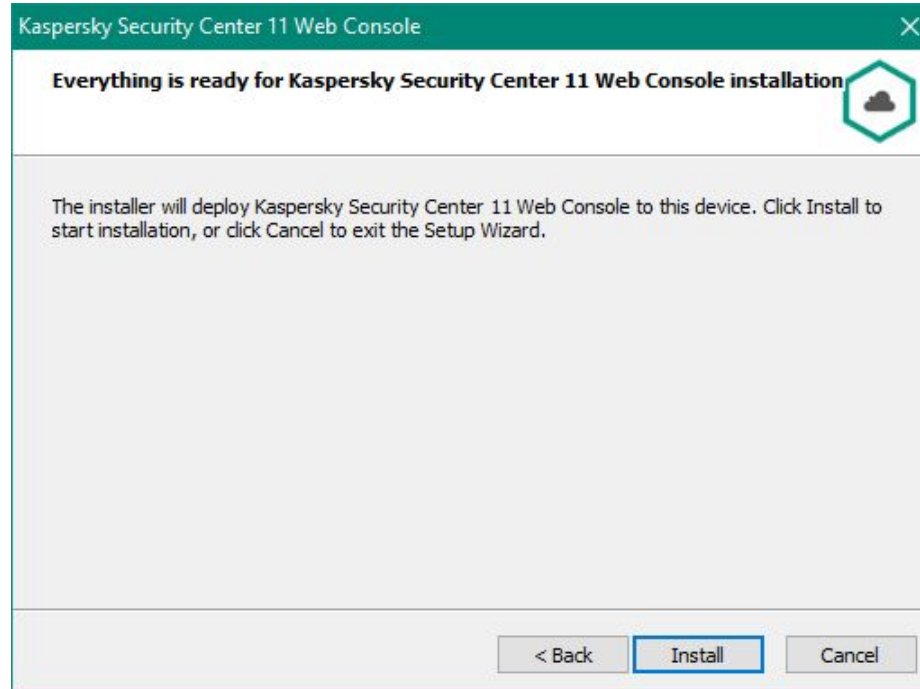
Если Web Console ставится на компьютер, на котором уже установлен KSC, то этот KSC автоматически появится в списке

Порт Сервера администрирования, по умолчанию 13299, но его можно изменить в свойствах Сервера

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Выберите язык
4. Укажите путь установки
5. Укажите параметры подключения к Web Console
6. Задайте учетные записи
7. Выберите сертификат
8. Укажите параметры подключения к Kaspersky Security Center
9. Запустите установку
10. Завершите установку – запустите KSC 11 Web Console

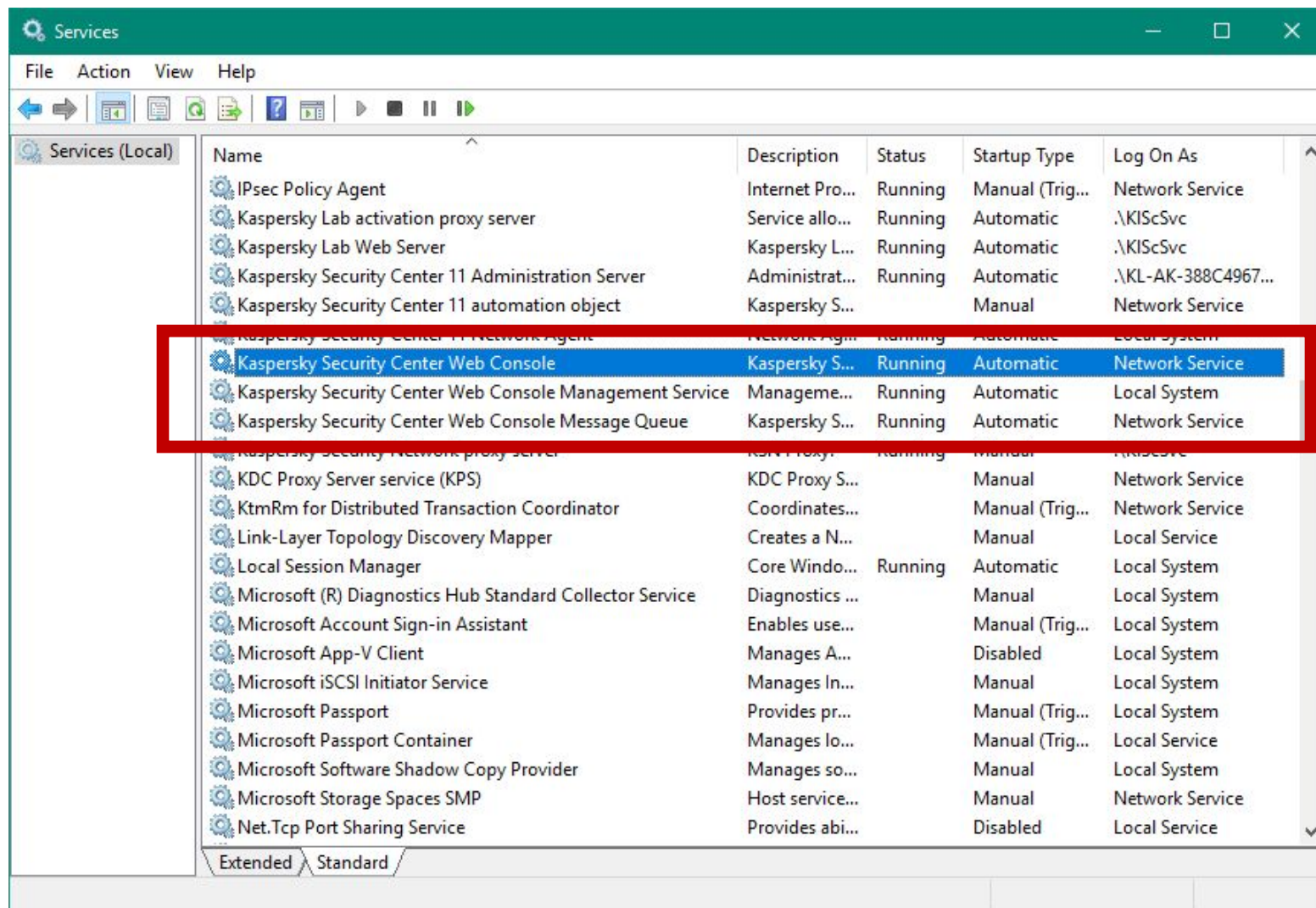
Установка Web Console



Предпоследний шаг – это запустить процесс установки кнопкой Install.

Ну и последний шаг – запустить Web Console и завершить мастер или просто завершить мастер.

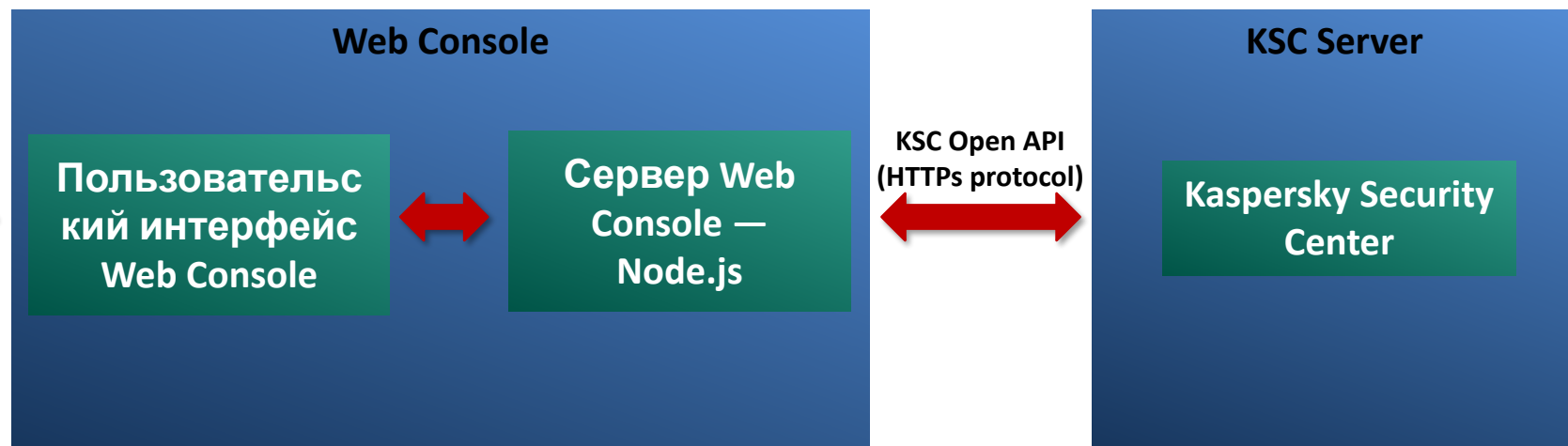
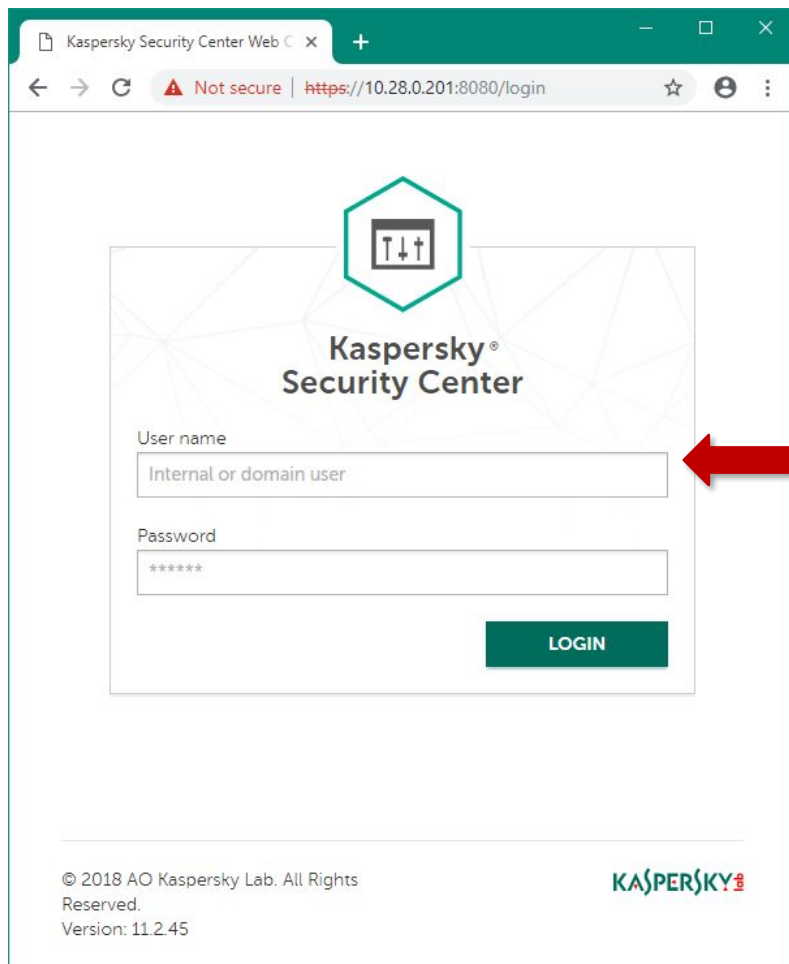
Службы Web Console



В процессе установки Web Console устанавливаются следующие службы:

- Kaspersky Security Center Management Service
- Kaspersky Security Center Web Console
- Kaspersky Security Center Web Console Message Queue — платформа для обработки очереди сообщений на базе NSQ

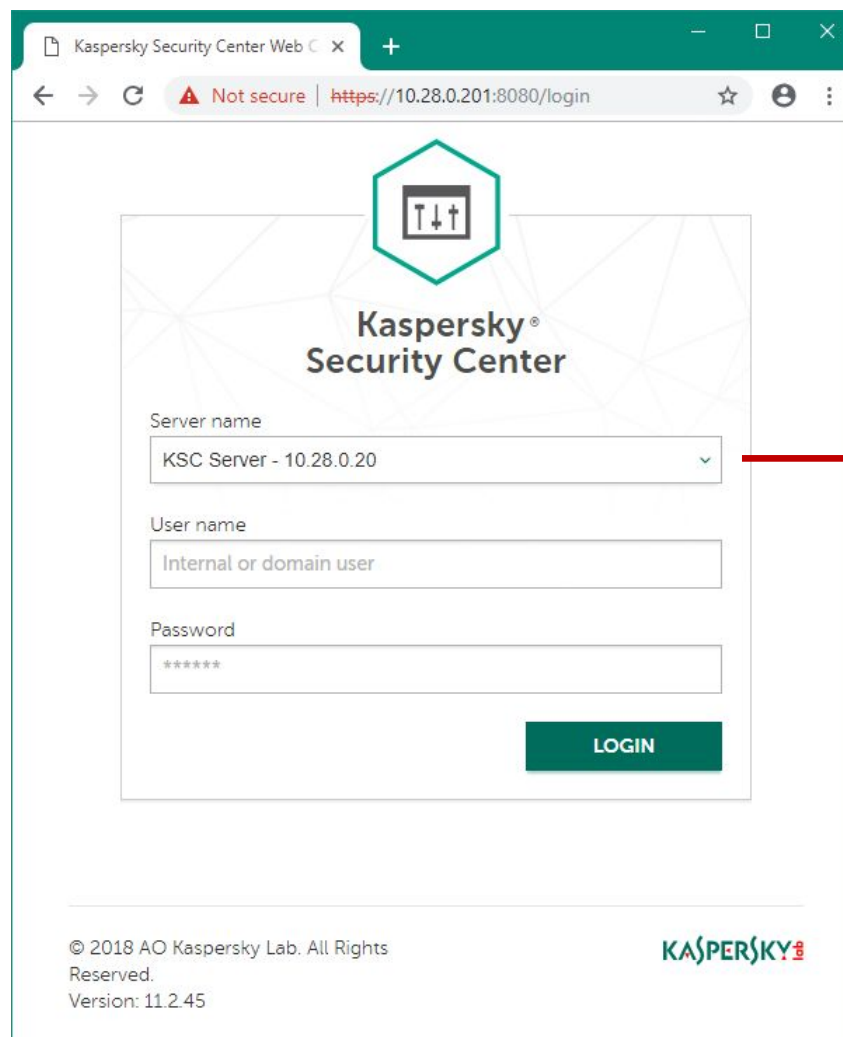
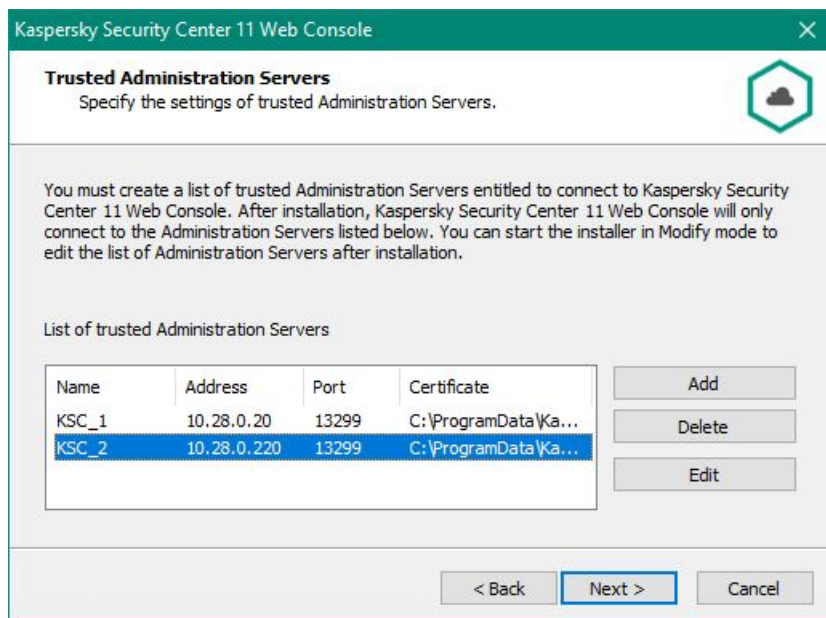
Web Console: взаимодействие



Подключение к нескольким KSC

Запустить **Update** в мастере удаления программы

Если Web Console видит, что у нее больше одного доверенного сервера, то на странице входа появится дополнительное поле **Server name**

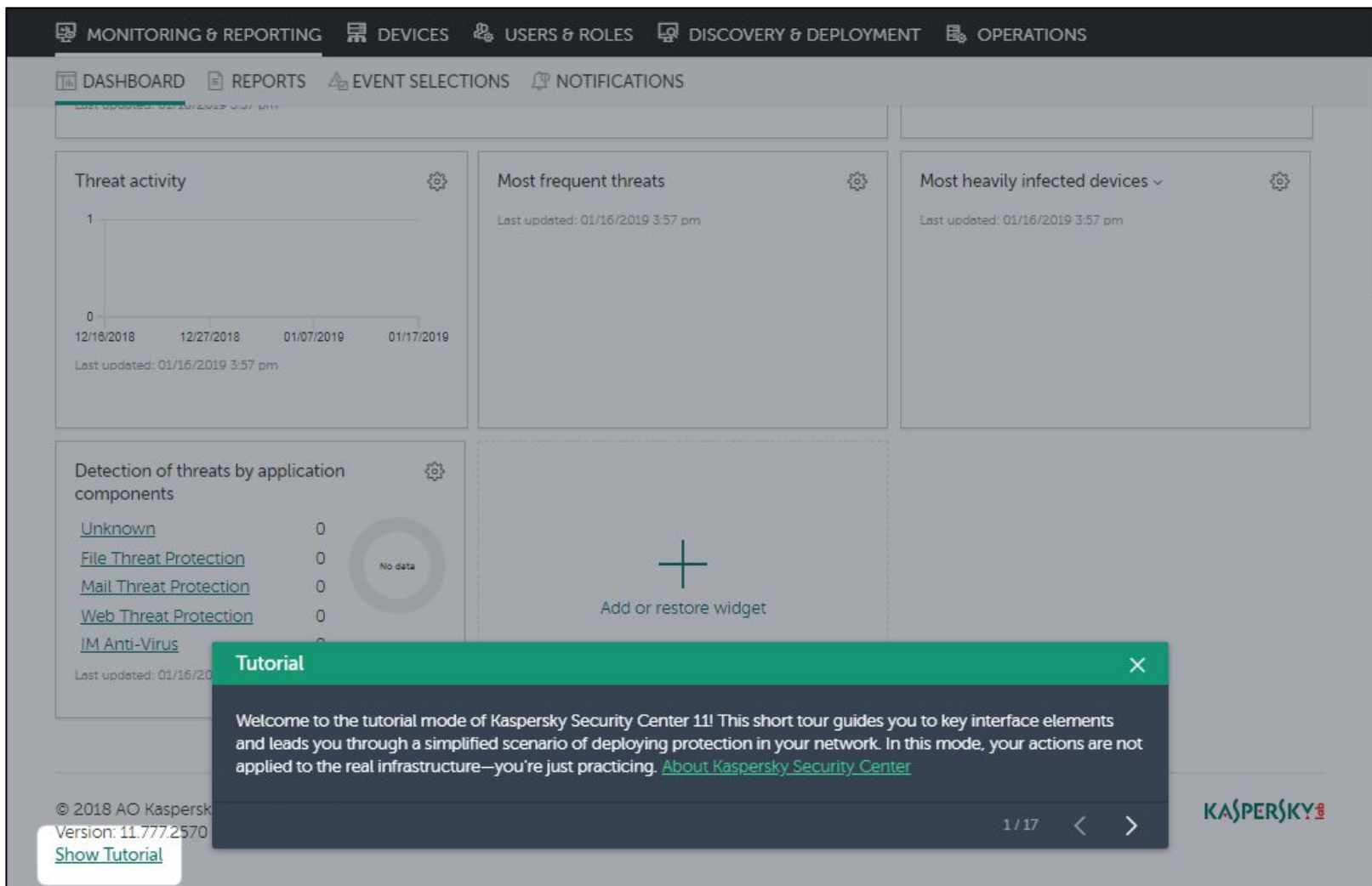


Trusted servers
KSC Server - 10.28.0.20
KSC Server - 10.28.0.200

Требования к браузерам для работы с Web Console

- Поддерживаемые браузеры:
 - Google Chrome
 - Mozilla Firefox
 - Safari

Где что в Kaspersky Security Center Web Console?



При первом подключении к Web Console выскакивает **Tutorial**

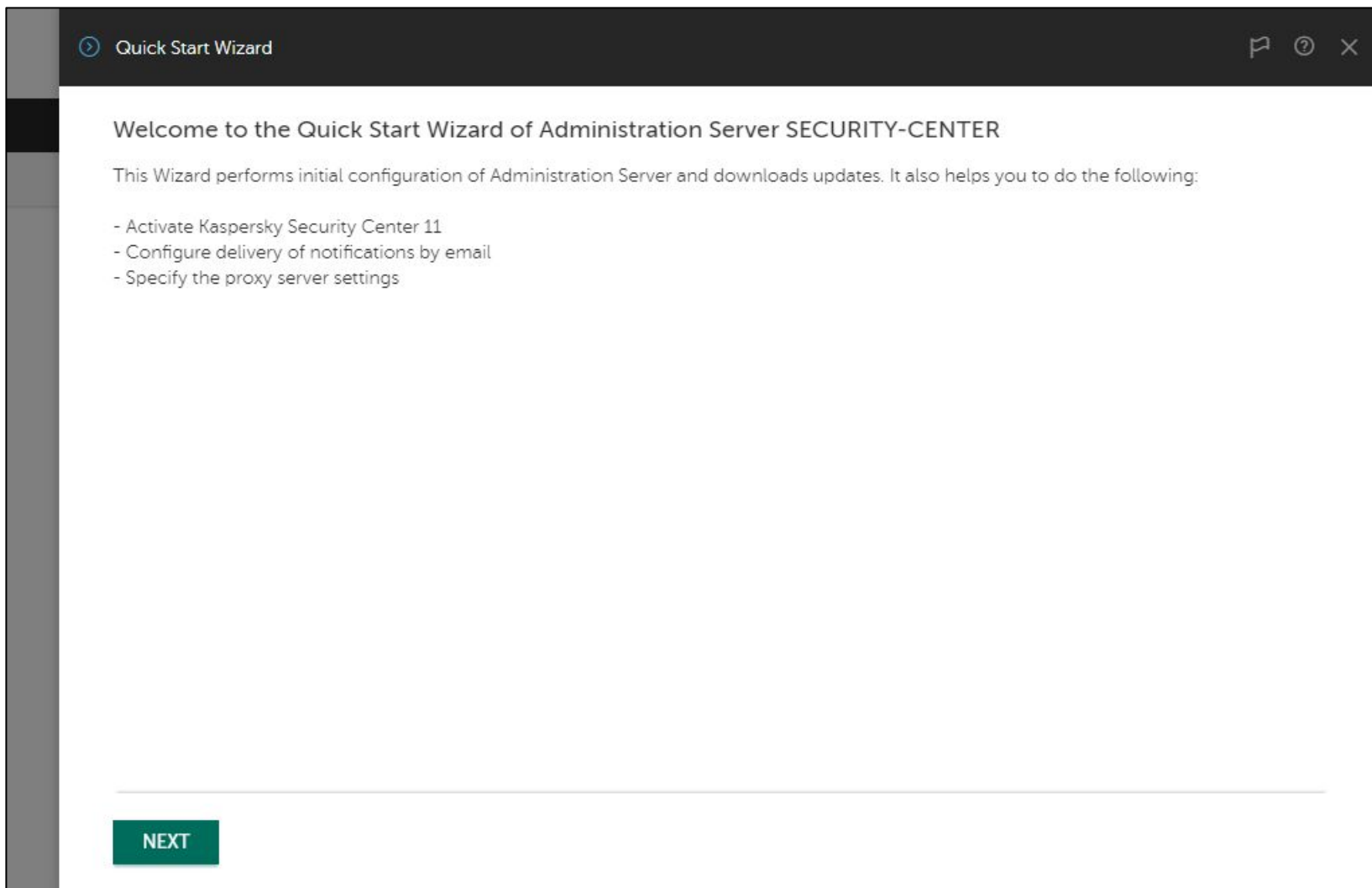
Это 17 шагов, которые рассказывают, где что находится в Web Console

Мы рекомендуем ознакомиться с этим **Tutorial**

Если вы случайно закрыли Tutorial или хотите еще раз ознакомиться с ним, в главном окне внизу есть ссылка **Show Tutorial**

При первом подключении после закрытия **Tutorial** запускается **Quick Start Wizard**

Мастер первоначальной настройки



Мастер первоначальной настройки запускается после первого подключения к серверу и готовит сервер к работе:

- Создает задачи и политики
- Загружает обновления в хранилище на Сервере администрирования

Мастер просит администратора:

- Настроить подключение к Интернет
- Добавить лицензию
- Принять соглашение Kaspersky Security Network
- Указать почтовый адрес, на который будут приходить отчеты и уведомления

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Настройка доступа в Интернет

Quick Start Wizard

Internet connection required

☐ Use proxy for Internet access

Proxy server address

Proxy server port

☐ Bypass proxy server for local addresses

☐ Proxy server authentication

User name

Password SHOW

BACK NEXT

Укажите параметры прокси-сервера для доступа в Интернет, или пропустите этот шаг, если для доступа в Интернет прокси-сервер не используется

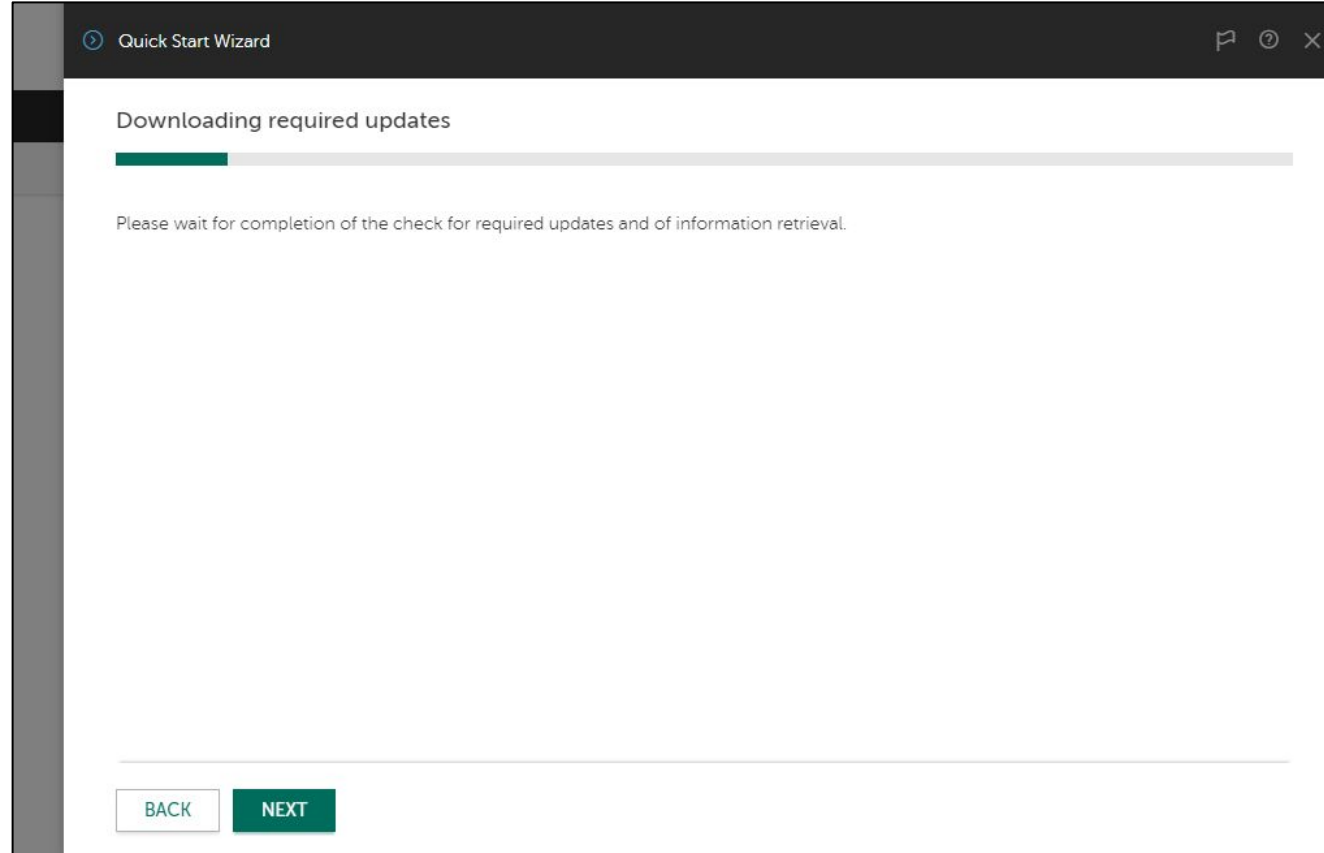
Доступ в Интернет нужен:

- Чтобы загружать обновления
- Чтобы перенаправлять запросы в Kaspersky Security Network от клиентских компьютеров, когда Сервер администрирования выступает в роли KSN Proxy

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Загрузка обновлений



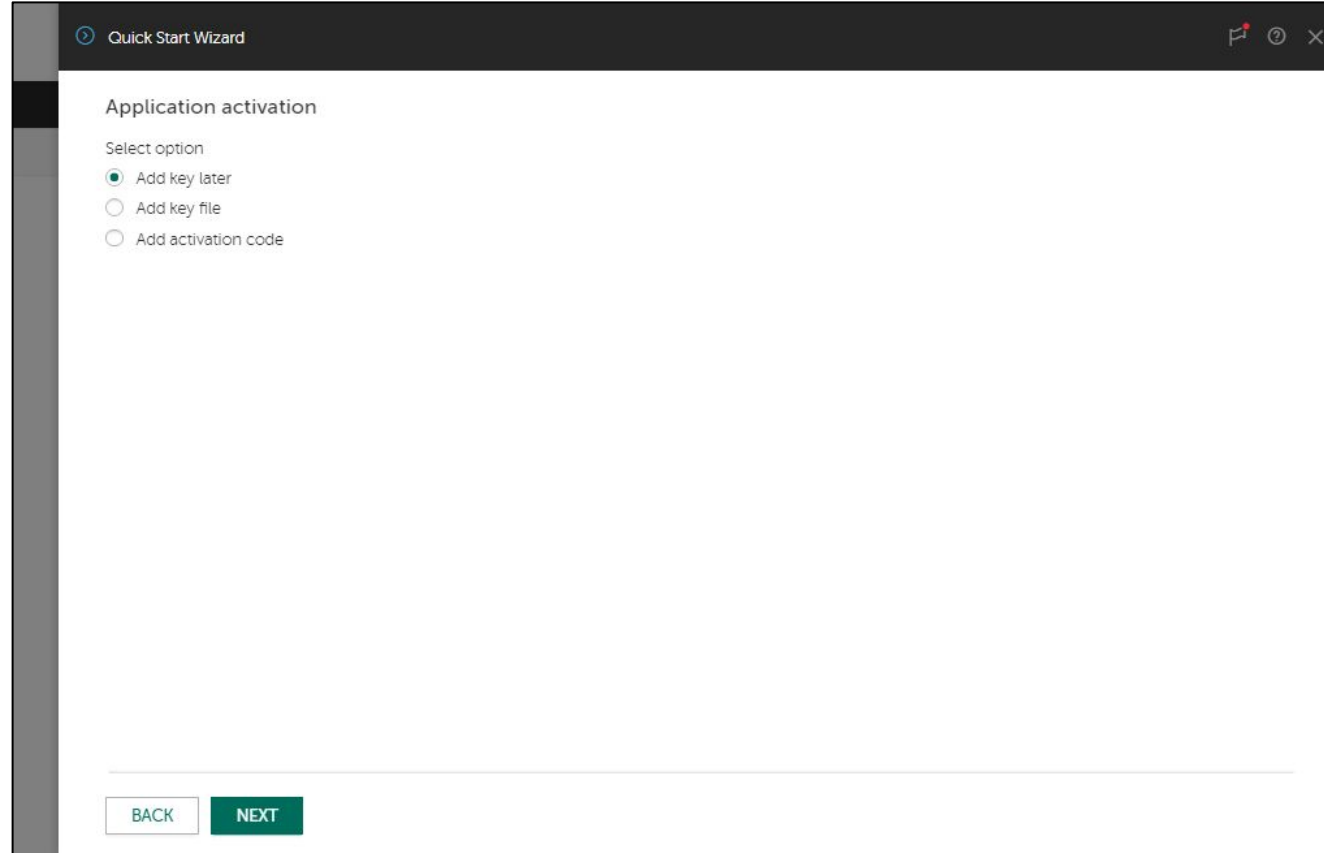
Сервер администрирования автоматически загружает обновления для продуктов, инсталляционные пакеты которых есть в хранилище

Кнопка **Next** не прерывает обновление

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. **Добавьте лицензию**
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Выбор лицензии



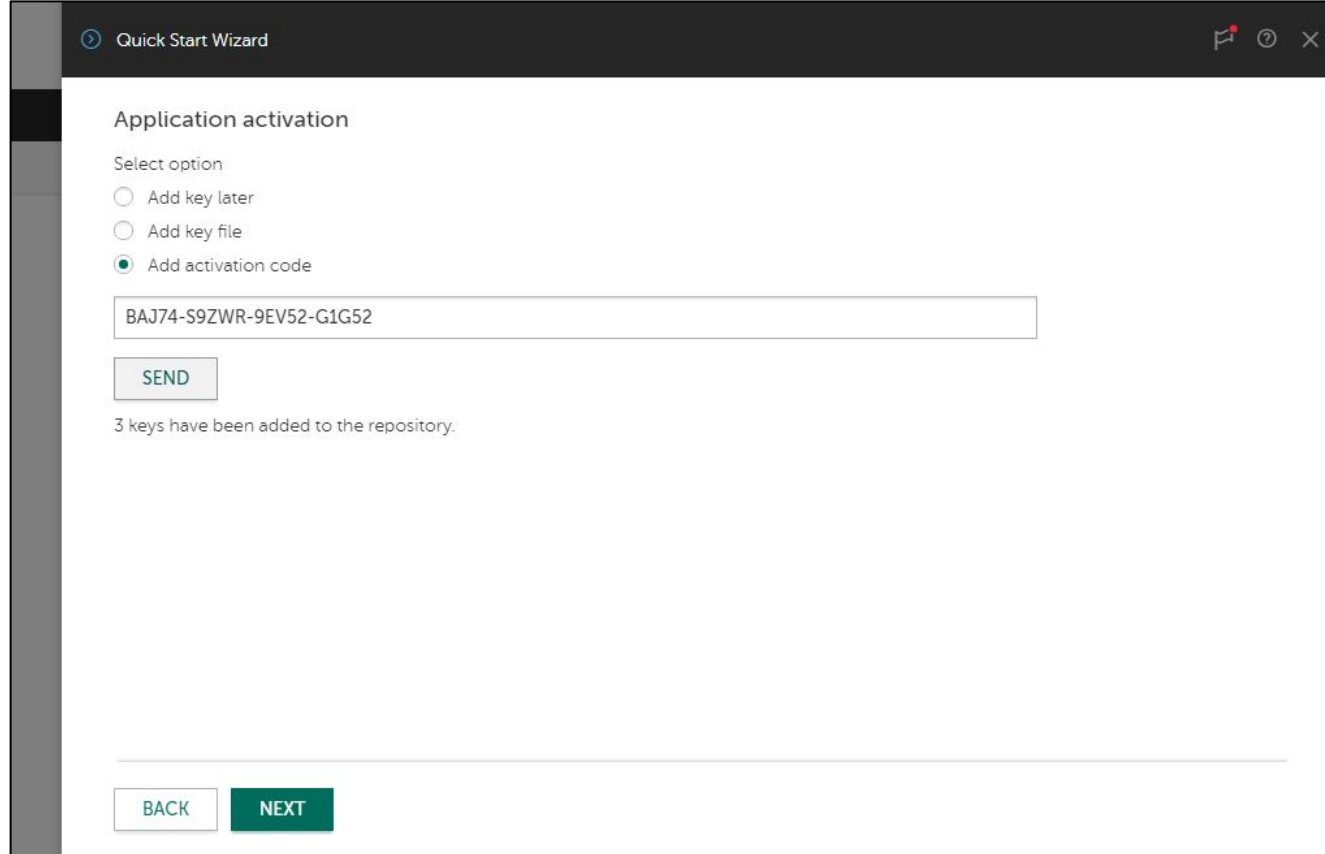
Активируйте Сервер администрирования лицензией в виде кода активации или файла-ключа

Либо пропустите этот шаг и активируйте Kaspersky Security Center позже

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. **Добавьте лицензию**
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Активация кодом



Quick Start Wizard

Application activation

Select option

☐ Add key later

☐ Add key file

☒ Add activation code

BAJ74-S9ZWR-9EV52-G1G52

SEND

3 keys have been added to the repository.

BACK NEXT

Для активации кодом нужен доступ в Интернет

Кодом можно активировать сразу и Сервер администрирования и Kaspersky Endpoint Security на компьютерах

Опция автоматически распространять лицензию на клиентские устройства отсутствует, но ее можно указать позднее, чтобы не выбирать лицензию в задачах удаленной установки

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. **Добавьте лицензию**
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Активация ключом

Quick Start Wizard

Application activation

Select option

☐ Add key later

☒ Add key file

☐ Add activation code

[SELECT KEY FILE](#)

Application name	Kaspersky Security for Storage, Server International Edition. 10-14 FileServer 1 year NFR License
Major version	
Licenses count	10
License term (days)	
License expiration date	09/02/2019 5:00 pm
Key type	Commercial

☒ Automatically deploy key to managed devices

This key is not valid for Kaspersky Security Center 11.

[BACK](#) [NEXT](#)

Если активировать Сервер администрирования ключом, позже нужно будет добавить на Сервер еще один ключ, чтобы активировать Kaspersky Endpoint Security

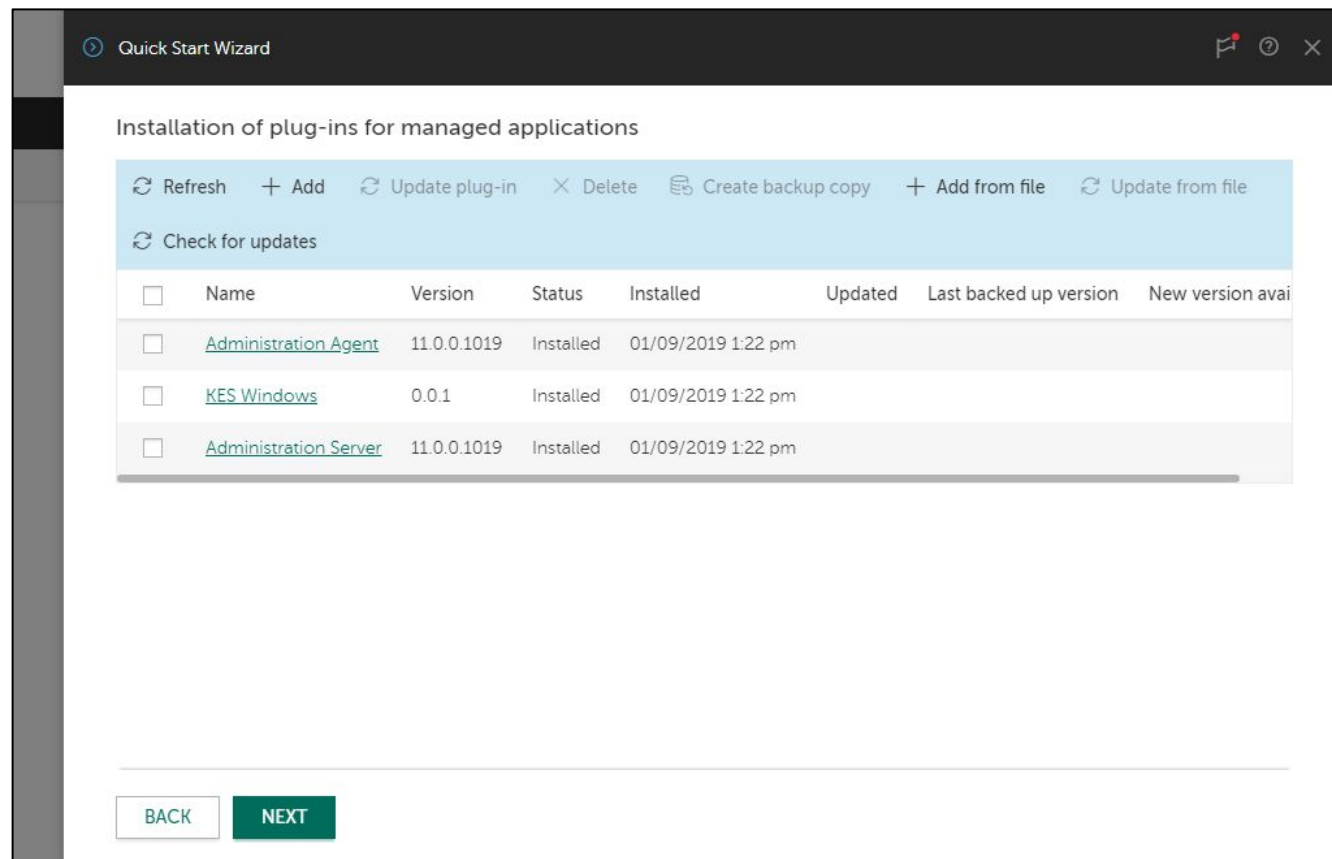
Используйте активацию ключом, если нет доступа в Интернет

В отличие от кода активации у ключа есть опция автоматического распространения

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Список установленных плагинов



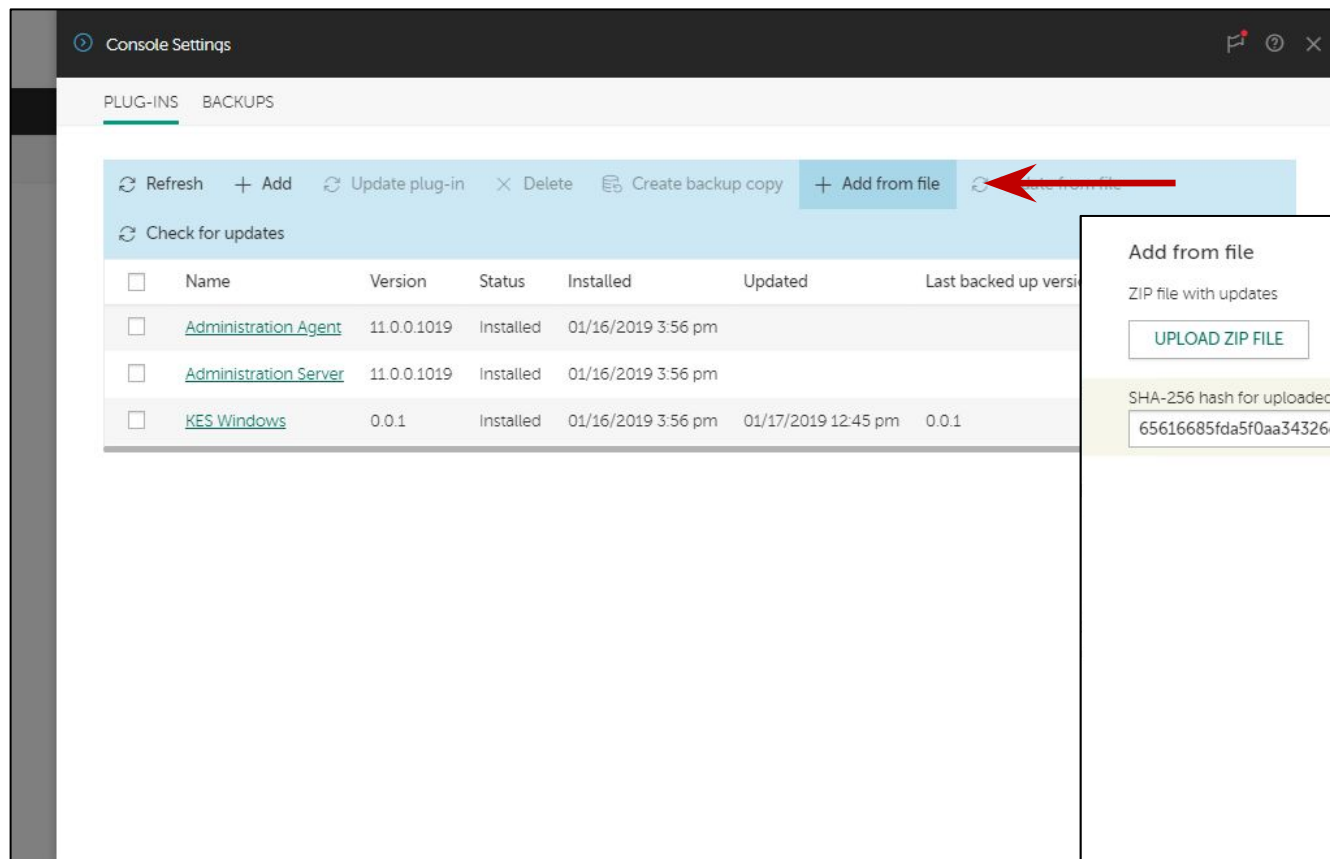
Мастер первоначальной настройки показывает список предустановленных плагинов

Также можно проверить есть ли другие доступные плагины или обновления для уже установленных

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Загрузка плагинов



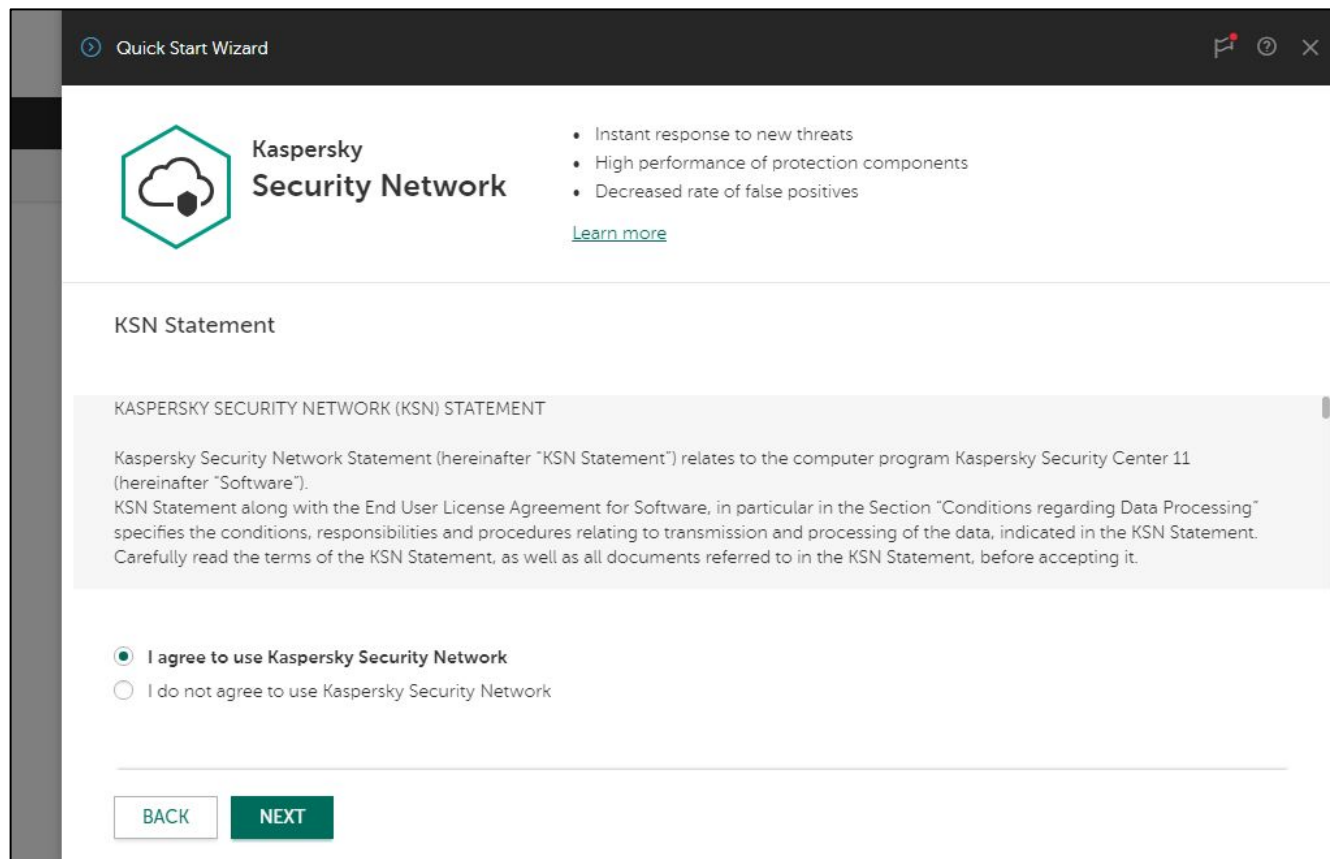
Также плагин можно добавить из файла, для этого нужно указать путь к zip-архиву и контрольную сумму



Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Kaspersky Security Network



Kaspersky Security Network (KSN) это постоянно обновляемая онлайн-база (в «облаке») репутаций исполняемых файлов и веб-ресурсов

Kaspersky Endpoint Security получает из KSN самую свежую информацию об угрозах и о файлах, которым можно доверять

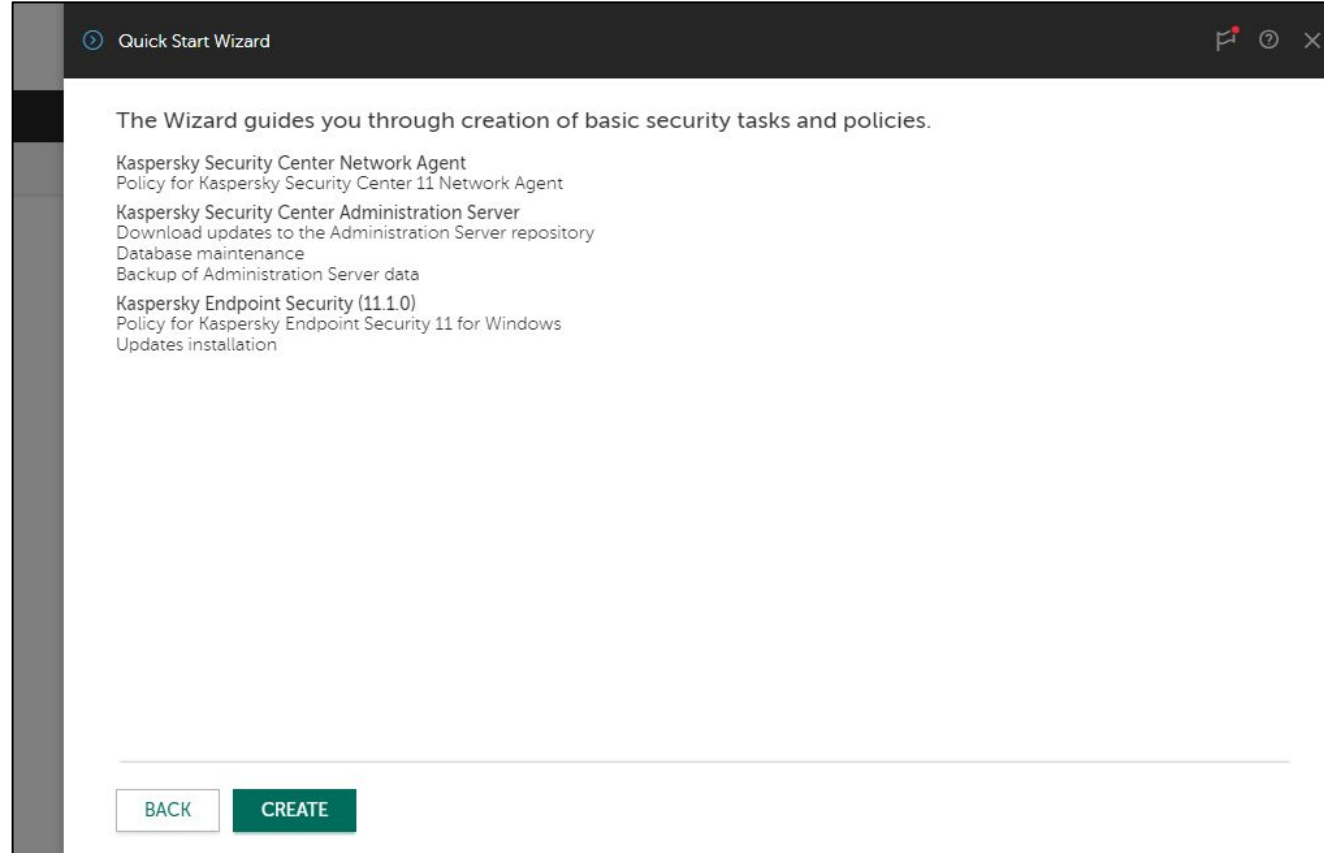
Принимая соглашение KSN, администратор включает KSN для Kaspersky Endpoint Security в политике по умолчанию и для KSC в свойствах сервера администрирования

Администратор всегда может включить или выключить KSN для любого продукта в настройках или политике продукта

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Создание задач и политик



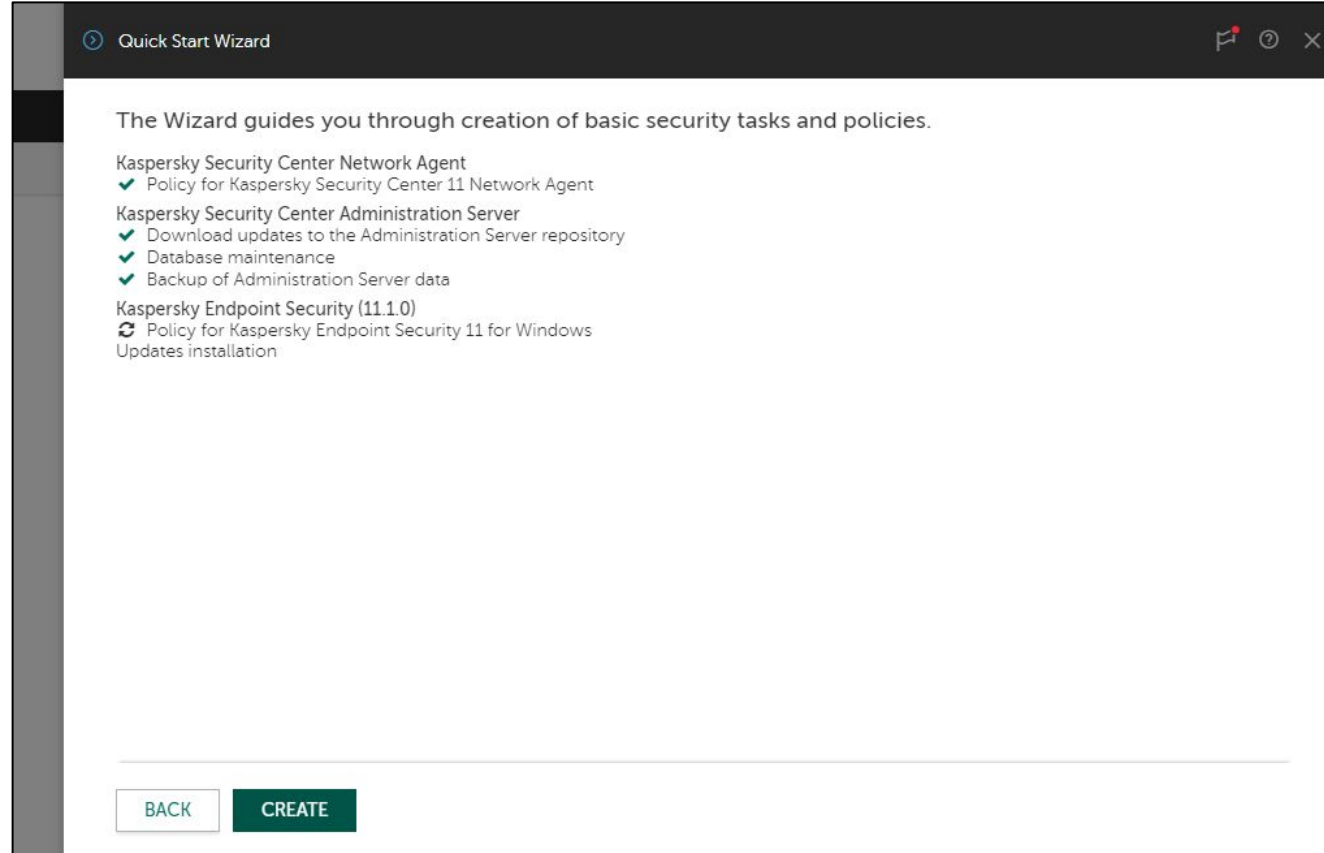
Мастер создает задачи Сервера администрирования:

- Загрузка обновлений в хранилище
- Обслуживание базы данных
- Резервное копирование данных Сервера администрирования

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Создание задач и политик



Мастер создает групповые политики:

- Агента администрирования KSC
- Kaspersky Endpoint Security for Windows

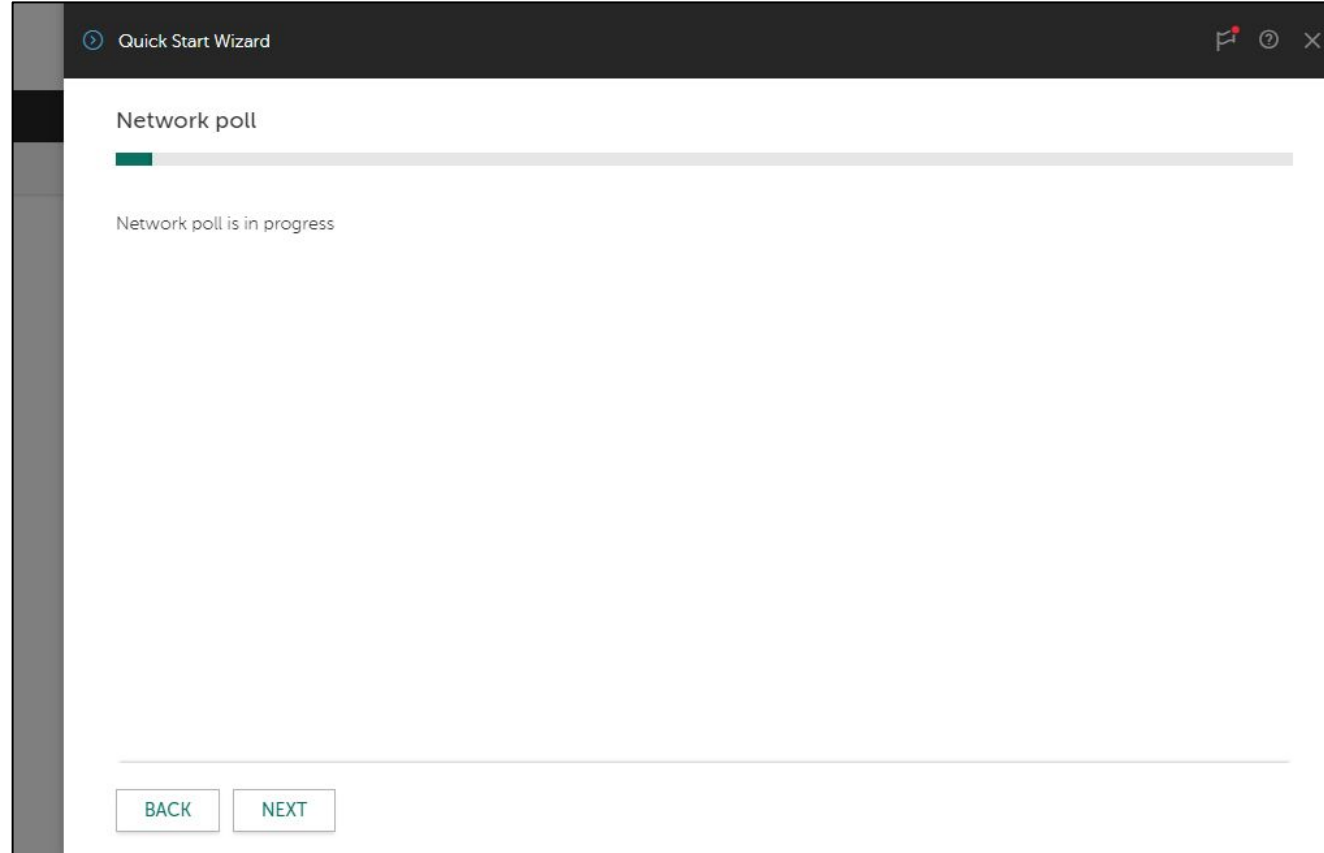
Групповые задачи:

- Установка обновлений

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Сканирование сети

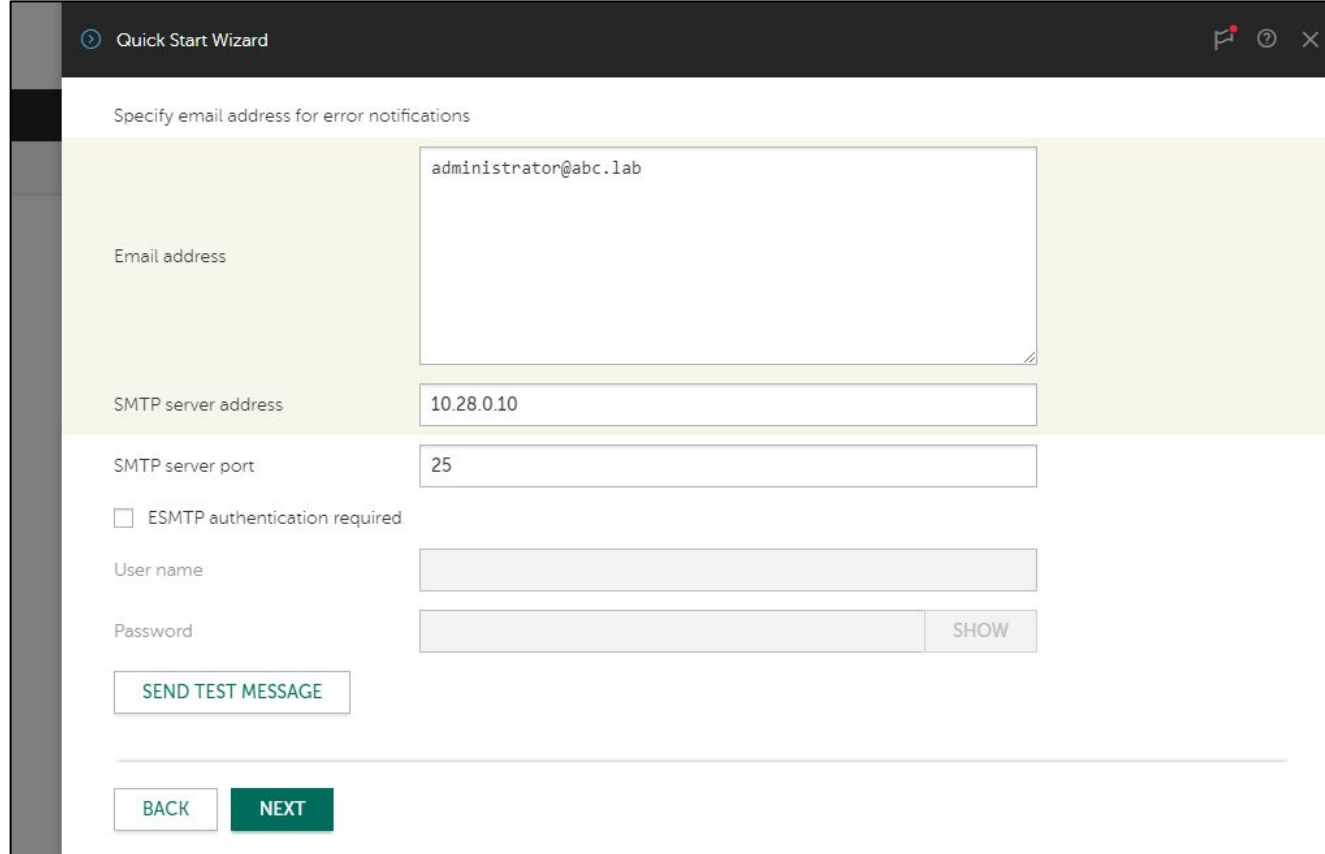


Мастер запускает сканирование сети средствами Microsoft Windows

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Настройка доставки почтовых уведомлений



The screenshot shows the 'Quick Start Wizard' window with the title 'Specify email address for error notifications'. The form contains the following fields and controls:

- Email address:** A text box containing 'administrator@abc.lab'.
- SMTP server address:** A text box containing '10.28.0.10'.
- SMTP server port:** A text box containing '25'.
- ESMTP authentication required:** An unchecked checkbox.
- User name:** An empty text box.
- Password:** An empty text box with a 'SHOW' button to its right.
- SEND TEST MESSAGE:** A button located below the password field.
- Navigation:** 'BACK' and 'NEXT' buttons at the bottom.

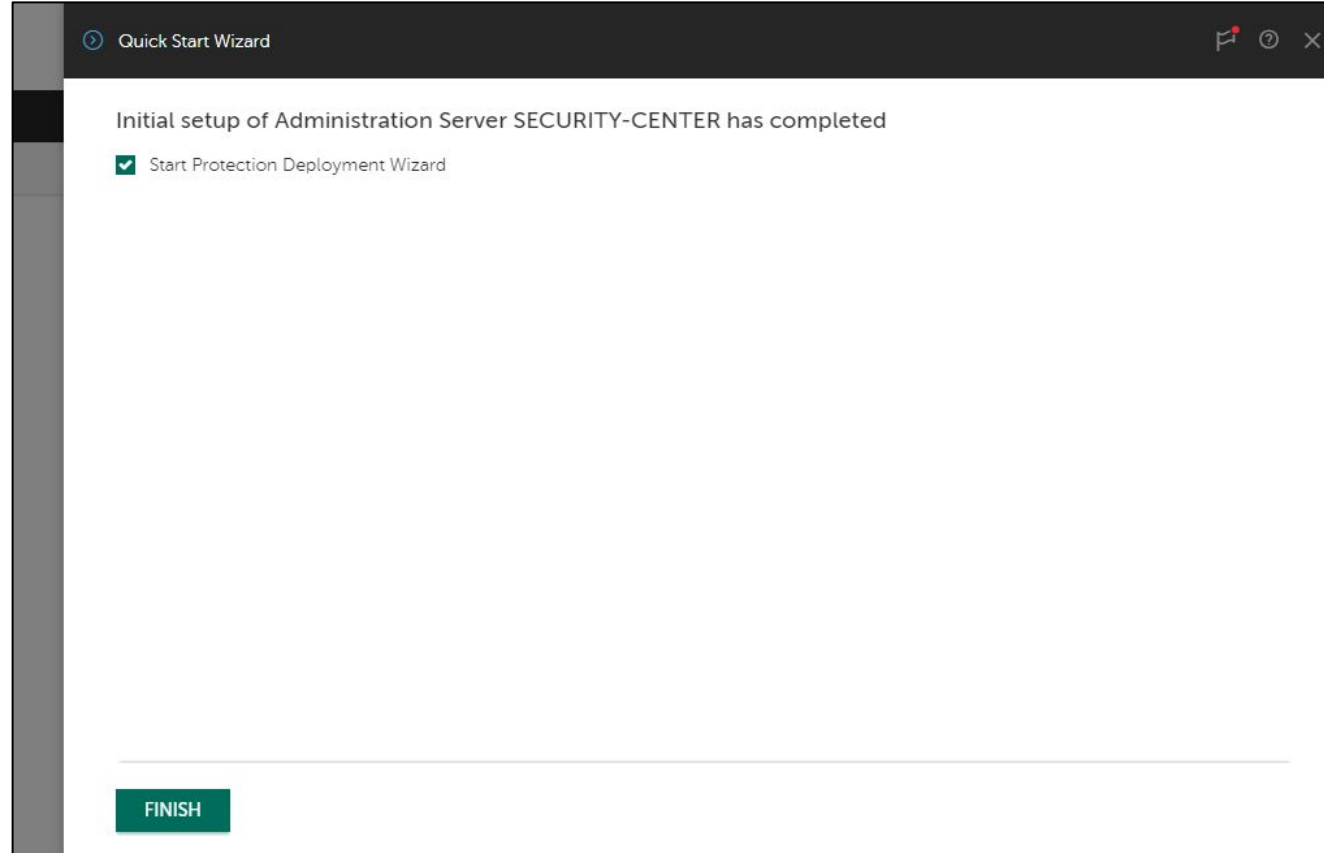
Параметры используются для доставки уведомлений и отчетов

Однако мастер не создает задачу рассылки отчетов, но ее можно создать вручную в любое время

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Завершение первоначальной настройки



Снимите отметку у параметра Start Protection Deployment Wizard

Не начинайте разворачивать защиту, пока не подготовитесь

Автоматическое распространение лицензии

Kaspersky Security Center ADMINISTRATION SERVER SECURITY-CENTER Console Settings ABC\Administrator

MONITORING & REPORTING DEVICES USERS & ROLES DISCOVERY & DEPLOYMENT OPERATIONS

LICENSING THIRD-PARTY APPLICATIONS REPOSITORIES KASPERSKY LAB APPLICATIONS

Application name	Key
☒ Kaspersky Endpoint Security for Business - Advanced International Edition. 10-14 Node 1 year NFR License: Kaspersky Security for WS and FS	250A-00045
☐ Kaspersky Endpoint Security for Business - Advanced International Edition. 10-14 Node 1 year NFR License: Security Center	250A-0003P
☐ Kaspersky Endpoint Security for Business - Advanced International Edition. 10-14 Node 1 year NFR License: Security Center	250A-0003P

+ Add × Delete ↻ Refresh Filter

250A-000451-57179582

GENERAL DEVICES

Key	250A-000451-57179582
Application name	Kaspersky Endpoint Security for Business - Advanced International Edition. 10-14 Node 1 year NFR License: Kaspersky Security for WS and FS
Key type	Commercial
License term (days)	365
License expiration date	02/18/2019 4:00 pm
Key expiration date	02/18/2019 4:00 pm
Limit	14
	☒ Deploy key automatically

© 2018 AO Kaspersky Lab. All Rights Reserved.
Version: 11.777.2570
[Show Tutorial](#)

Если в мастере первоначальной настройки добавлялся код активации, то после завершения мастера рекомендуется включить опцию автоматического распространения, чтобы не забыть



Лабораторная работа №1

Установка Веб-консоли Kaspersky Security Center

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



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

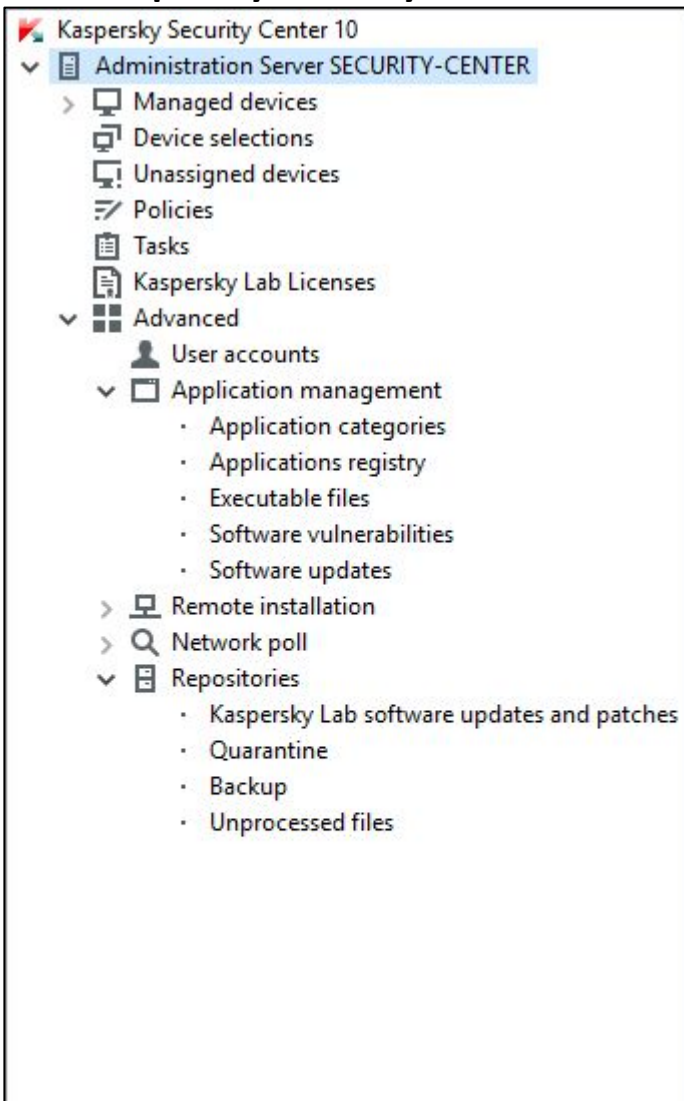
Проверка зашифрованного трафика

Защита от MAC Spoofing

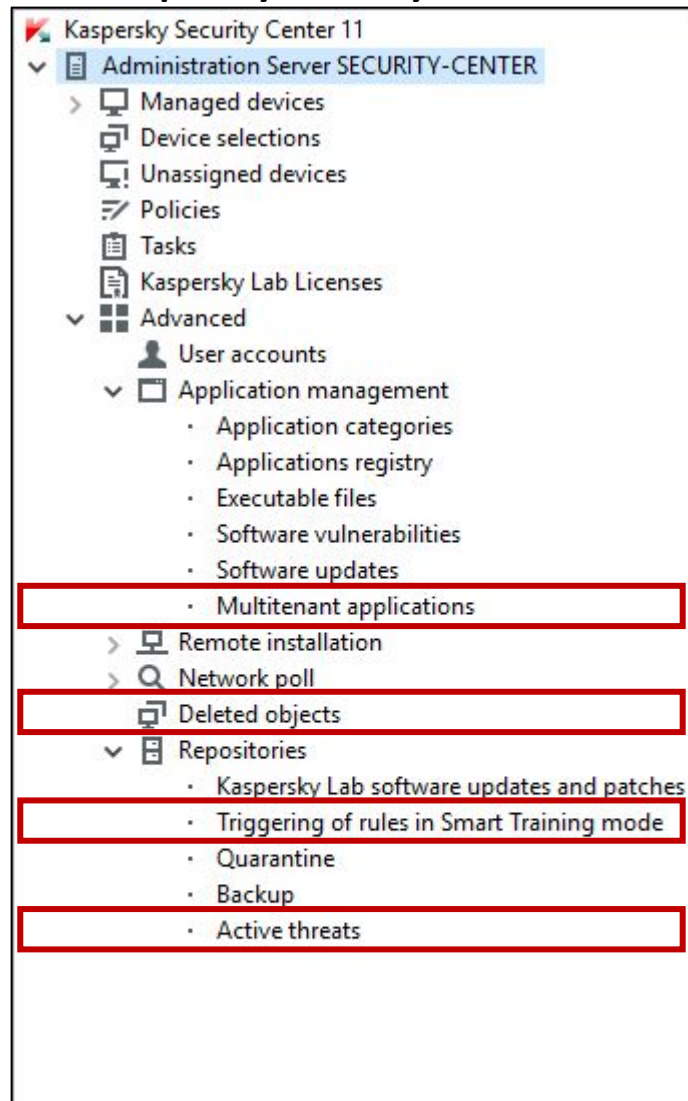
Role Based Access Control for KES

Kaspersky Security Center 11: изменения в интерфейсе

Kaspersky Security Center 10



Kaspersky Security Center 11



- Новые узлы в дереве консоли Сервера Администрирования:
 - Multitenant applications
 - Deleted objects
 - Triggering of rules in Smart Training mode
 - Active threats

Kaspersky Security Center 11: узел Deleted objects

Administration Server SECURITY-CENTER > Advanced > Deleted objects

Deleted objects

No filter specified, records total: 8

Type:

- Policy
- Task
- Installation package
- Virtual Administration Server
- User
- Security group
- Administration group

Name	Type	Time	User
Database maintenance	Task	10/26/2018 12:31:43 PM	ABC\Administrator
Deploy Kaspersky Security Center 11 Network Agent (11.0.0.887)	Task	10/26/2018 12:31:40 PM	ABC\Administrator
iOS MDM Server (11.0.0.887)	Installation package	10/25/2018 4:43:49 PM	ABC\Administrator
Jon Snow	User	10/26/2018 12:36:10 PM	ABC\Administrator
Kaspersky Endpoint Security for Windows (11.1.0) (1)	Policy	10/26/2018 12:31:31 PM	ABC\Administrator
Kaspersky Security Center Network Agent (1)	Policy	10/26/2018 12:31:29 PM	ABC\Administrator
Managed devices/Workstations/Test/	Administration group	10/25/2018 4:46:28 PM	ABC\Administrator
Microsoft Exchange Mobile Devices Server (11.0.0.887)	Installation package	10/25/2018 4:43:46 PM	ABC\Administrator

Database maintenance

Properties

Name: Database maintenance

Type: Task

Time: 10/26/2018 12:31:43 PM

User: ABC\Administrator

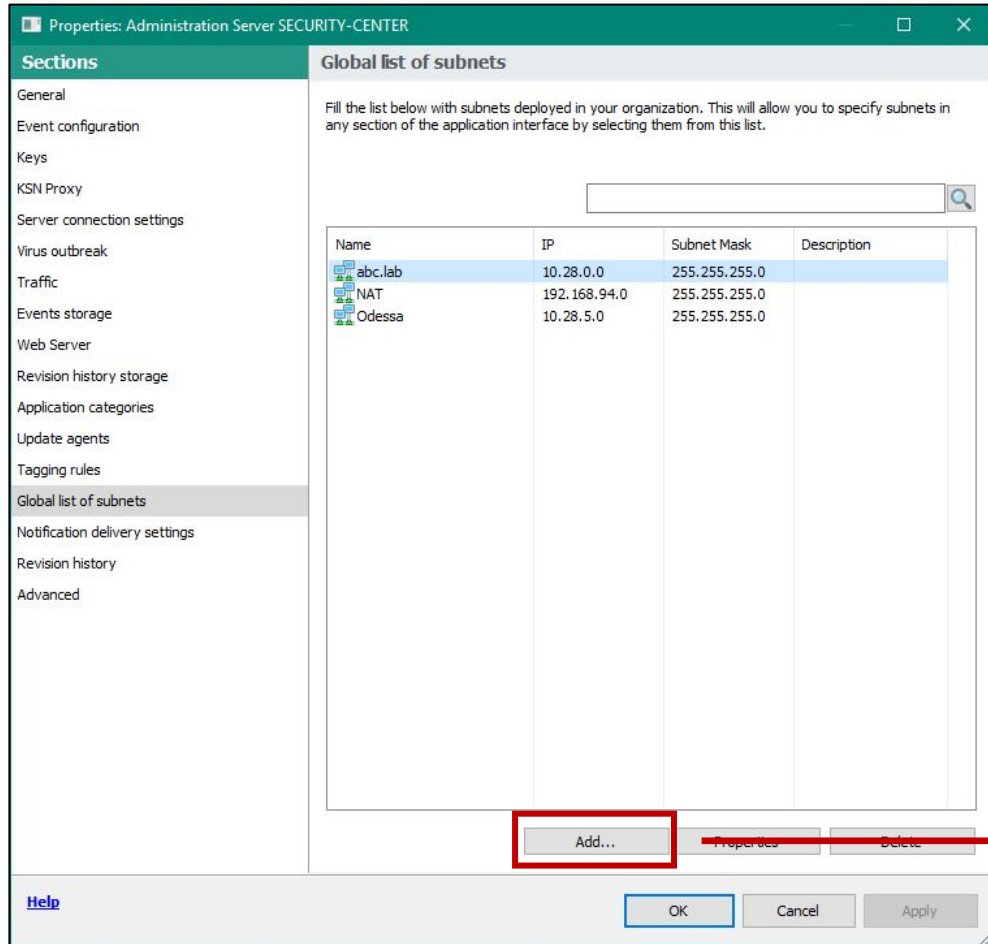
Actions

Properties

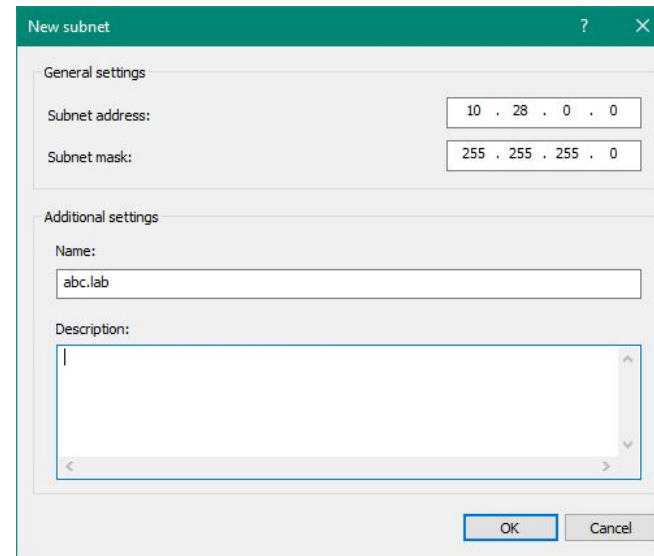
Delete

- В узел Deleted objects попадают все сущности, у которых есть ревизии:
- Policies
 - Tasks
 - Installation packages
 - Virtual Administration Servers
 - Users
 - Security groups
 - Administration groups

Kaspersky Security Center 11: Global list of subnets

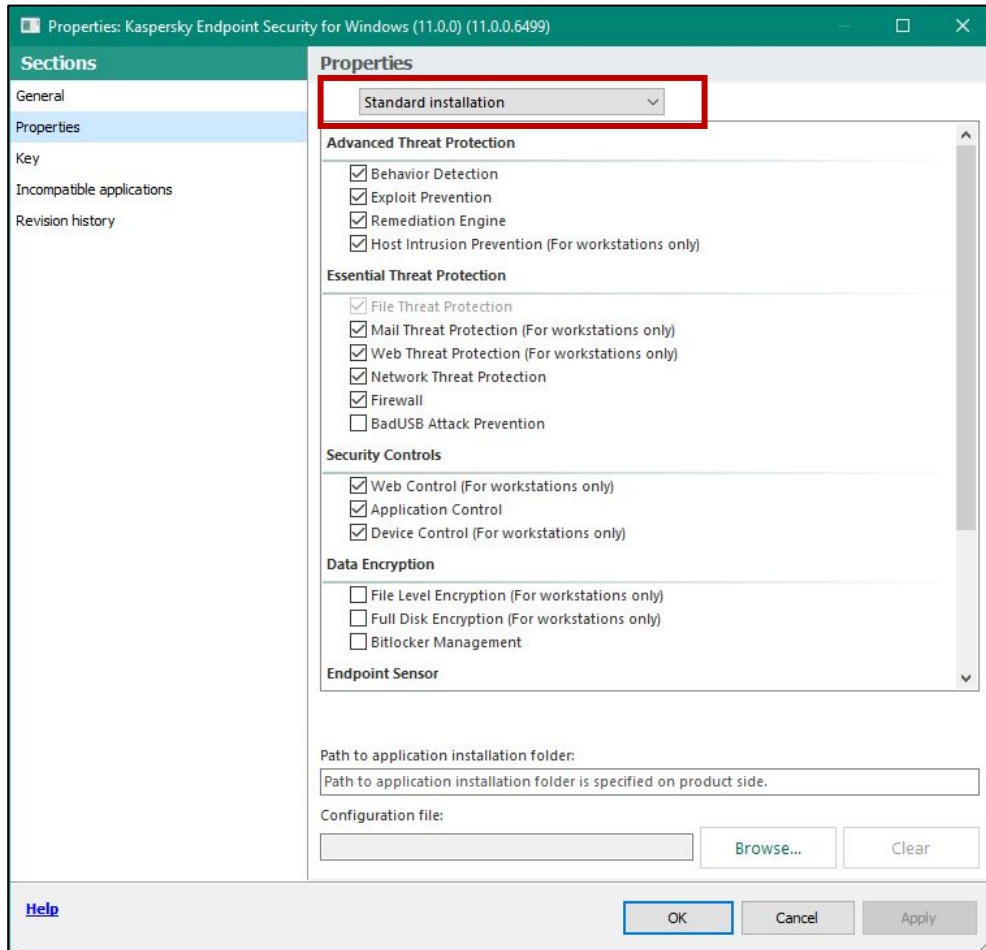


- Общий список подсетей, где можно задавать информацию о подсетях
- Список сквозной для KSC

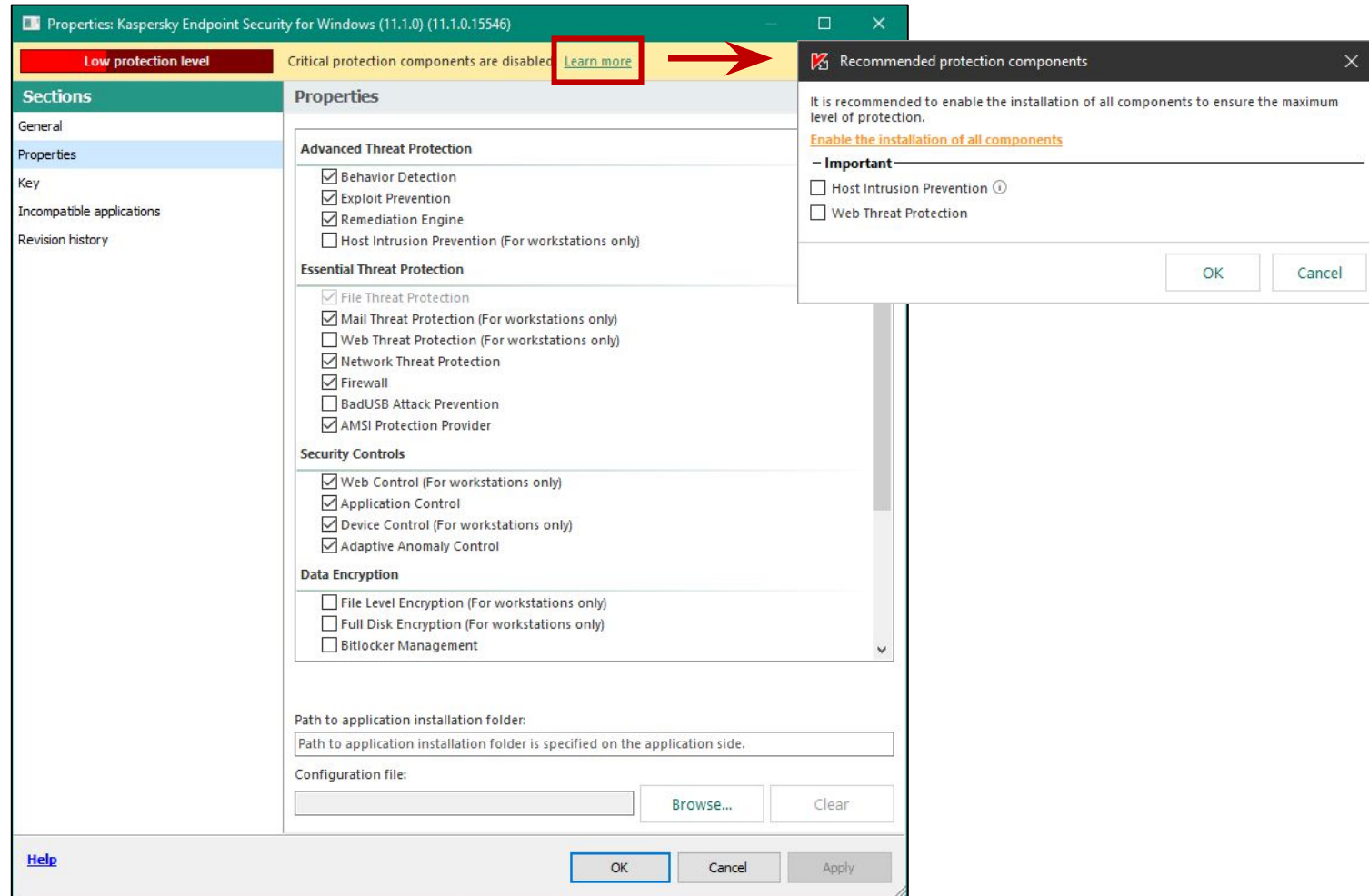


Инсталляционный пакет: индикатор уровня защиты

Kaspersky Security Center 10



Kaspersky Security Center 11





Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

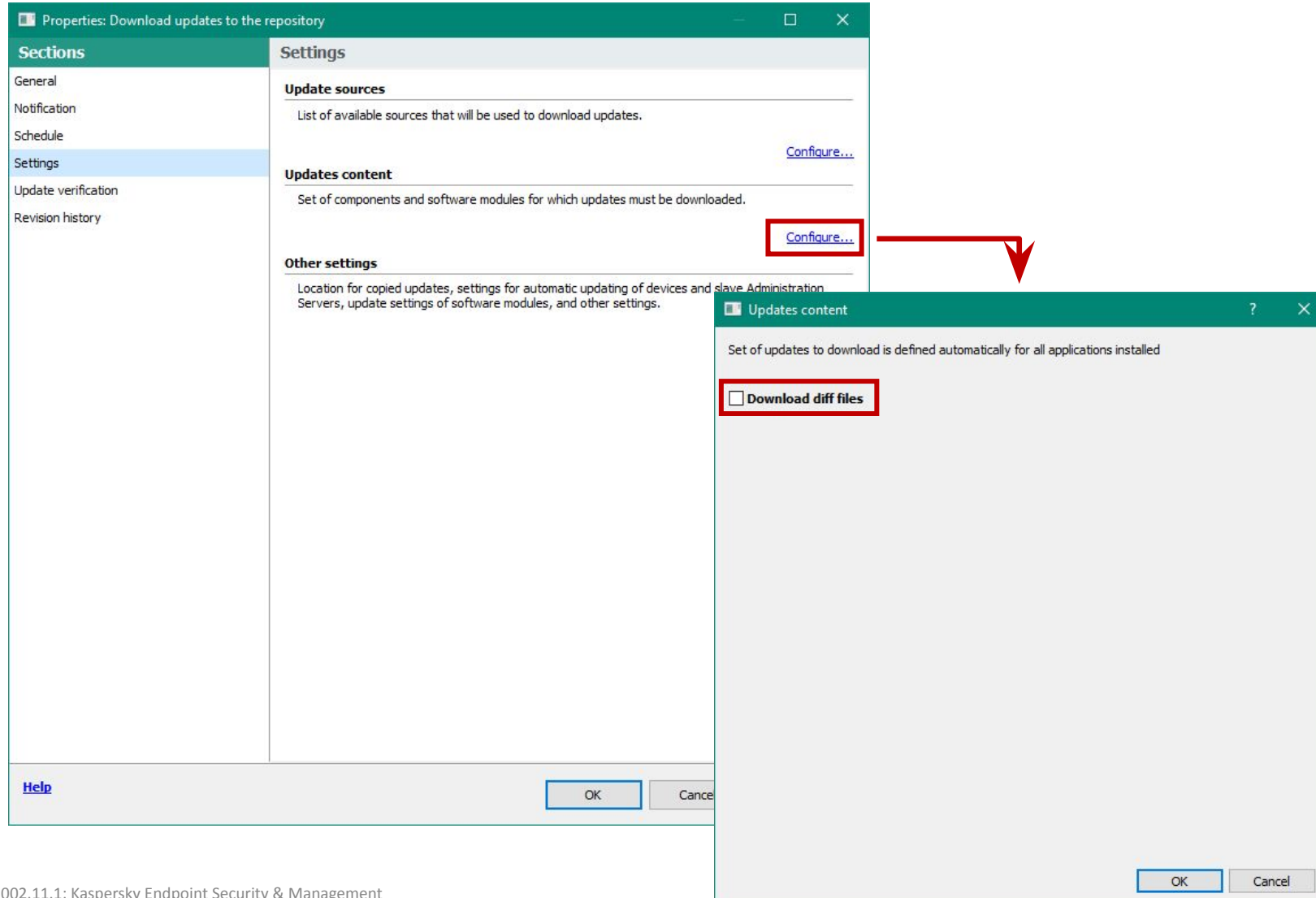
Компонент Adaptive Anomaly Control

Проверка зашифрованного трафика

Защита от MAC Spoofing

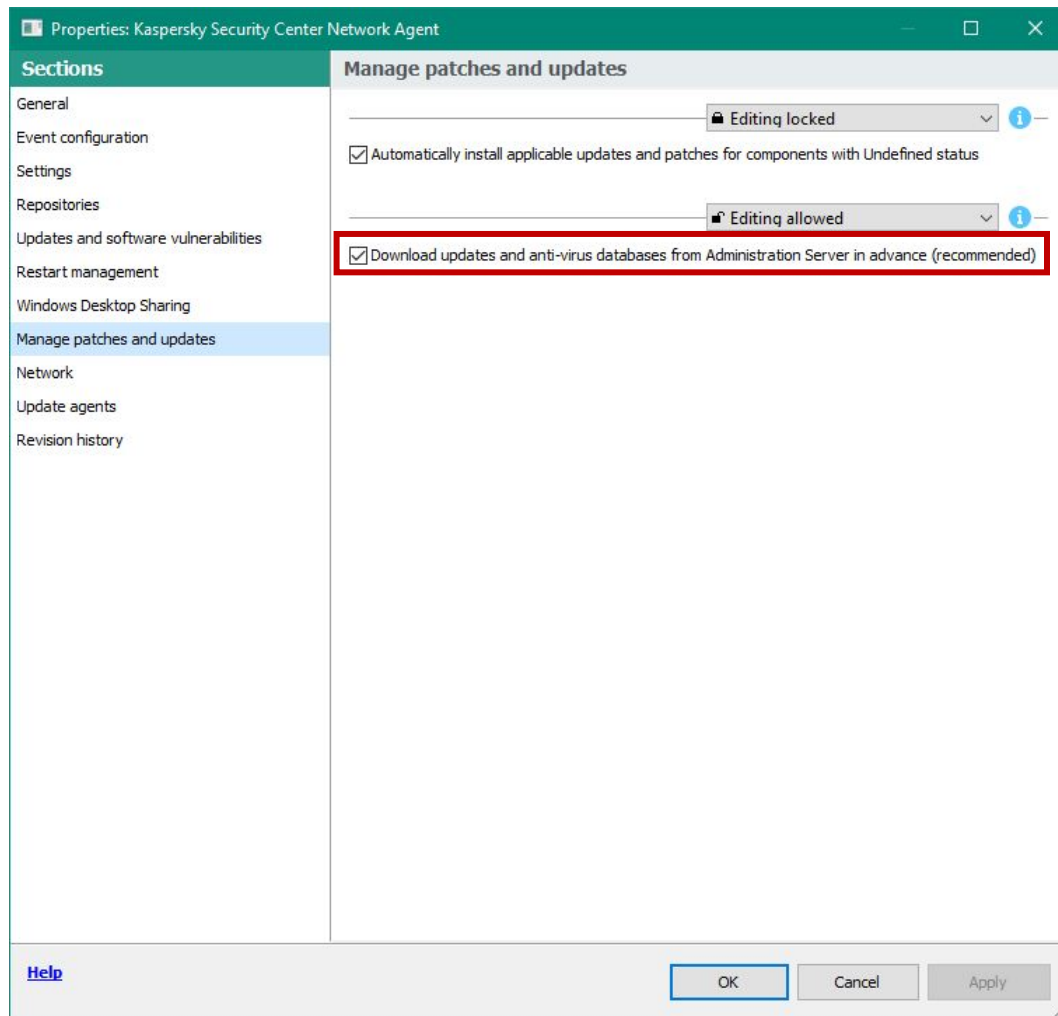
Role Based Access Control for KES

Kaspersky Security Center 11: поддержка DIFF-файлов обновлений



- Реализована поддержка DIFF-файлов для обновления баз угроз
- Обновление с помощью DIFF-файлов позволяет уменьшить внутренний сетевой трафик примерно в 20 раз

Агенты администрирования: поддержка DIFF-файлов обновлений



- Параметр загружать обновления заранее (offline-режим обновления) включен в политике Агента по умолчанию
- Ретрансляции DIFF-файлов **не работает** при включенном offline-режиме обновления
- DIFF-файлы обновлений не будут передаваться на старые версии Агентов



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

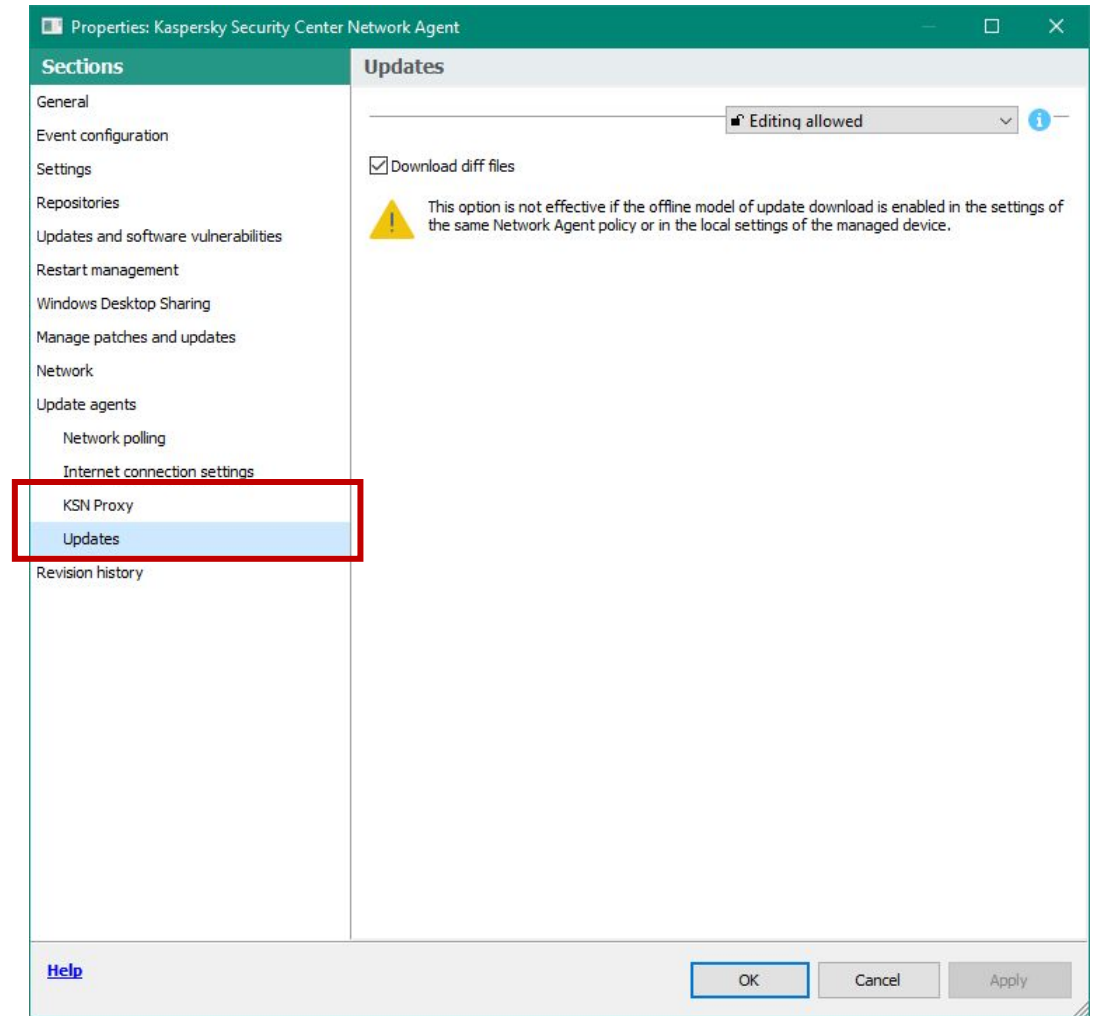
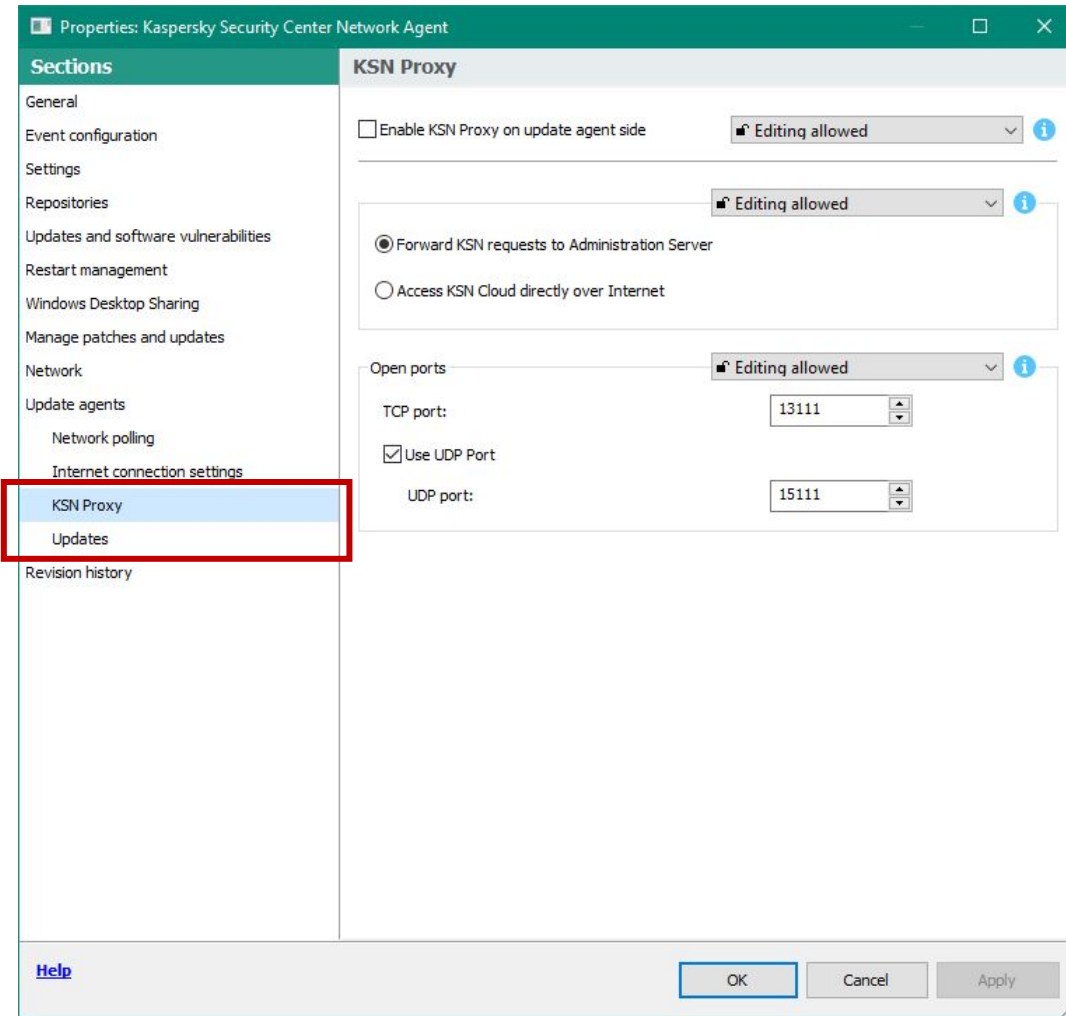
Компонент Adaptive Anomaly Control

Проверка зашифрованного трафика

Защита от MAC Spoofing

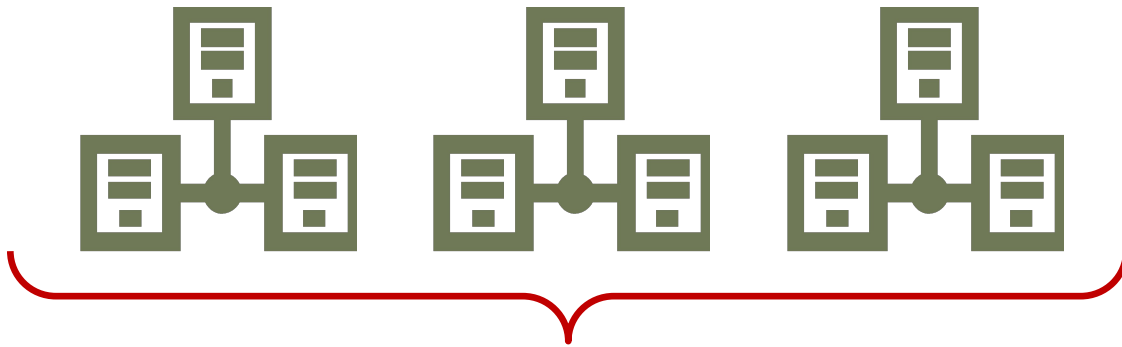
Role Based Access Control for KES

Kaspersky Security Center 11: агенты обновлений



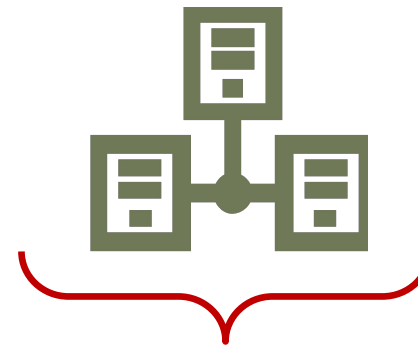
Update Agent: поддержка 10 000 узлов

Kaspersky Security Center 11



до 100 000

Update Agent

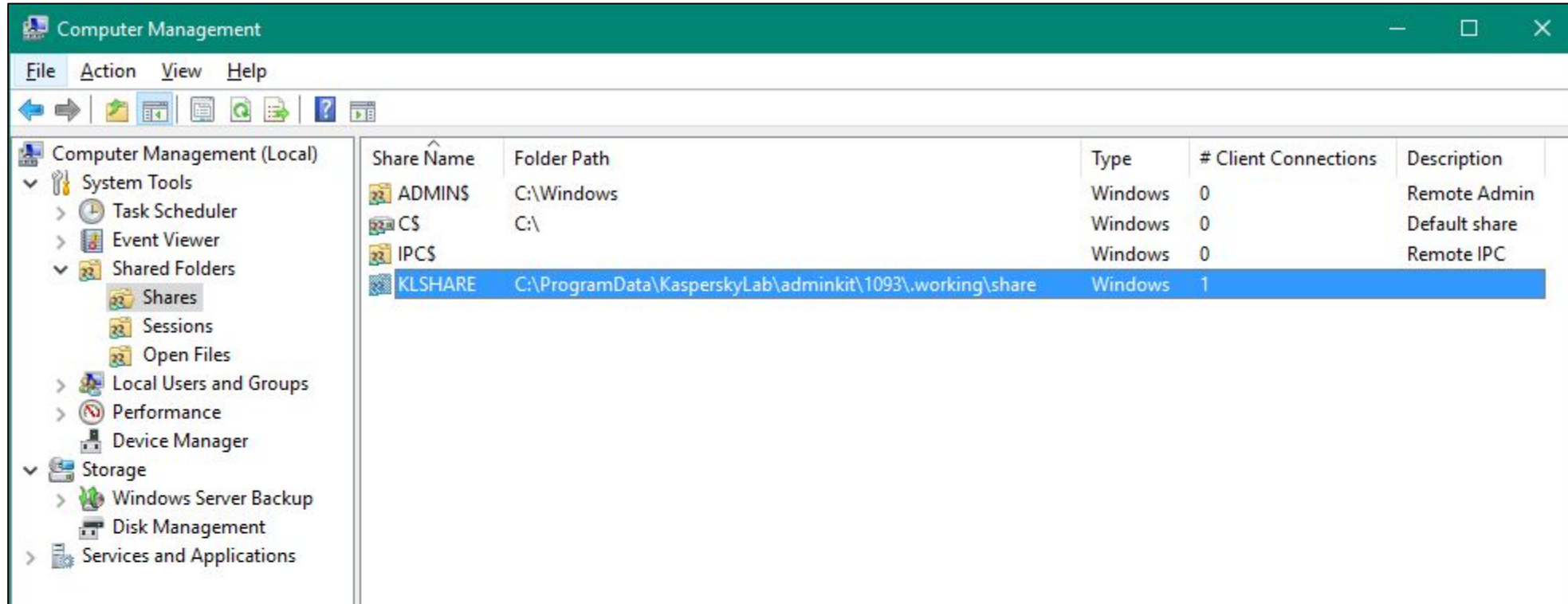


до 10 000

Update Agent: системные требования

- Процессор:
 - частота 3,6 ГГц или выше
- Оперативная память:
 - от 8 ГБ
- Объем свободного места на диске:
 - от 120 ГБ

Папка KLSHARE переехала



C:\ProgramData\KasperskyLab\adminkit\1093\working\share\



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

Проверка зашифрованного трафика

Защита от MAC Spoofing

Role Based Access Control for KES

Kaspersky Security Center 11: обратная совместимость плагинов KES

— Политики и задачи KES 11.1 теперь распространяются на KES 11

Administration Server SECURITY-CENTER > Managed devices > Workstations

Policies

Devices

Policies

Tasks

Create a policy

Import policy from file

Add/Remove columns

Refresh

Inherited policies: **hide** | [show](#)

Name	Status	Application
Kaspersky Endpoint Security for Windows (11.1.0)		
Kaspersky Endpoint Security for Windows (11.1.0)	Active	Kaspersky Endpoint Security for Windows (11.1.0)

Kaspersky Endpoint Security for Windows (11.1.0)

Application: Kaspersky Endpoint Security for Windows (11.1.0)

Created: 10/29/2018 2:06:38 PM

Changed: 10/29/2018 2:06:59 PM

Inherited policy: Not inherited

Affected: 2 devices

Enforcement successful: 2 devices

Details

Configure policy

Configure notifications

Name

Connecting to Server

Agent installed

Real-time protection status

Created

Application version

ABC-TEST	2 minutes ago	Yes	Running	1 weeks ago	11.0.0.6499
ALEX-DESKTOP	6 minutes ago	Yes	Running	2 weeks ago	11.1.0.15605

Help KASPERKY

Results of policy enforcement

Export to file...

Refresh

Device	Windows domain	Date
ABC-TEST	ABC	11/2/2018 6:10:46 PM
ALEX-DESKTOP	ABC	11/2/2018 6:10:47 PM

Kaspersky Security Center 11: удаленная установка

Kaspersky Security Center 10

The screenshot shows the 'New Task Wizard' window in Kaspersky Security Center 10. The 'Settings' section is active. Under 'Force download of the installation package', the options are:
- ☒ Using Network Agent
- ☐ Using operating system resources by means of update agents
- ☒ Using operating system resources by means of Administration Server
 To use AWS integration, the Administrator needs dedicated keys.
Below this, there are two more options:
- ☒ Do not install application if it is already installed
- ☐ Assign the package installation in the Active Directory group policies
At the bottom, there is a link: [Closing running applications before installation starts](#). The 'Next' button is highlighted with a blue border.

Kaspersky Security Center 11

The screenshot shows the 'New Task Wizard' window in Kaspersky Security Center 11. The 'Settings' section is active. Under 'Force installation package download', the options are:
- ☒ Using Network Agent
- ☐ Using operating system resources through distribution points
- ☒ Using operating system resources through Administration Server
 To perform installation by using the API of a cloud service provider, you need a special license. [Learn more...](#)
Below this, there is a section titled 'Behavior for devices managed through other Administration Servers' which is highlighted with a red rectangle. It contains two radio button options:
- ☒ Install always
- ☐ Install only on devices managed through this Administration Server
Below this section, there are two more options:
- ☒ Do not re-install application if it is already installed
- ☐ Assign package installation in Active Directory group policies
At the bottom, there is a link: [Close all running applications before installation starts](#). The 'Next' button is highlighted with a blue border.



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

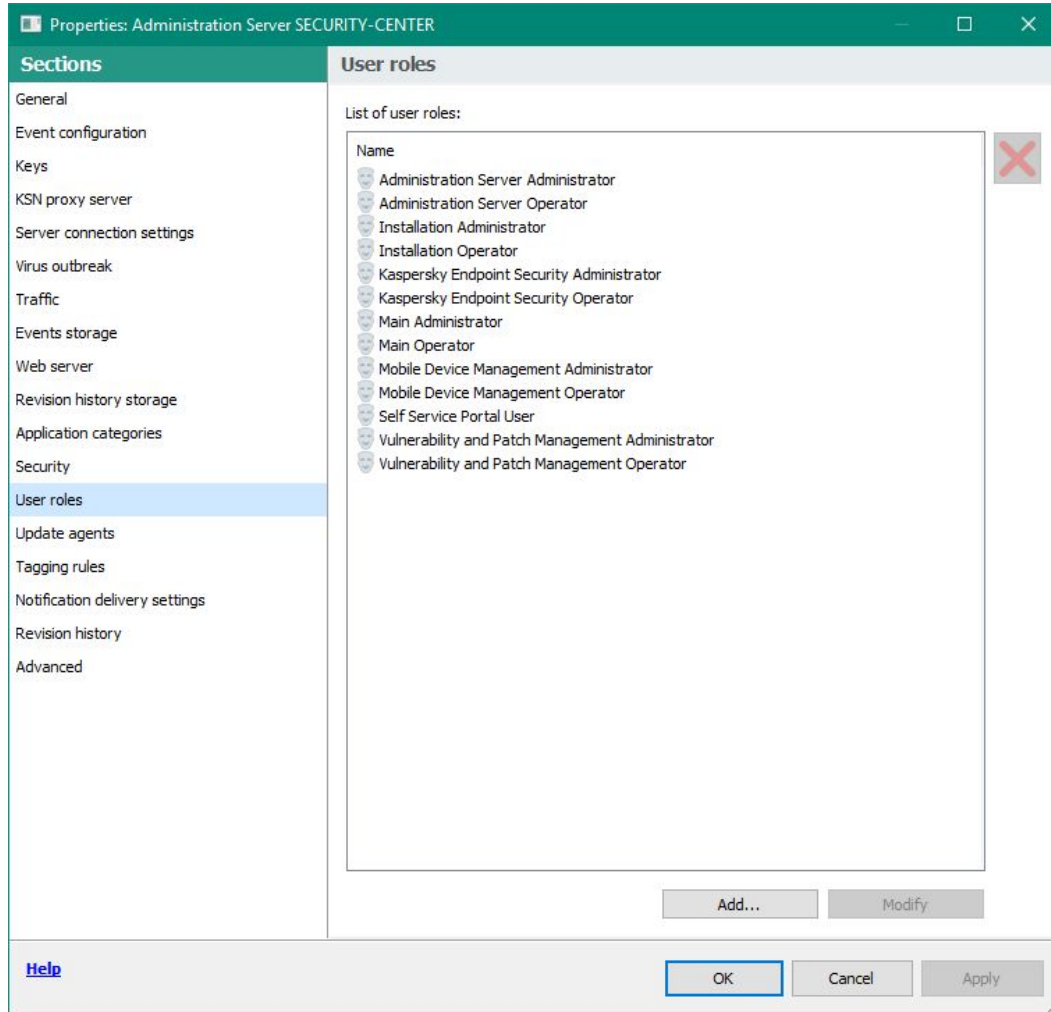
Проверка зашифрованного трафика

Защита от MAC Spoofing

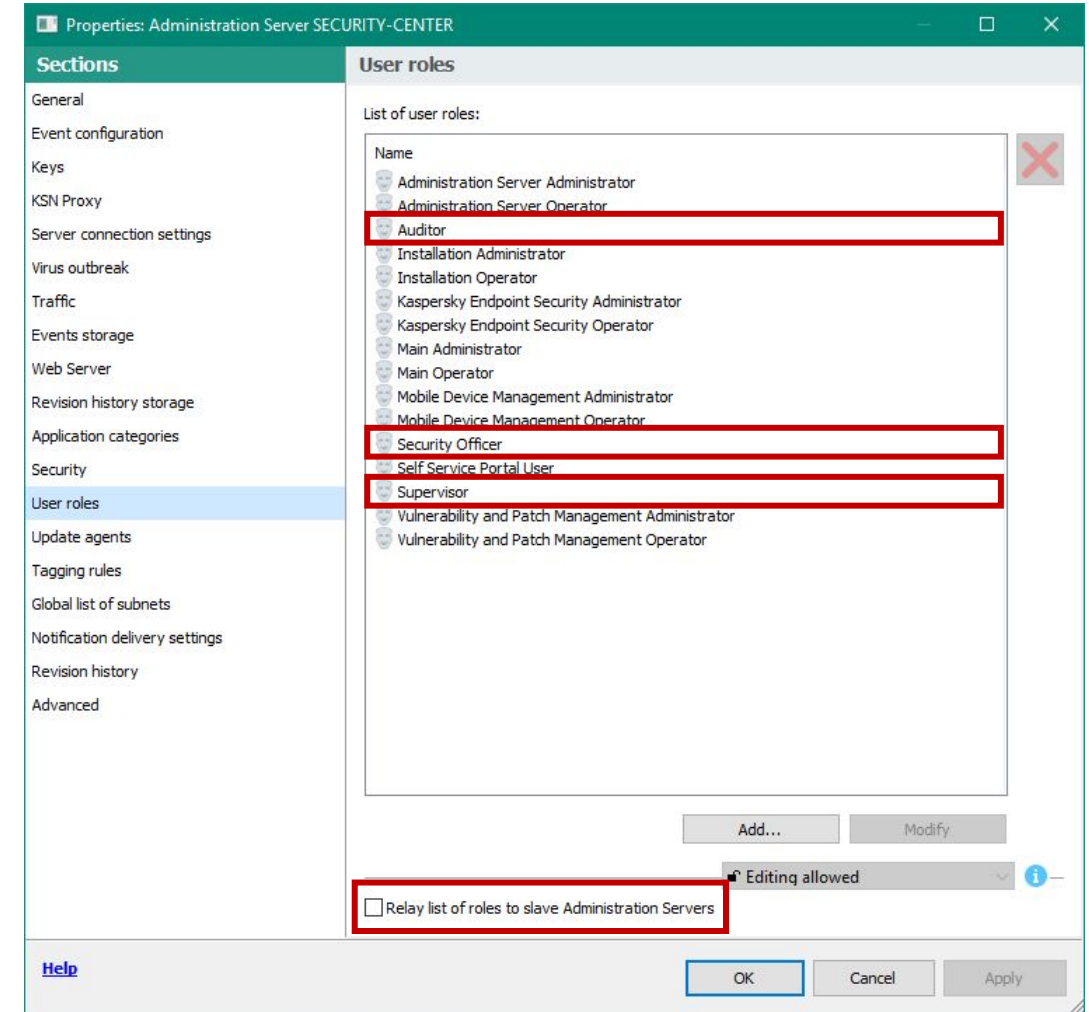
Role Based Access Control for KES

Kaspersky Security Center 11: улучшение RBAC

Kaspersky Security Center 10

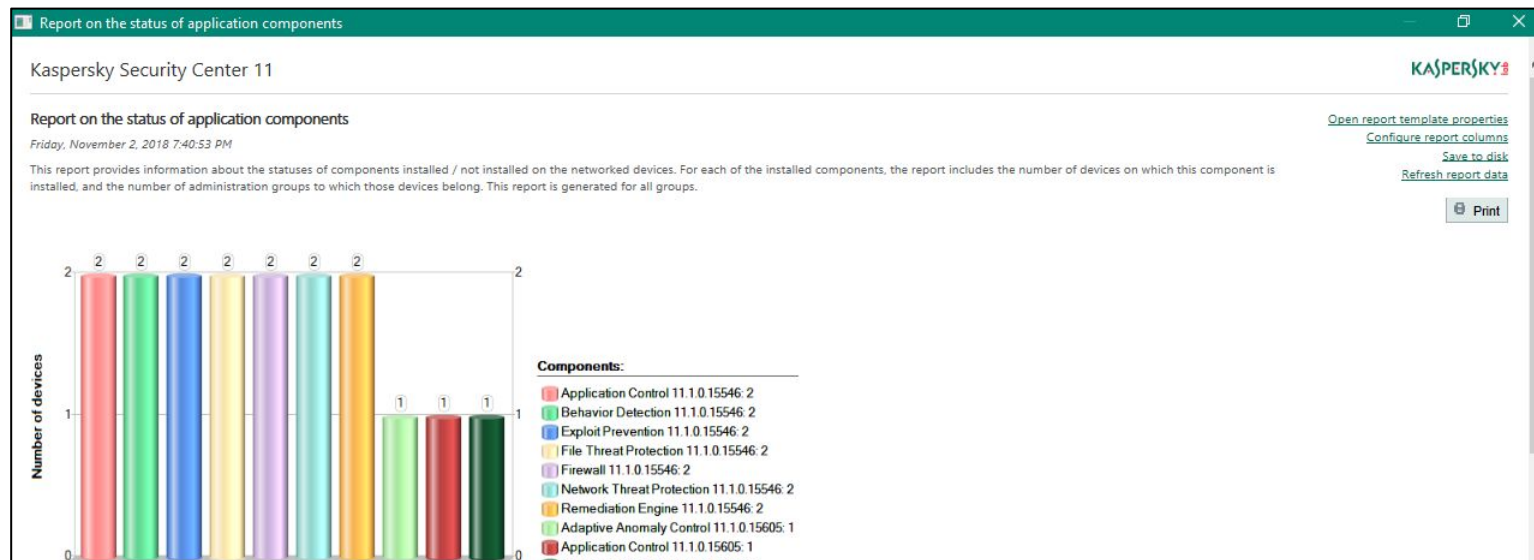


Kaspersky Security Center 11



Kaspersky Security Center 11: НОВЫЕ ОТЧЕТЫ

- Добавлены новые отчеты
 - Adaptive Anomaly Control report
 - Report on Adaptive Anomaly Control rules state
 - Report on the status of application components
 - Report on threat detection distributed by component and detection technology



Summary:

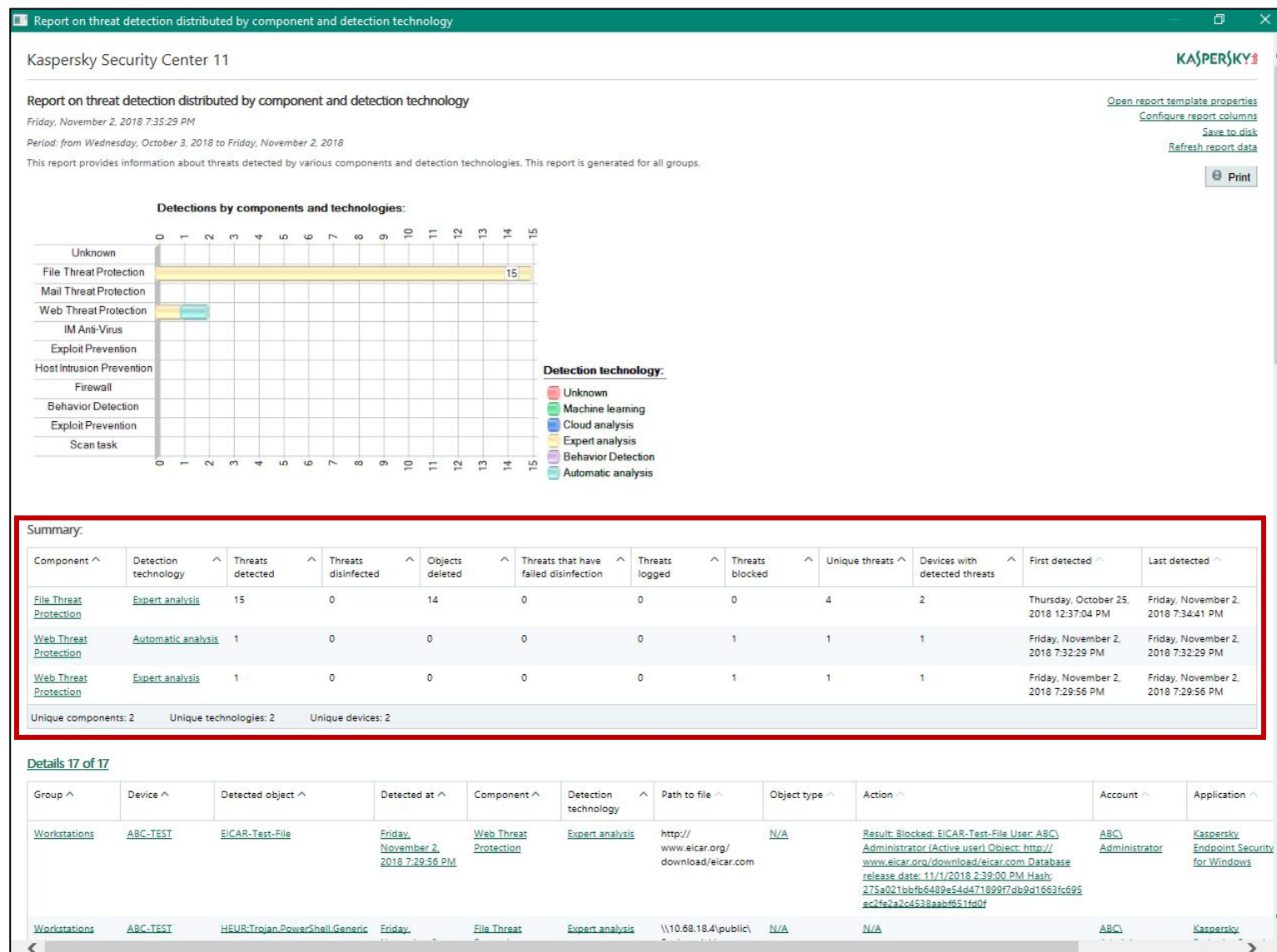
Component name ^	Component version ^
Adaptive Anomaly Control	11.1.0.15605
Application Control	11.1.0.15546
Application Control	11.1.0.15605
Behavior Detection	11.1.0.15546
Behavior Detection	11.1.0.15605
Device Control	11.1.0.15605
Exploit Prevention	11.1.0.15546
Exploit Prevention	11.1.0.15605
File Threat Protection	11.1.0.15546
File Threat Protection	11.1.0.15605
Firewall	11.1.0.15546
Firewall	11.1.0.15605
Host Intrusion Prevention	11.1.0.15605
Mail Threat Protection	11.1.0.15605
Network Threat Protection	11.1.0.15546

Report on the status of application components

Details 54 of 54

Virtual Administration Server ^	Group ^	Device ^	Application ^	Component name ^	Component status ^	Component version ^
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Adaptive Anomaly Control	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	AMSI Protection Provider	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Application Control	Stopped	11.1.0.15546
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	BadUSB Attack Prevention	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Behavior Detection	Running	11.1.0.15546
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Device Control	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Endpoint Sensor	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Exploit Prevention	Running	11.1.0.15546
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	File Level Encryption	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	File Threat Protection	Running	11.1.0.15546
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Firewall	Running	11.1.0.15546
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Full Disk Encryption	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Host Intrusion Prevention	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Mail Threat Protection	Not installed	
	Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.1.0)	Network Threat Protection	Running	11.1.0.15546

НОВЫЕ ОТЧЕТЫ: Report on threat detection distributed by component and detection technology



Интеграция с SIEM через Syslog

Properties: Events

Sections

Notification

Event export

Event export

☒ Automatically export events to SIEM system database

SIEM system:

Syslog (RFC 5424) format

SIEM system server address: 10.28.0.70

SIEM system server port: 514

Protocol: TCP/IP

Maximum message size, in bytes: 2048

To export listed events starting from the specified date, click the Export archive button.

Export archive...

Help OK Cancel Apply



QRadar (LEEF format)
ArcSight (CEF format)
Splunk (CEF format)
Syslog (RFC 5424) format

Чтобы отправлять события из Kaspersky Security Center в SIEM-систему по протоколу Syslog больше не нужна лицензия

Kaspersky Security Center 11: итого

- Основные изменения
 - Появилась полноценная KSC Web Console
 - Реализована поддержка DIFF-файлов обновлений
 - Реализована поддержка обратной совместимости плагинов KES
 - Агенты обновлений могут выступать в роли KSN-прокси и поддерживают до 10000 узлов
- Неосновные изменения
 - Добавление новых ролей в RBAC не требует лицензии KSC
 - Добавлены новые отчеты
 - Интеграция с SIEM системами через Syslog больше не требует лицензии KSC



Лабораторная работа №2

Внедрение Kaspersky Endpoint Security

1. Установите Kaspersky Endpoint Security для Windows на компьютеры сети
2. Изучите результаты установки

Лабораторная работа №3

Создание структуры управляемых компьютеров

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

Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC



Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

Проверка зашифрованного трафика

Защита от MAC Spoofing

Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: операционные системы

- Операционные системы:
 - Windows 10 Redstone 5
 - Windows Server 2019

Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе MMC-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC



Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES

Компонент AMSI Protection Provider

Компонент Adaptive Anomaly Control

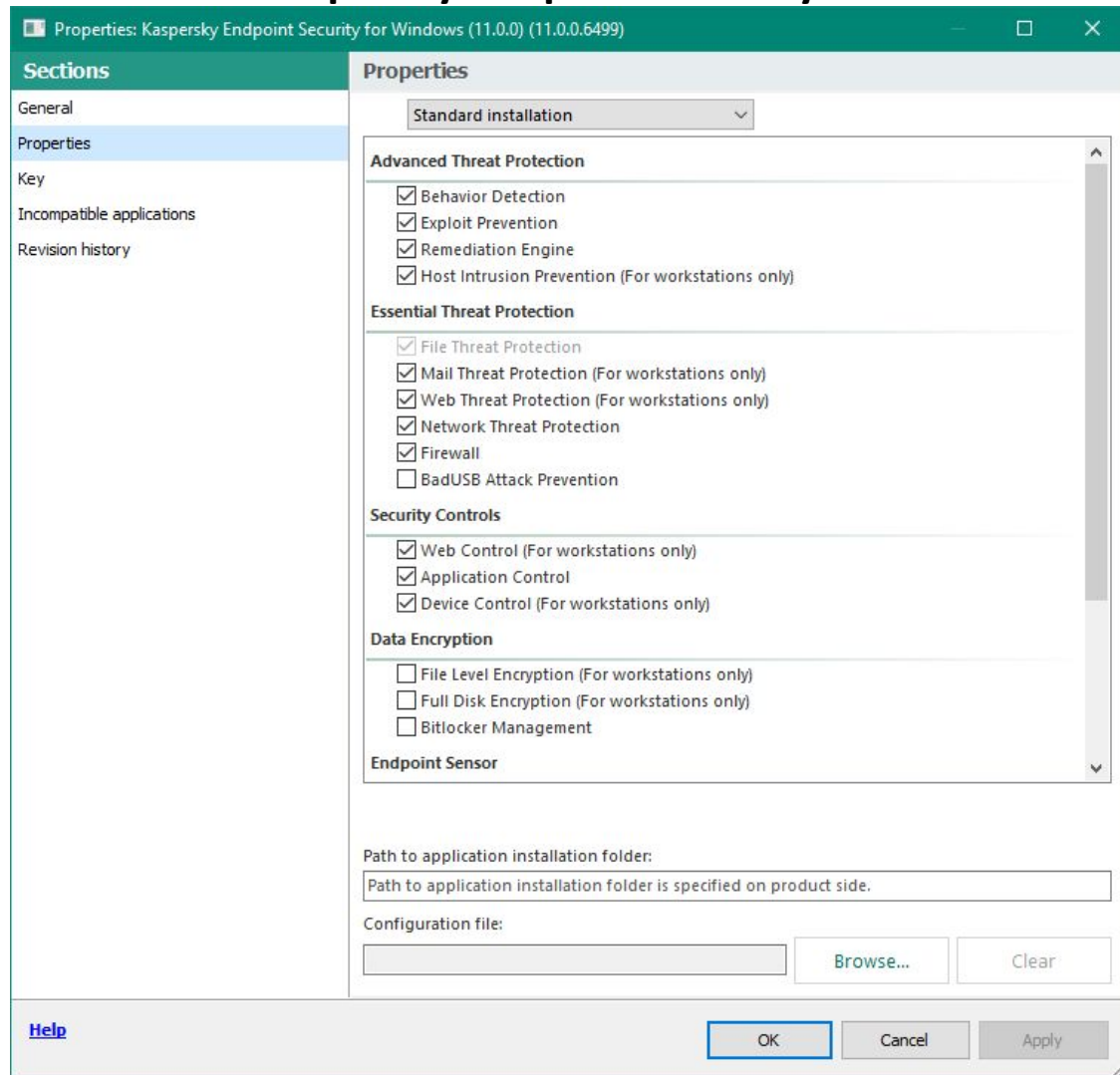
Проверка зашифрованного трафика

Защита от MAC Spoofing

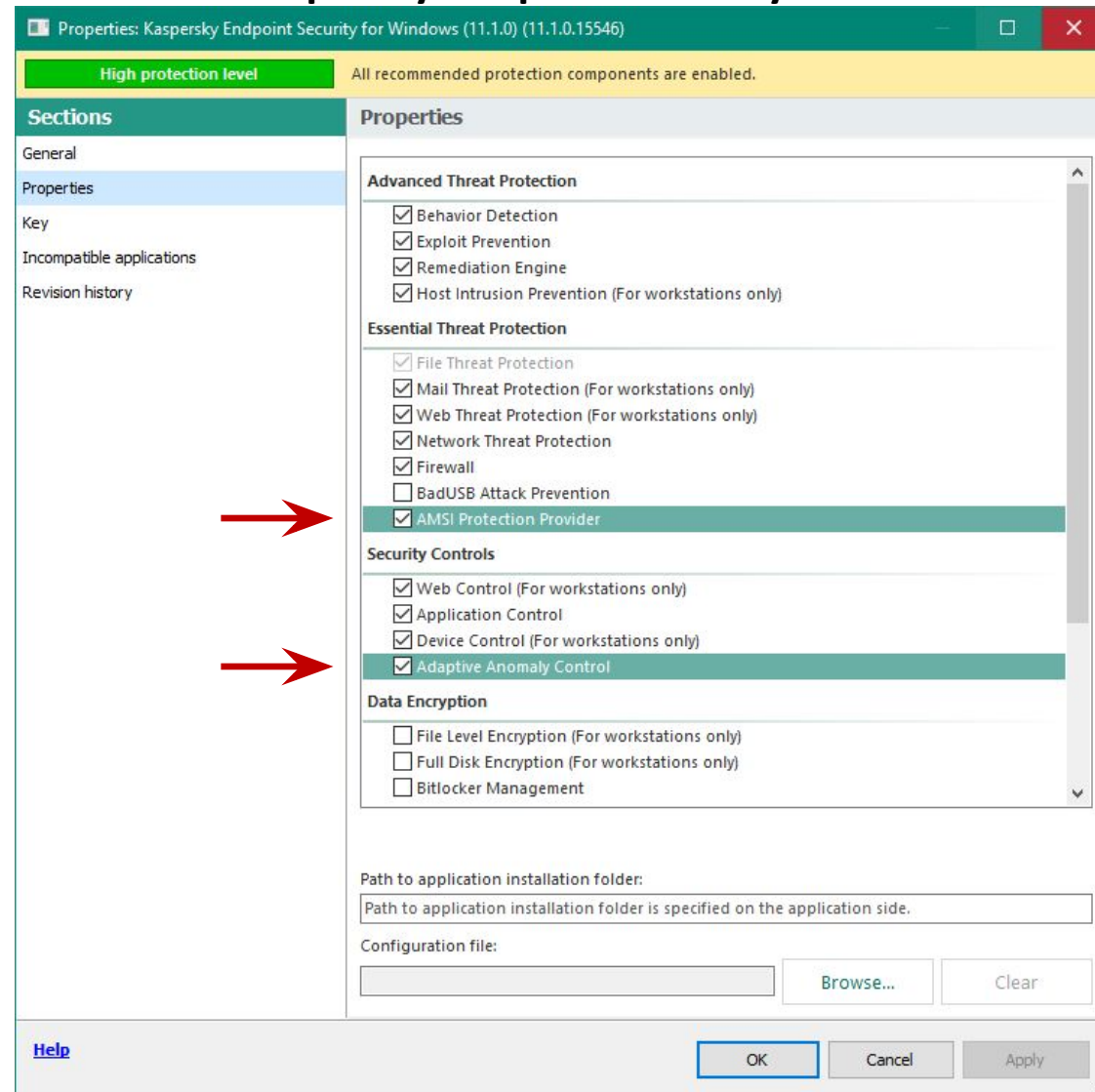
Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: НОВЫЕ КОМПОНЕНТЫ

Kaspersky Endpoint Security 11.0



Kaspersky Endpoint Security 11.1



Что нового в Kaspersky Security Center 11

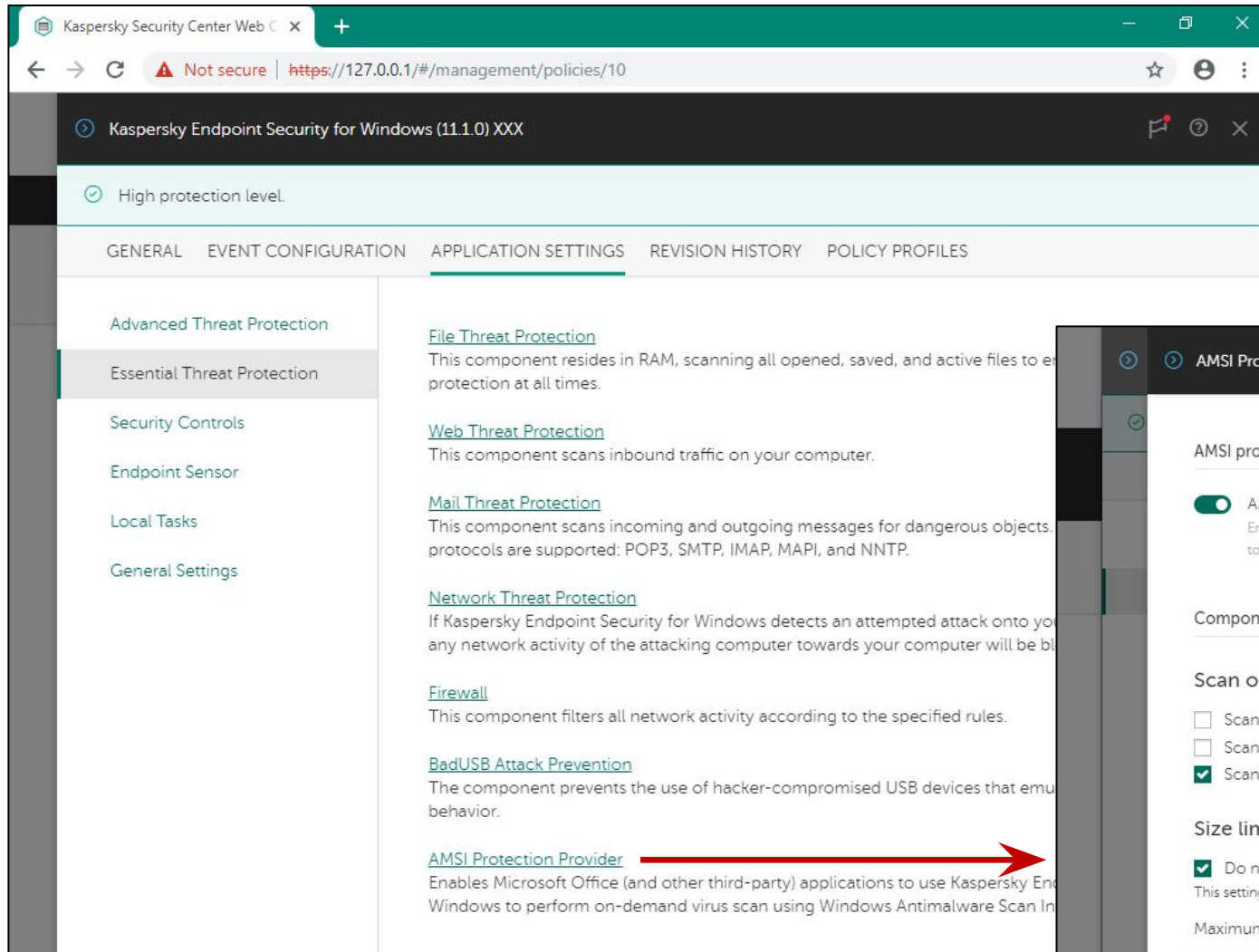
- Операционные системы
- New Web Console
- Изменения в интерфейсе MMC-консоли администрирования
- Поддержка DIFF-файлов обновлений
- Изменения в работе Агентов обновлений
- Обратная совместимость плагинов KES
- Улучшения в RBAC



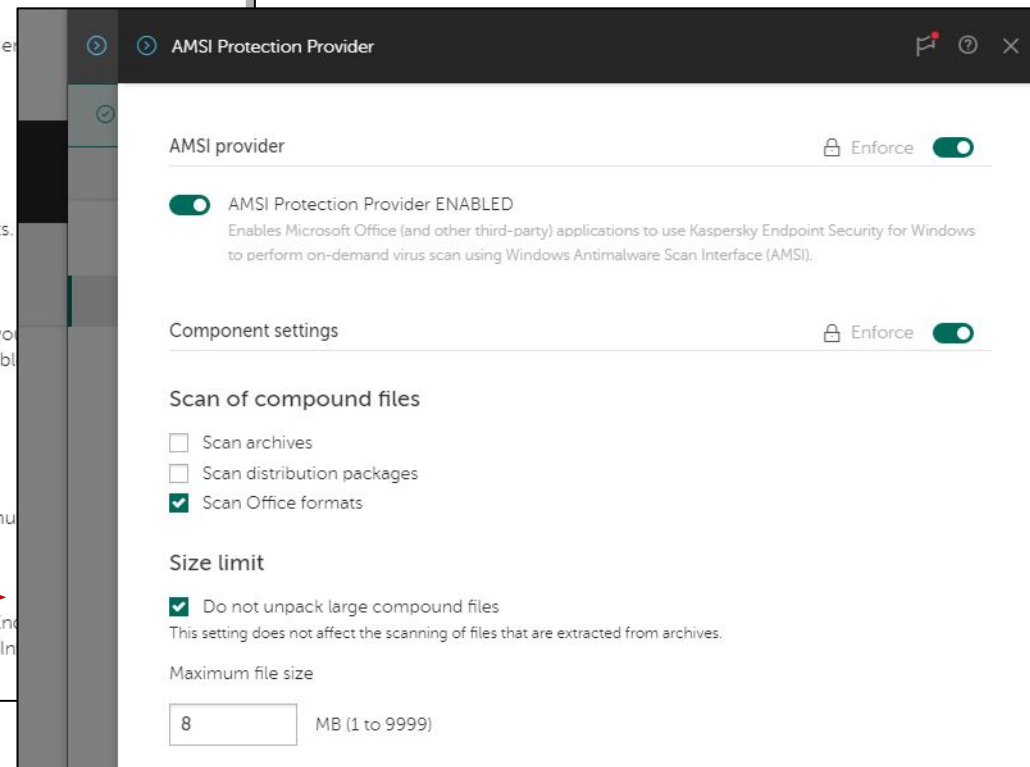
Что нового в Kaspersky Endpoint Security 11.1

- Операционные системы
- Новые компоненты KES
- Компонент AMSI Protection Provider**
- Компонент Adaptive Anomaly Control
- Проверка зашифрованного трафика
- Защита от MAC Spoofing
- Role Based Access Control for KES

Как поставщик AMSI-защиты защищает от новых угроз?



Взаимодействие с AMSI, позволяет KES увеличить уровень обнаружения вредоносных скриптов, сценариев выполняющихся в памяти и применяющих различные технологии маскировки (obfuscation and evasion techniques)

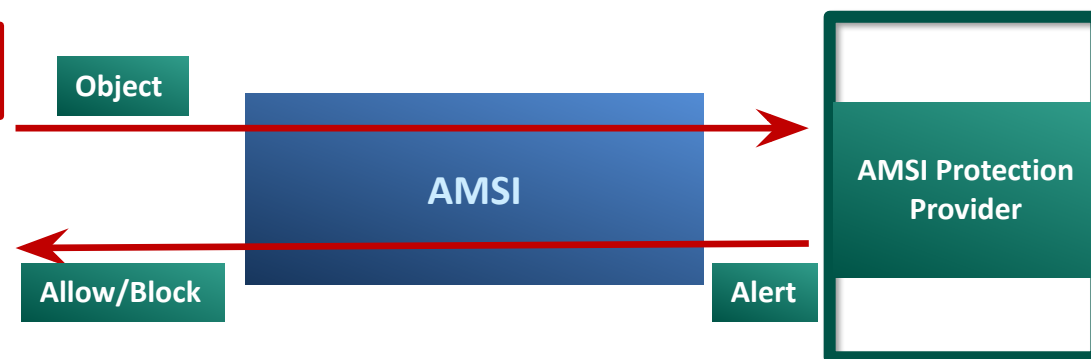


AMSI Protection Provider: как это работает

Программа, прежде чем выполнить скрипт, отправляет его AMSI (Windows Antimalware Scan interface), и ждет вердикта

AMSI получает скрипты от программ, обрабатывает их и передает на проверку Protection Provider (KES)

KES 11.1



KES – получает PowerShell, VBScript, Jscript от AMSI, проверяет их и отправляет назад вердикты

Выполнит или нет программа скрипт, зависит от полученного вердикта и настроек программы

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\test_files\bsstest_amsi\
PS C:\test_files\bsstest_amsi> .\bsstest_amsi.ps1
@{Version=5.1.17134.228}
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# AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...

This script contains malicious content and has been blocked by your antivirus software.
Test succeeded
PS C:\test_files\bsstest_amsi>
```

AMSI Protection Provider: события

The screenshot shows the 'Reports' window in Kaspersky Endpoint Security. The left sidebar lists various security features, with 'AMSI Protection Provider' highlighted under 'Security Controls'. The main pane displays a list of events for the AMSI Protection Provider, filtered for 'Today, 12-Nov-18'. The events include task starts, malicious object detections, and warnings about scan results being sent to third-party applications. A detailed view of a warning event is shown at the bottom.

Event date	Name	Application
12-Nov-18 10:43:08	Task started	Kaspersky End
12-Nov-18 11:53:26	Malicious object detected	Windows Pow
12-Nov-18 11:53:26	The object scan result has been sent to a third-party application	Windows Pow
12-Nov-18 11:53:26	Malicious object detected	Windows Pow
12-Nov-18 11:53:27	The object scan result has been sent to a third-party application	Windows Pow
12-Nov-18 11:53:27	Malicious object detected	Windows Pow
12-Nov-18 11:53:27	The object scan result has been sent to a third-party application	Windows Pow
12-Nov-18 11:53:28	Malicious object detected	Windows Pow
12-Nov-18 11:53:28	The object scan result has been sent to a third-party application	Windows Pow

12-Nov-18 11:53:26 : The object scan result has been sent to a third-party application

Application: Windows PowerShell
User: DESKTOP-MJ8QETO\VB (Active user)
Component: AMSI Protection Provider
Result: Untreated: HEUR:Trojan.Multi.AmsiKdbDetect.gen
Object: unnamed_amsi_stream_16
Reason: Logged
Hash: 57b998003317995fe77ba724267e555aeeb6be33930c5febbacbf54351c514e5

This screenshot shows the 'Event properties' window for a 'Malicious object detected' event. The 'General' tab displays the following details:

- Severity:** Critical event
- Application:** Kaspersky Endpoint Security for Windows (11.1.0)
- Version number:** 11.1.0.15626
- Task name:** AMSI Protection Provider
- Device:** DESKTOP-MJ8QETO
- Group:** WORKGROUP
- Time:** 11/12/2018 11:53:29 AM
- Virtual Administration Server name:**
- Description:**
Result: Detected: HEUR:Trojan.Multi.AmsiKdbDetect.gen
User: DESKTOP-MJ8QETO\VB (Active user)
Object: unnamed_amsi_stream_17
Reason: Expert analysis
Database release date: 11/12/2018 8:37:00 AM
Hash: 5f853d3b102811bbca1b9912c44d8aa627d0e91ed2900602ce96c73e085bfa8a|

This screenshot shows the 'Event properties' window for a warning event: 'The object scan result has been sent to a third-party application'. The 'General' tab displays the following details:

- Severity:** Warning
- Application:** Kaspersky Endpoint Security for Windows (11.1.0)
- Version number:** 11.1.0.15626
- Task name:** AMSI Protection Provider
- Device:** DESKTOP-MJ8QETO
- Group:** WORKGROUP
- Time:** 11/12/2018 11:53:29 AM
- Virtual Administration Server name:**
- Description:**
Event type: The object scan result has been sent to a third-party application
Application\Name: Windows PowerShell
Application\Path: C:\Windows\System32\WindowsPowerShell\v1.0\
Application\Process ID: 6900
User: DESKTOP-MJ8QETO\VB (Active user)
Component: AMSI Protection Provider
Result\Description: Untreated
Result\Type: Trojan
Result\Name: HEUR:Trojan.Multi.AmsiKdbDetect.gen
Result\Threat level: High
Result\Precision: Exactly
Object: unnamed_amsi_stream_17//amsi_script_utf8
Object\Type: String
Object\Path: unnamed_amsi_stream_17//amsi_script_utf8
Object\Name: amsi_script_utf8
Reason: Logged
Hash: 5f853d3b102811bbca1b9912c44d8aa627d0e91ed2900602ce96c73e085bfa8a|



Лабораторная работа №4

Как проверить Защиту от бесфайловых угроз

Что нового в Kaspersky Security Center 11

- Операционные системы
- New Web Console
- Изменения в интерфейсе MMC-консоли администрирования
- Поддержка DIFF-файлов обновлений
- Изменения в работе Агентов обновлений
- Обратная совместимость плагинов KES
- Улучшения в RBAC



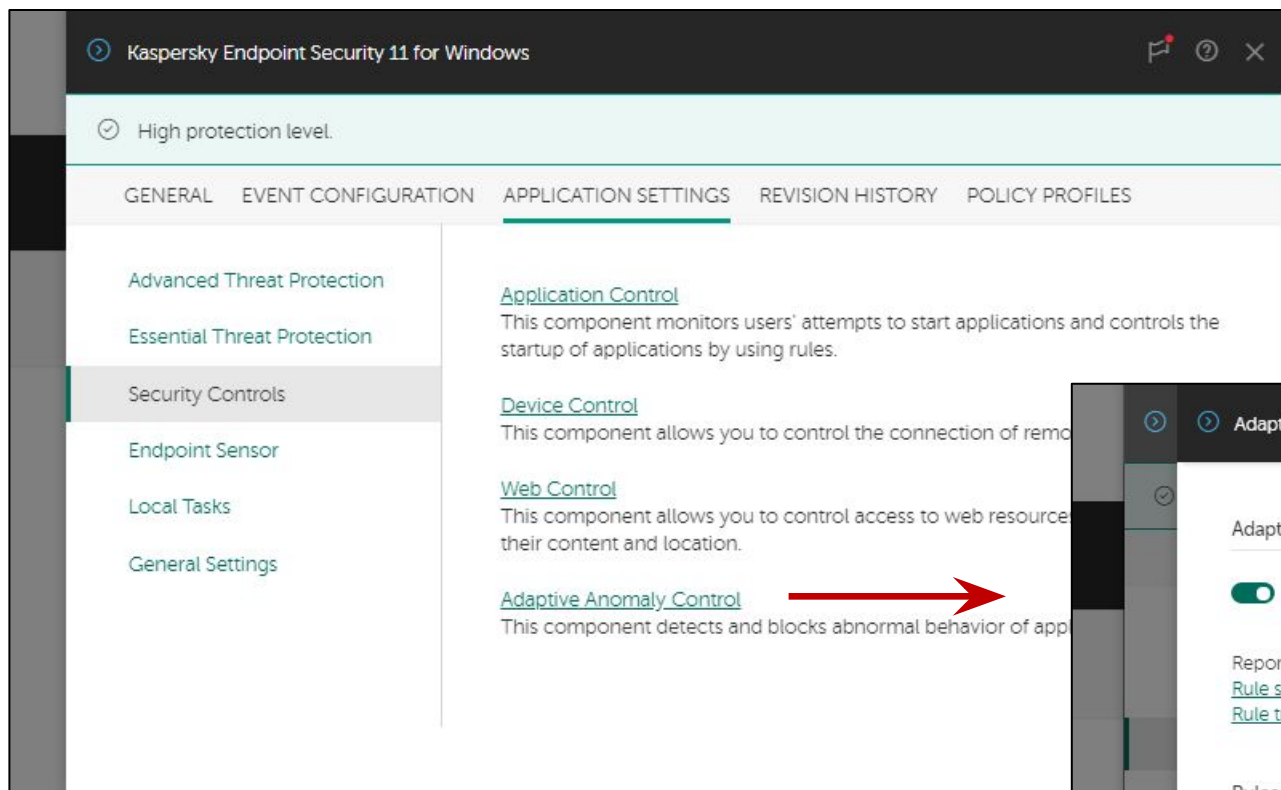
Что нового в Kaspersky Endpoint Security 11.1

- Операционные системы
- Новые компоненты KES
- Компонент AMSI Protection Provider
- Компонент Adaptive Anomaly Control**
- Проверка зашифрованного трафика
- Защита от MAC Spoofing
- Role Based Access Control for KES

Что такое Adaptive Anomaly Control

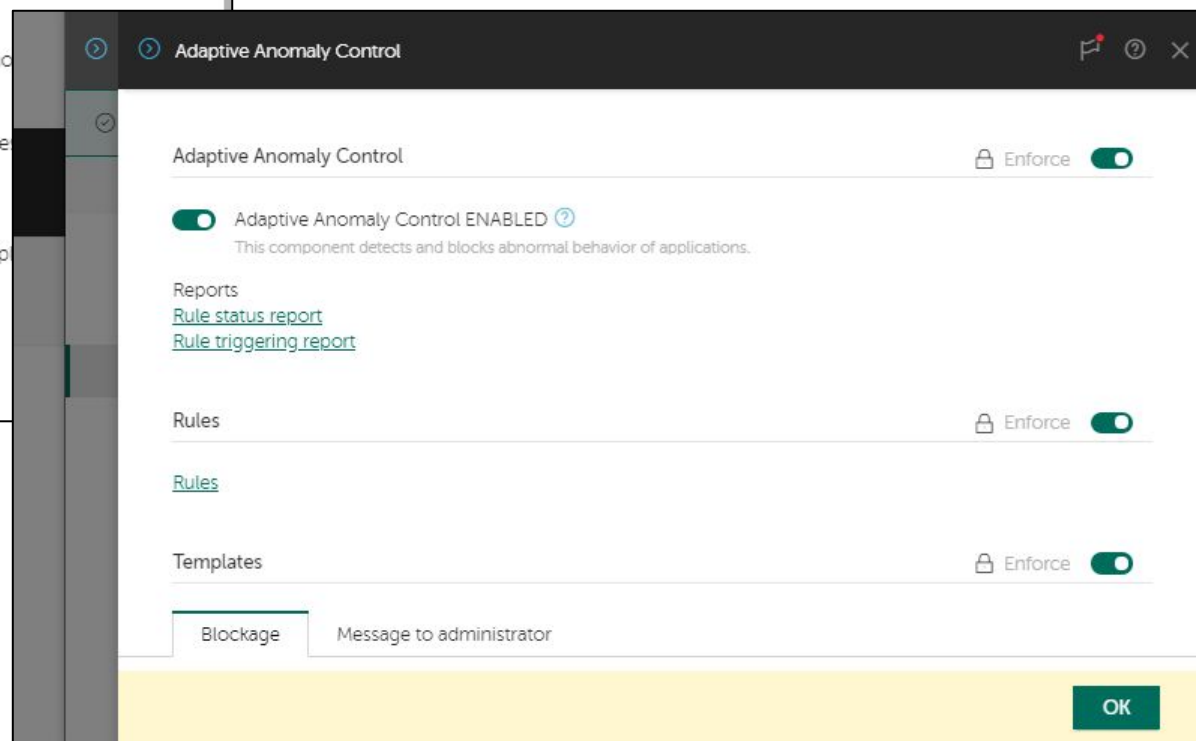
- Новый компонент, который предназначен для детектирования и блокирования нетипичного поведения приложений
- Для детектирования аномального поведения Adaptive Anomaly Control использует набор правил, которые поставляются вместе с базами
- Нетипичное поведение необязательно вредоносное, поэтому по умолчанию компонент Adaptive Anomaly Control работает в Smart Mode
- В течение нескольких недель компонент отслеживает активность на компьютерах и передает информацию о срабатываниях на Сервер администрирования
- Администратор должен обработать событие, подтвердить, что это аномальная активность или добавить в исключения, если активность легитимная
- На каждом компьютере, для каждого правила обучение происходит независимо, т.е. где-то обучение завершится раньше, где-то позже

Где настраивается Adaptive Anomaly Control

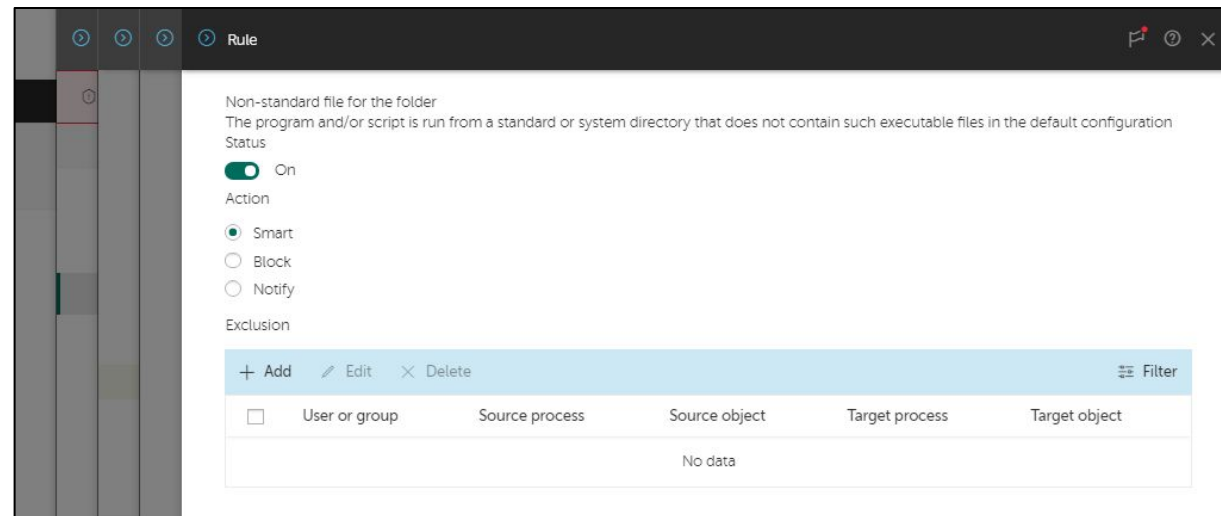
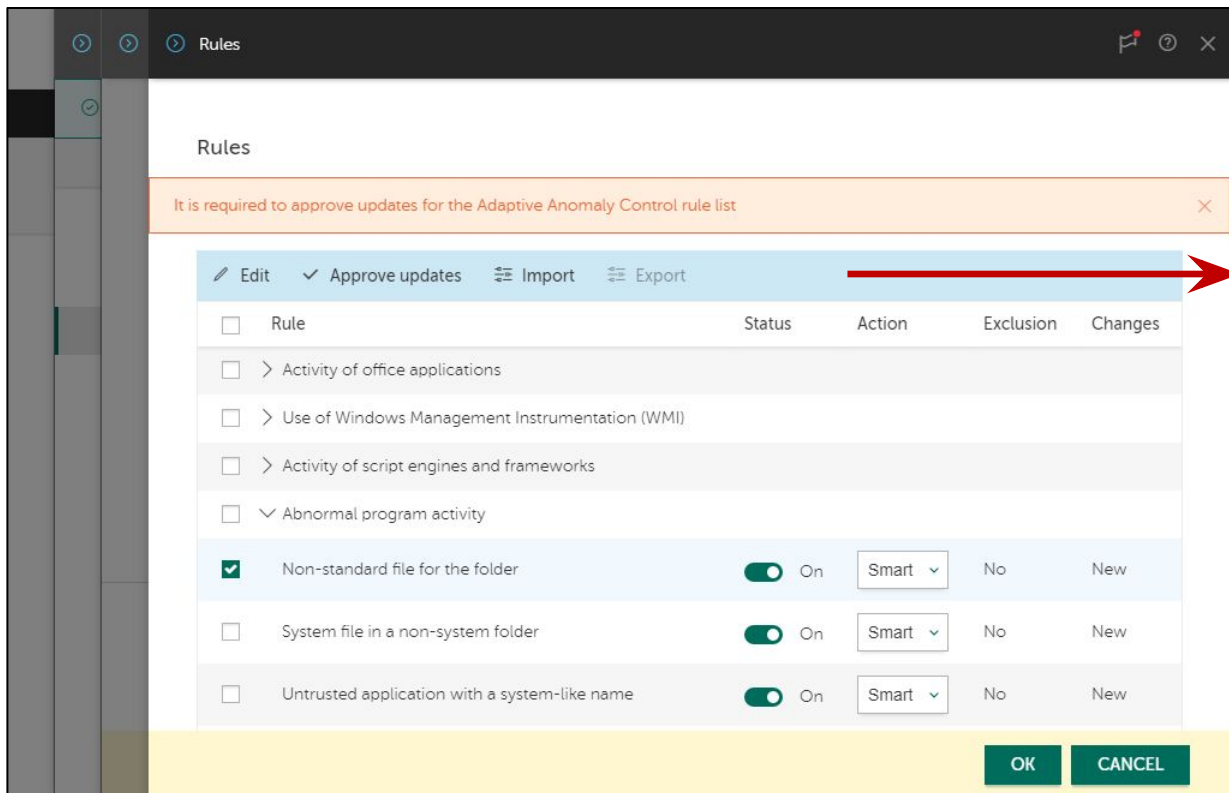


В политике Kaspersky Endpoint Security

По умолчанию ААС включен и работает в режиме Smart



Правила Adaptive Anomaly Control

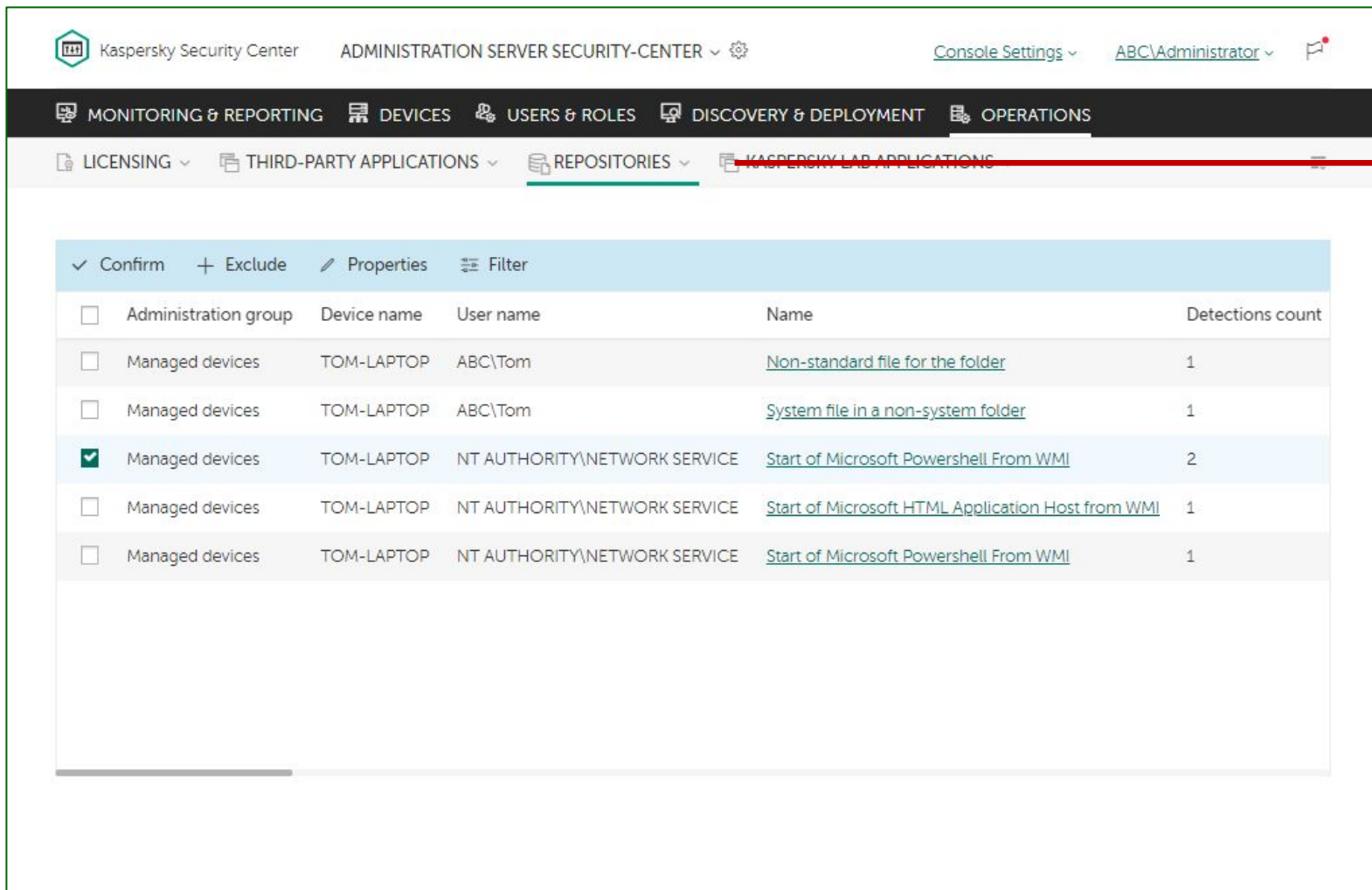


Из настроек у правил есть состояние **Вкл/Выкл**, режим работы **Smart/Block/Notify** и исключения

Adaptive Anomaly Control имеет предустановленный набор правил, которые могут обновляться вместе с базами

Сообщение Approve Updates носит уведомительный характер

Что происходит в режиме Smart Training



Kaspersky Security Center ADMINISTRATION SERVER SECURITY-CENTER Console Settings ABC\Administrator

MONITORING & REPORTING DEVICES USERS & ROLES DISCOVERY & DEPLOYMENT OPERATIONS

LICENSING THIRD-PARTY APPLICATIONS REPOSITORIES **KASPERSKY LAB APPLICATIONS**

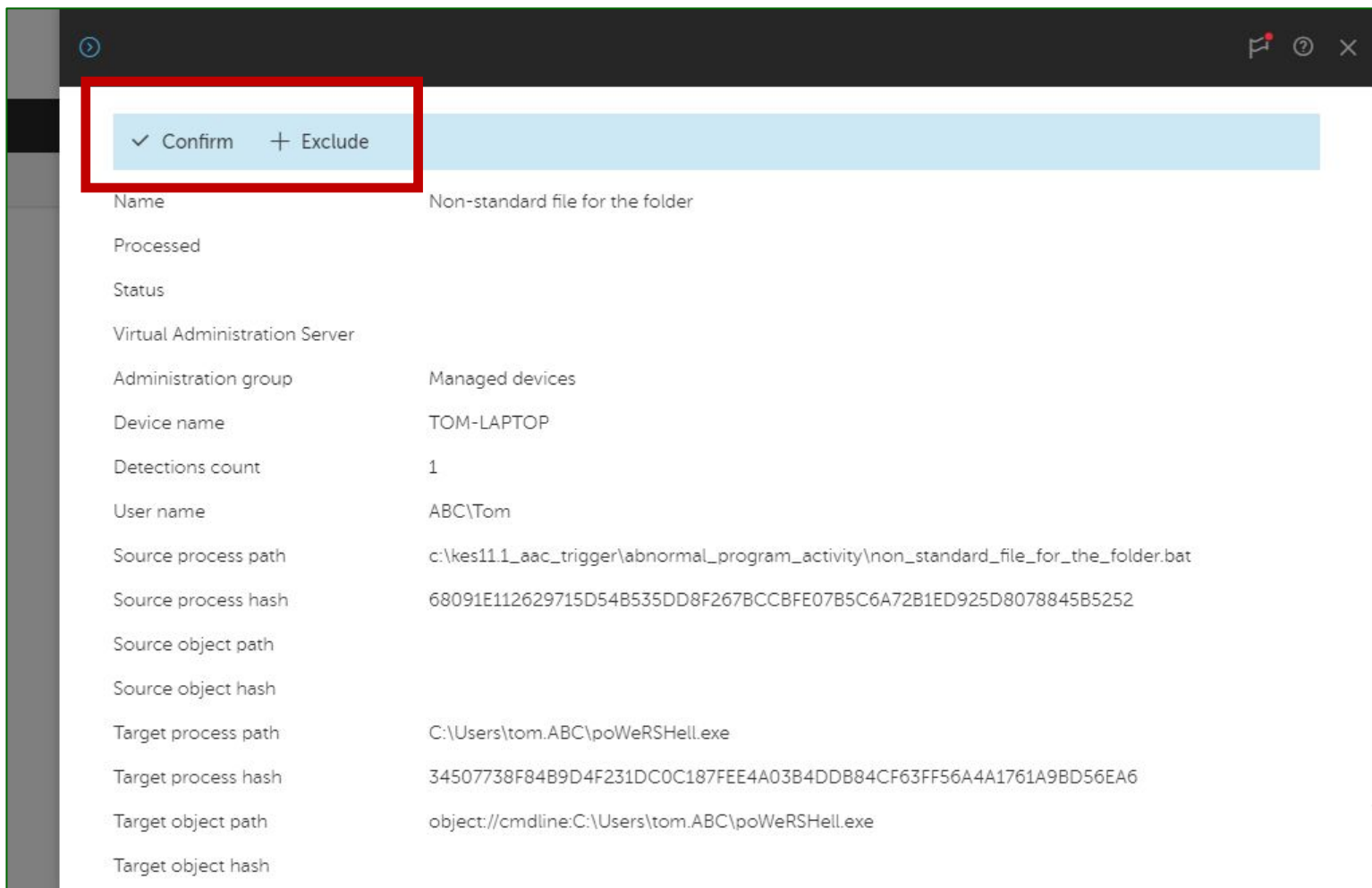
Confirm	Exclude	Properties	Filter			
☐		Administration group	Device name	User name	Name	Detections count
☐		Managed devices	TOM-LAPTOP	ABC\Tom	Non-standard file for the folder	1
☐		Managed devices	TOM-LAPTOP	ABC\Tom	System file in a non-system folder	1
☒		Managed devices	TOM-LAPTOP	NT AUTHORITY\NETWORK SERVICE	Start of Microsoft Powershell From WMI	2
☐		Managed devices	TOM-LAPTOP	NT AUTHORITY\NETWORK SERVICE	Start of Microsoft HTML Application Host from WMI	1
☐		Managed devices	TOM-LAPTOP	NT AUTHORITY\NETWORK SERVICE	Start of Microsoft Powershell From WMI	1

- BACKUP
- QUARANTINE
- ACTIVE THREATS
- INSTALLATION PACKAGES
- HARDWARE
- DELETED OBJECTS
- TRIGGERING OF RULES IN SMART TRAINING MODE

По умолчанию AAC работает в режиме Smart

В этом режиме ничего не блокируется, однако информация обо всех срабатываниях попадает в KSC в контейнер **Triggering of Rules in Smart Training Mode**

Что делать с событиями в режиме Smart

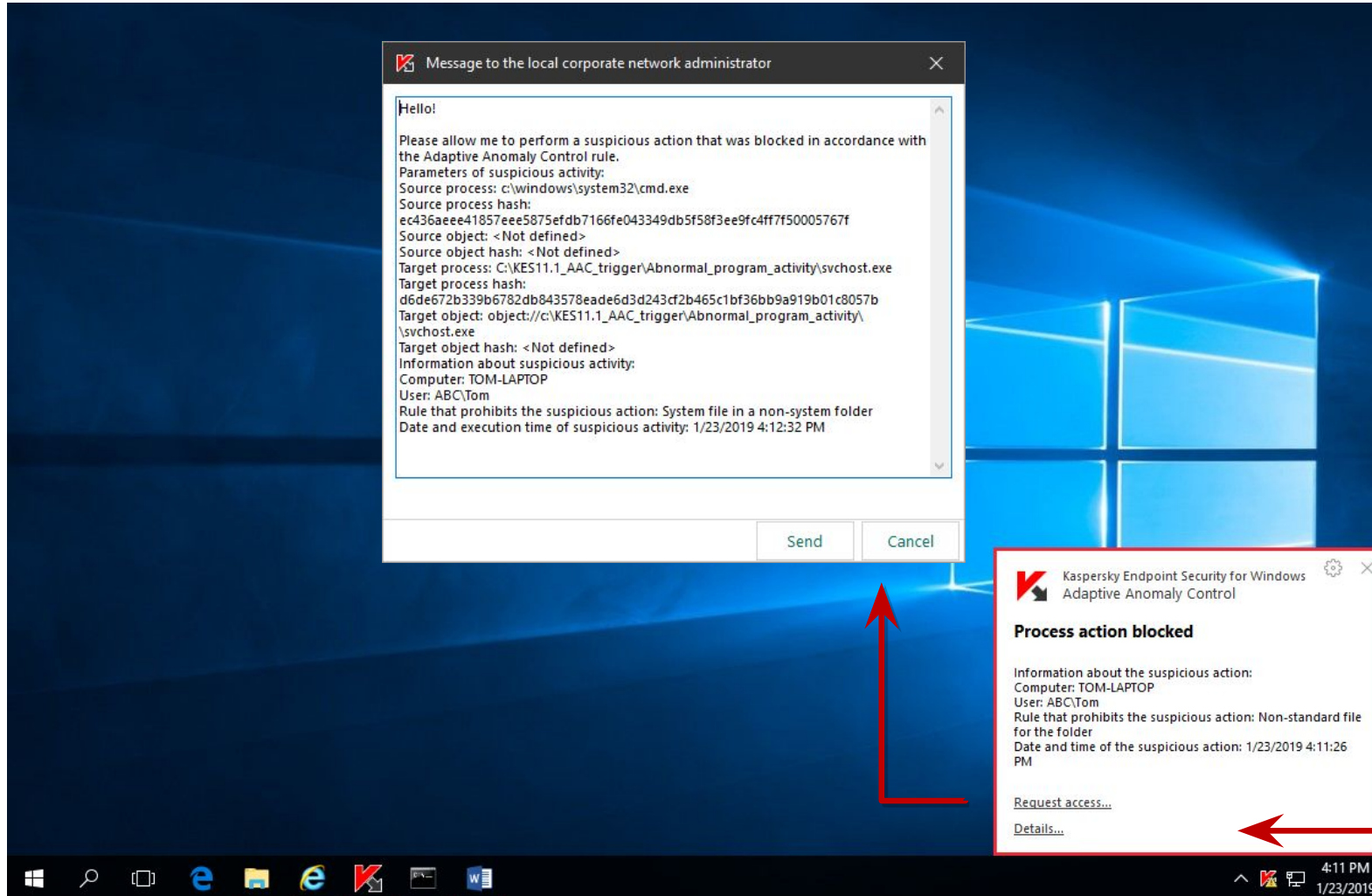


Режим Smart предполагает участие администратора

Администратору желательно обработать событие:

- Confirm
- Exclude

Что увидит пользователь, если ААС перешел в режим Block?



Пользователь может:

- Смириться
- Пожаловаться (ссылка Запросить доступ)

Шаблон запроса настраивается в политике KES

Куда уйдет просьба пользователя?

The screenshot shows the Kaspersky Security Center Administration Server interface. The 'EVENT SELECTIONS' tab is active, displaying a list of selection types. A red arrow points to the 'User requests' selection type, which is checked. An 'Event details' pop-up window is open, showing information about a specific event.

Event details window:

- Task name: Protection
- Application activity blockage message to administrator: 01/23/2019 5:12 am
- Managed devices: TOM-LAPTOP
- Application: Kaspersky Endpoint Security 11 for Windows
- Version: 11.1.0.17068
- Description: Hello!

Event Selections table:

Selection type	Selection name	Selection type
☒	User requests	Predefine
☐	Recent events	Predefine
☐	Critical events	Predefine
☐	Functional failures	Predefine
☐	Warnings	Predefine
☐	Informational messages	Predefine
☐	Audit events	Predefine
☐	AppControl	User selected
☐	Device Control	User selected
☐	New event selection	User selected

На Сервер KSC в виде события, в котором будет:

- Текст, который пользователь может редактировать
- Описание подозрительной активности, которая была заблокирована, с указанием процессов и контрольных сумм
- Имя пользователя
- Компьютер
- Дата и время

Администратор может:

- Ознакомиться с сообщением
- Просмотреть свойства компьютера
- Подумать
- Добавить в исключения AAC

Как еще можно добавить исключения в ААС?

В ААС можно добавлять в исключения прямо из событий

Result of Recent events on 01/23/2019 7:41 am

Refresh list Delete Export to file Assign to category Revision history **Exclude from Adaptive Anomaly Control** Filter

☐	Time	Device	Event	Description
☐	01/23/2019 5:52 am	SECURITY-CENTER	Runtime error.	Runtime error: Database error occurred: #19: Error details: 1950/8152 (Generic db error: "6
☒	01/23/2019 5:49 am	TOM-LAPTOP	Process action skipped	Event type: Process action blocked User: ABC\Tom (Active user) Component: Adaptive Anomaly Control Rule name: Start of Microsoft Windows Com Path to source process file: c:\program files Source process file hash: 270fe63cca815691 Path to source object: c:\kes11.1_aac_trigge Source object hash: f5eee1b8c1d0e12b8ea3 Path to target process file: C:\Windows\SysV Target process file hash: 4c3ea4c44aab7435 Path to target object: object://cmd.exe
☐	01/23/2019 5:46 am	SECURITY-CENTER	Audit: Object has been modified.	Policy "Kaspersky Endpoint Security 11 for W
☐	01/23/2019 5:45 am	SECURITY-CENTER	Audit: Object has been modified.	Policy "Kaspersky Endpoint Security 11 for W
☐				Event type: Process action blocked User: ABC\Tom (Active user) Component: Adaptive Anomaly Control Rule name: Start of Microsoft Windows Com Path to source process file: c:\program files



Event details

Task name Adaptive Anomaly Control

Process action skipped
⚠️
01/23/2019 5:49 am
[Managed devices](#)
[TOM-LAPTOP](#)

Application Kaspersky Endpoint Security 11 for Windows

Version 11.1.0.17068

Event type: Process action blocked
User: ABC\Tom (Active user)
Component: Adaptive Anomaly Co
Rule name: Start of Microsoft Wind
application
Path to source process file: c:\prog
office\office15\winword.exe
Source process file hash:
270fe63cca8156911303ebdf9481b
Path to source object: c:\kes11.1_a
prompt.doc
Source object hash:
f5eee1b8c1d0e12b8ea3ab0266e80
Path to target process file: C:\Wind
Target process file hash:
4c3ea4c44aab74350355c419826b
Path to target object: object://cmd.

Description

Event registered 01/23/2019 5:49 am

BACK NEXT

Какие события есть у Adaptive Anomaly Control?

The screenshot shows the 'AAC' configuration window with the 'Events' tab active. The configuration includes fields for 'Application name', 'Version', 'Task name', and 'Severity level' (set to 'Critical'). A checkbox 'Include general events' is checked. Below this is a table of event types:

☐	Severity level	Event name
☐	Critical	The object cannot be deleted
☐	Critical	Processing error
☐	Critical	Dangerous link blocked
☐	Critical	Dangerous link opened
☐	Critical	Previously opened dangerous link detected
☐	Critical	Process terminated
☐	Critical	Unable to terminate process
☒	Critical	Process action skipped

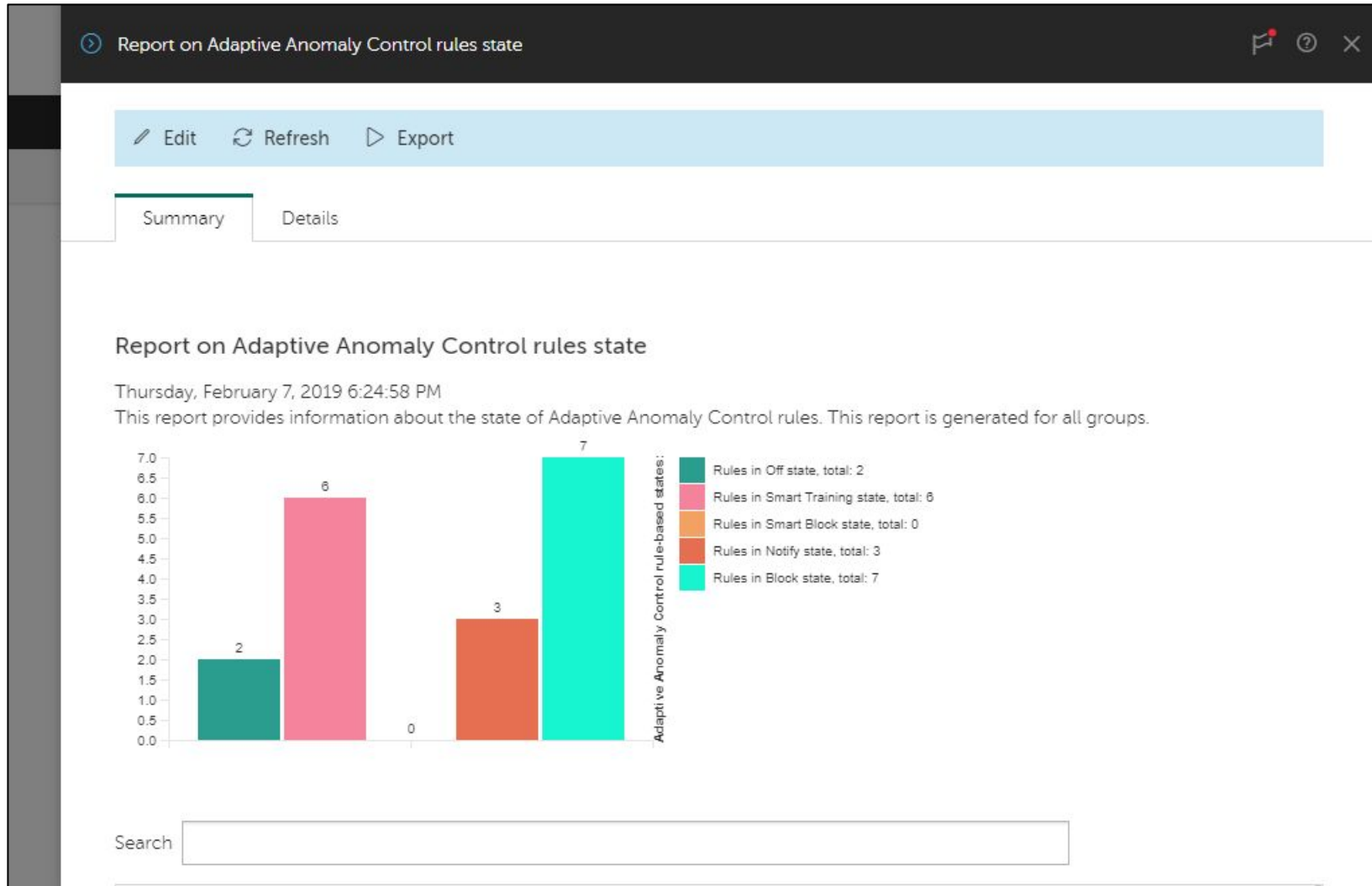
At the bottom, there is a 'Pending changes' status and 'SAVE' and 'CANCEL' buttons.

У Adaptive Anomaly Control есть два типа событий:

- Process action skipped
- Process action blocked

Можно создать отдельную выборку на эти два события

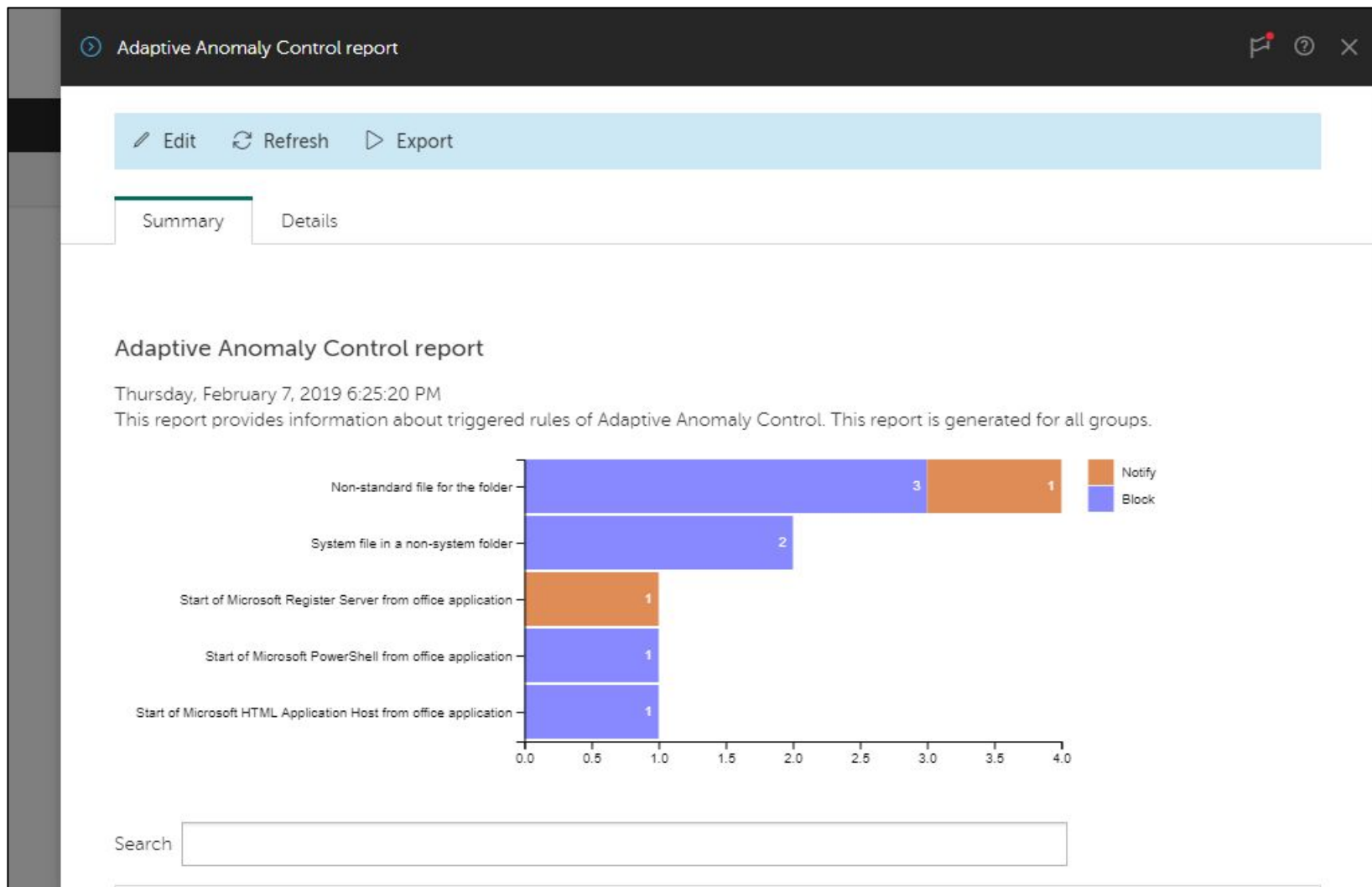
Отчеты есть? Обязательно!



Report on Adaptive Anomaly Control rules state – показывает в каком режиме находится то или иное правило

Это единственное место, где можно посмотреть закончилось ли обучение, т.е. перешло ли правило из Smart Training режима в Smart Block

Отчеты есть? Обязательно!



Adaptive Anomaly Control report – показывает как часто какие правила срабатывают



Лабораторная работа №5

Как настроить Adaptive Anomaly Control

1. Настройте блокировку запуска макросов и скриптов в офисных документах
2. Проверьте, что Adaptive Anomaly Control блокирует запуск вредоносного макроса
3. Заблокируйте запуск вредоносного макроса Защитой от эксплоитов

Лабораторная работа №6

Как проверить Защиту от эксплоитов

1. Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру
2. Включите защиту от эксплоитов

Что нового в Kaspersky Security Center 11

- Операционные системы
- New Web Console
- Изменения в интерфейсе MMC-консоли администрирования
- Поддержка DIFF-файлов обновлений
- Изменения в работе Агентов обновлений
- Обратная совместимость плагинов KES
- Улучшения в RBAC



Что нового в Kaspersky Endpoint Security 11.1

- Операционные системы
- Новые компоненты KES
- Компонент AMSI Protection Provider
- Компонент Adaptive Anomaly Control
- Проверка зашифрованного трафика**
- Защита от MAC Spoofing
- Role Based Access Control for KES

Как работает защита от сетевых угроз?

Фильтр соединений

Перехватывает
исходящие
соединения по
протоколу TCP

Фильтр портов

Проверяет соединения
на **заданные порты**

Обработчик протоколов

Извлекает данные из
протоколов:

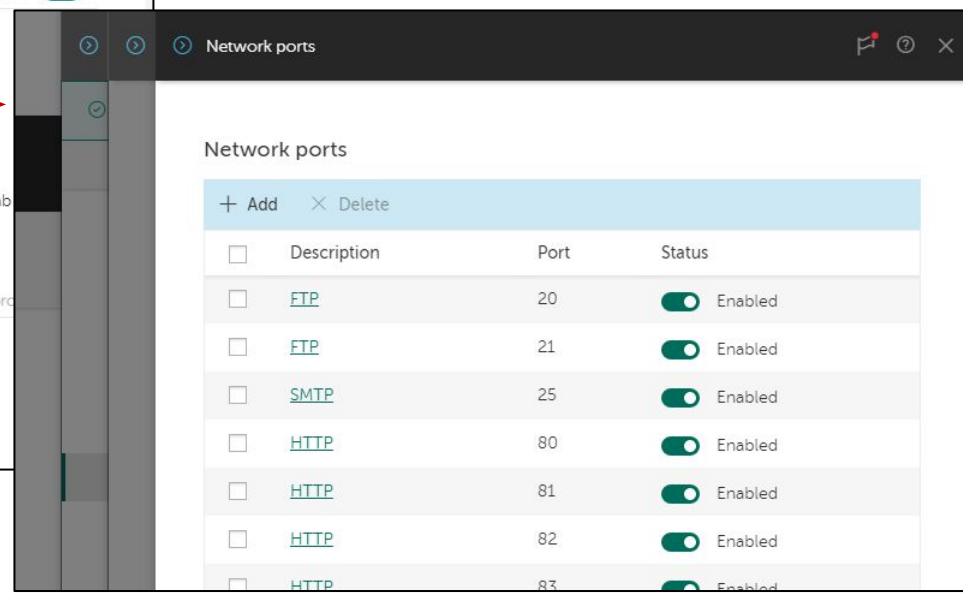
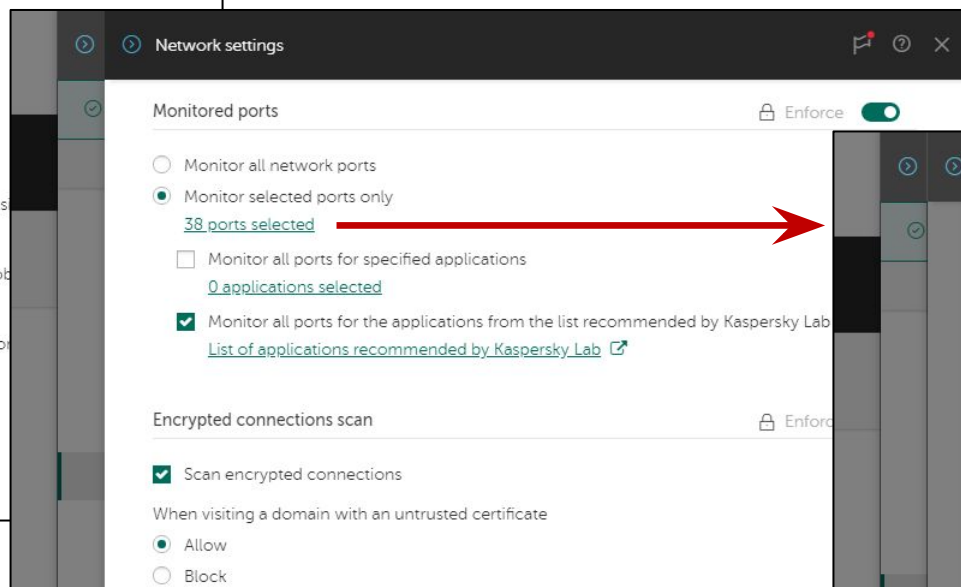
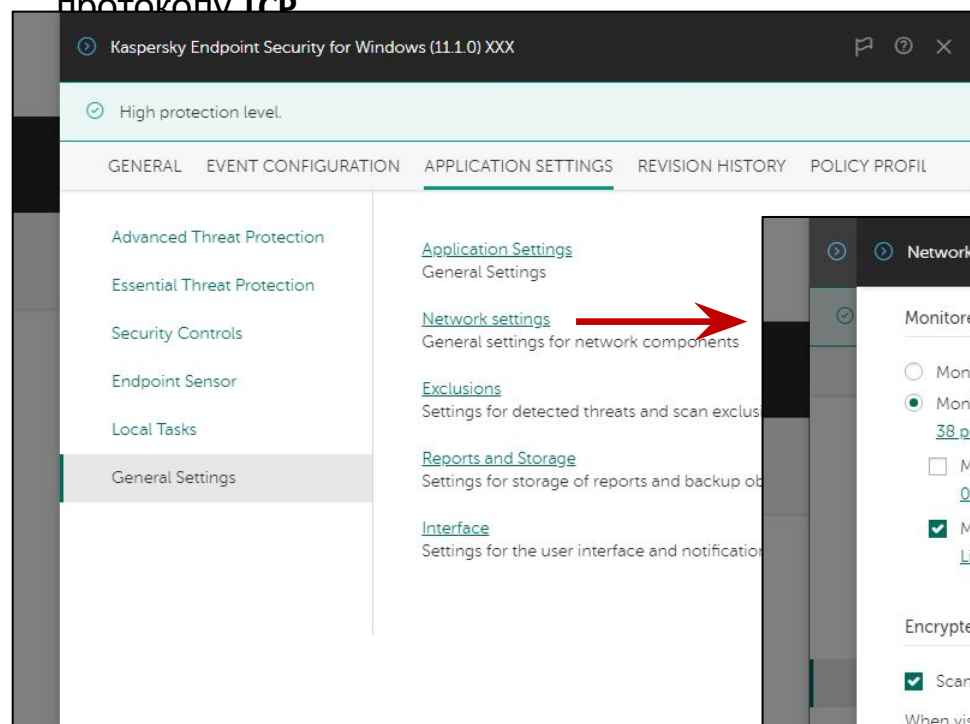
- HTTP, HTTPS, FTP
- SMTP, POP3, POP3S, IMAP, NNTP

Защита от веб-угроз

Веб-контроль

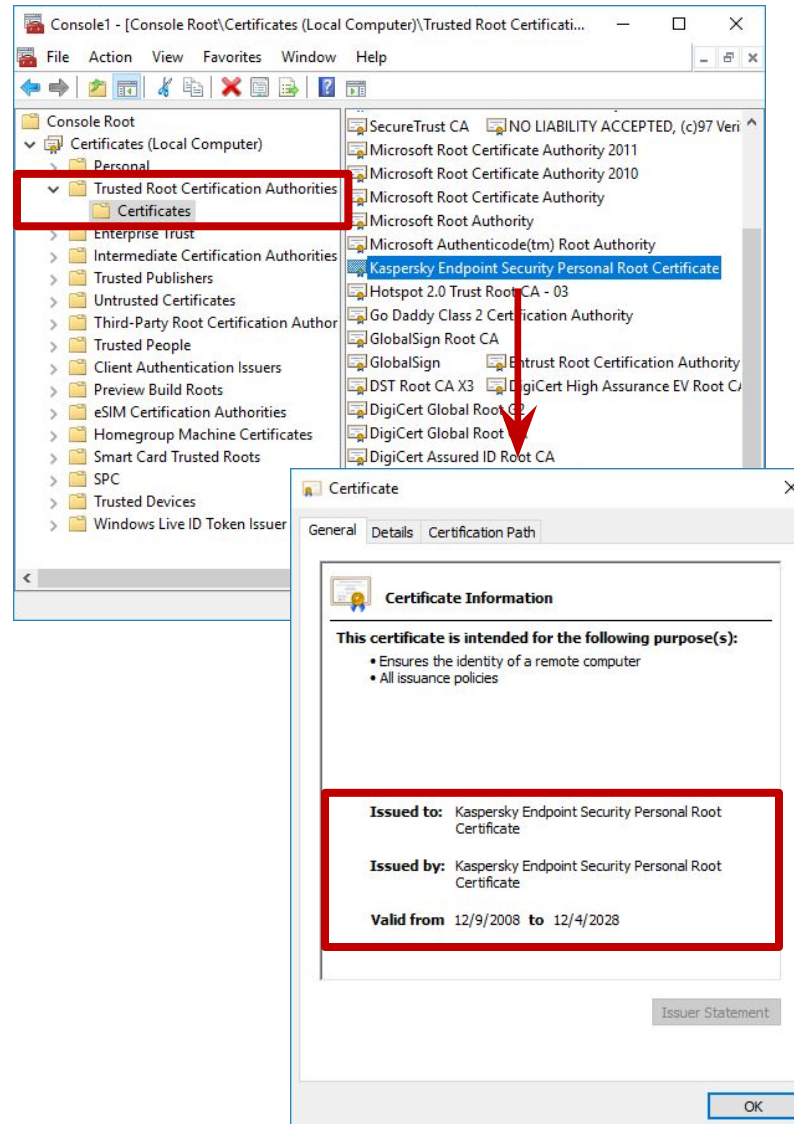
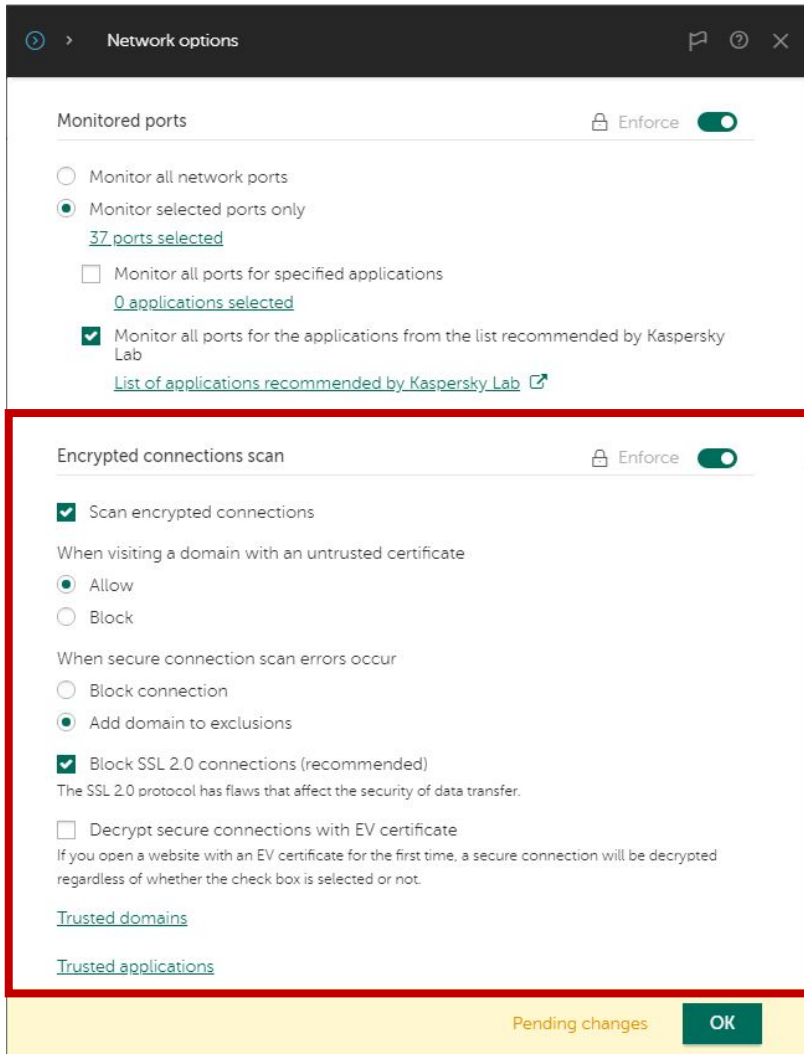
Защита от почтовых угроз

Проверяют защищенные соединения

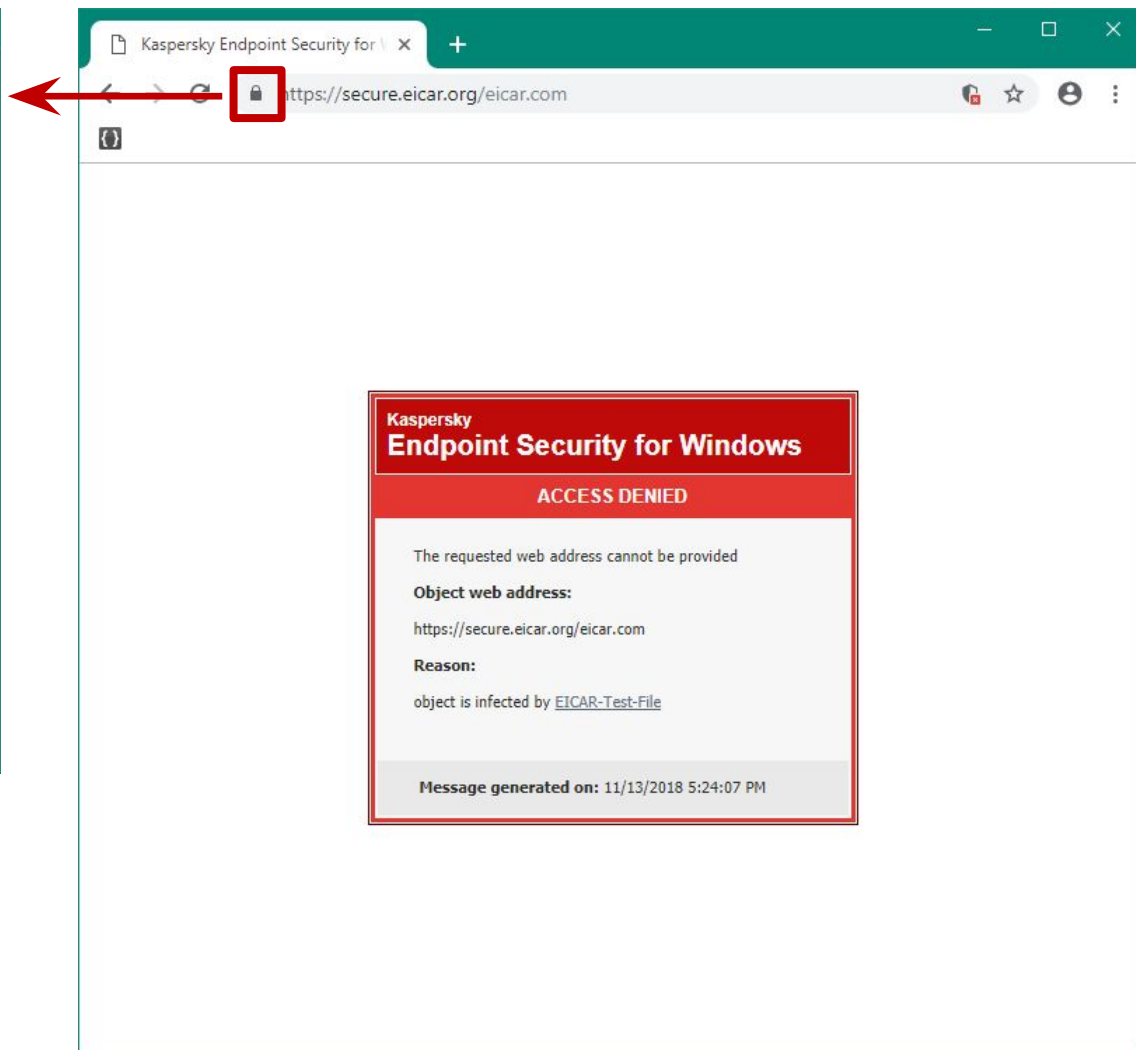
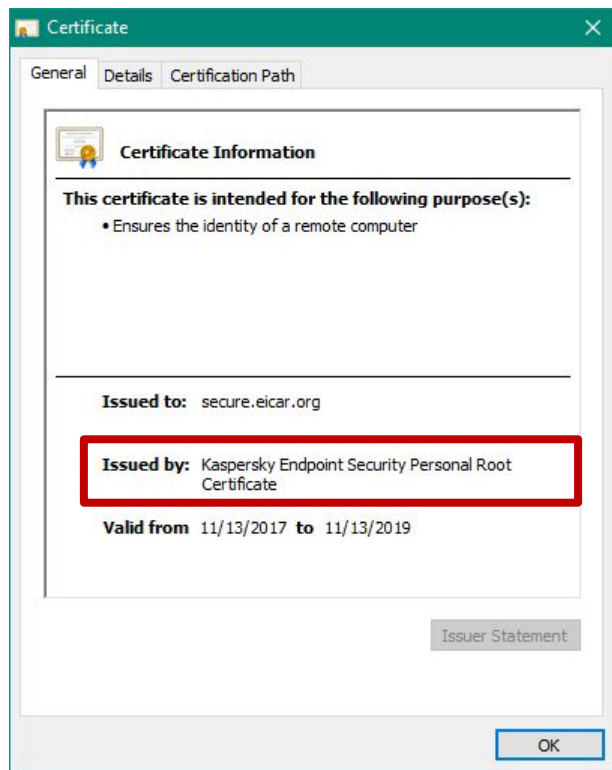


Kaspersky Endpoint Security 11.1: проверка шифрованного трафика

- Добавлена проверка зашифрованного трафика, основанная на подмене сертификатов
- KES создает сертификат при установке и помещает его в локальное хранилище Trusted Root Certification Authorities
- При каждом запуске KES проверяет наличие сертификата в хранилище и если его там нет восстанавливает

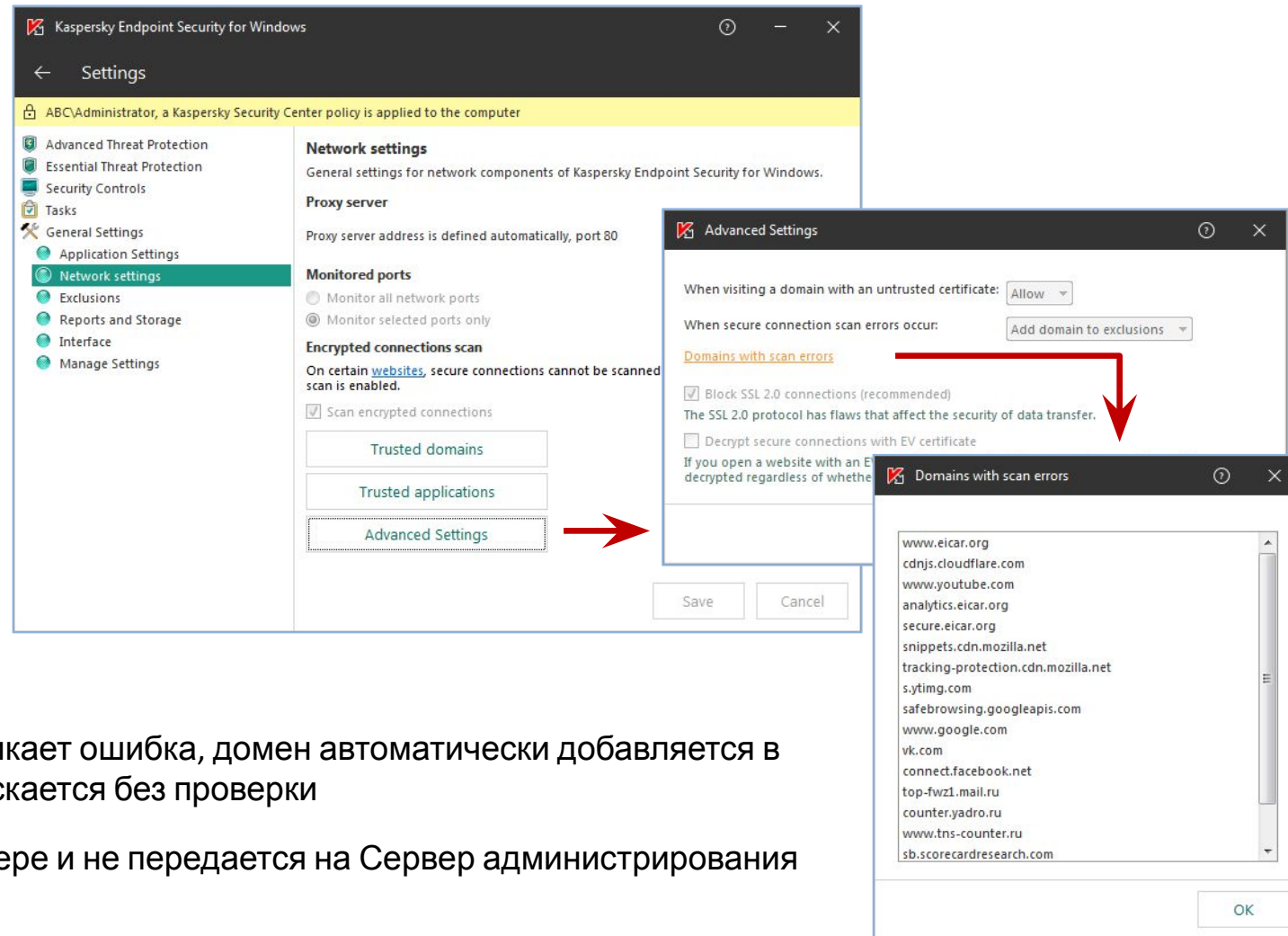
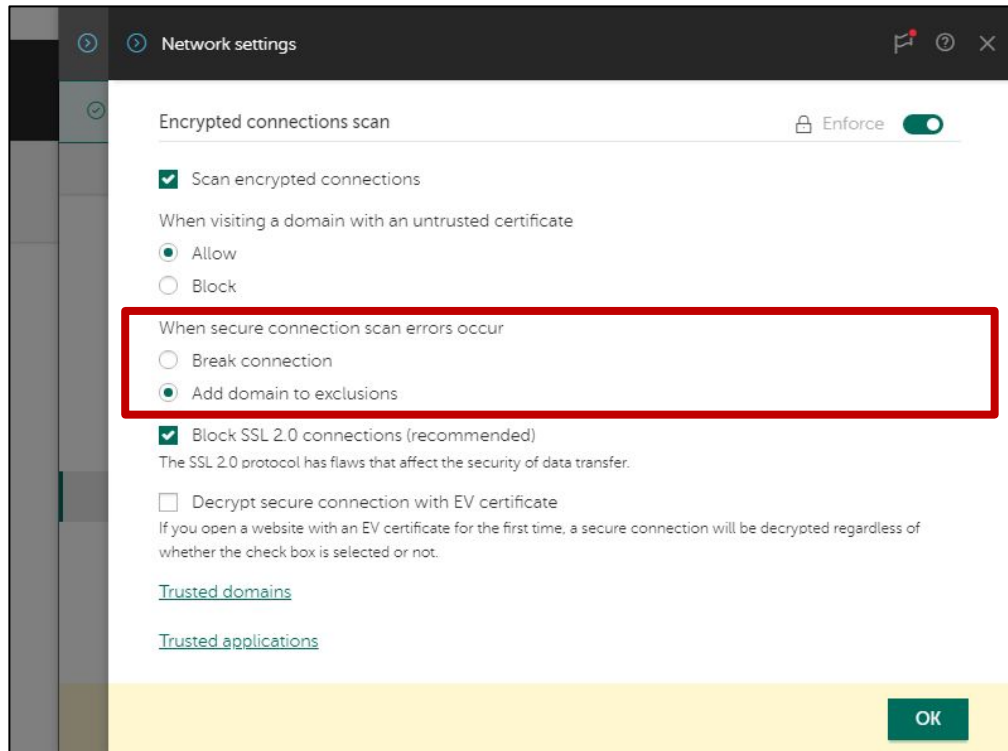


Web Threat Protection: подмена сертификата



- Kaspersky Endpoint Security Personal Root Certificate:
 - срок действия 10 лет
 - алгоритм шифрования SHA 256
 - длина ключа 2048 bits
- Проверка зашифрованного трафика влияет на работу следующих компонентов:
 - Web Threat Protection
 - Web Control
 - Mail Threat Protection

Что если при проверке защищенных соединений возникает ошибка?



Если при попытке проверки зашифрованного трафика возникает ошибка, домен автоматически добавляется в исключения и весь его трафик шифрованный трафик пропускается без проверки

Список исключения хранится локально на каждом компьютере и не передается на Сервер администрирования

Что если проверка зашифрованного трафика мешает работе программы?

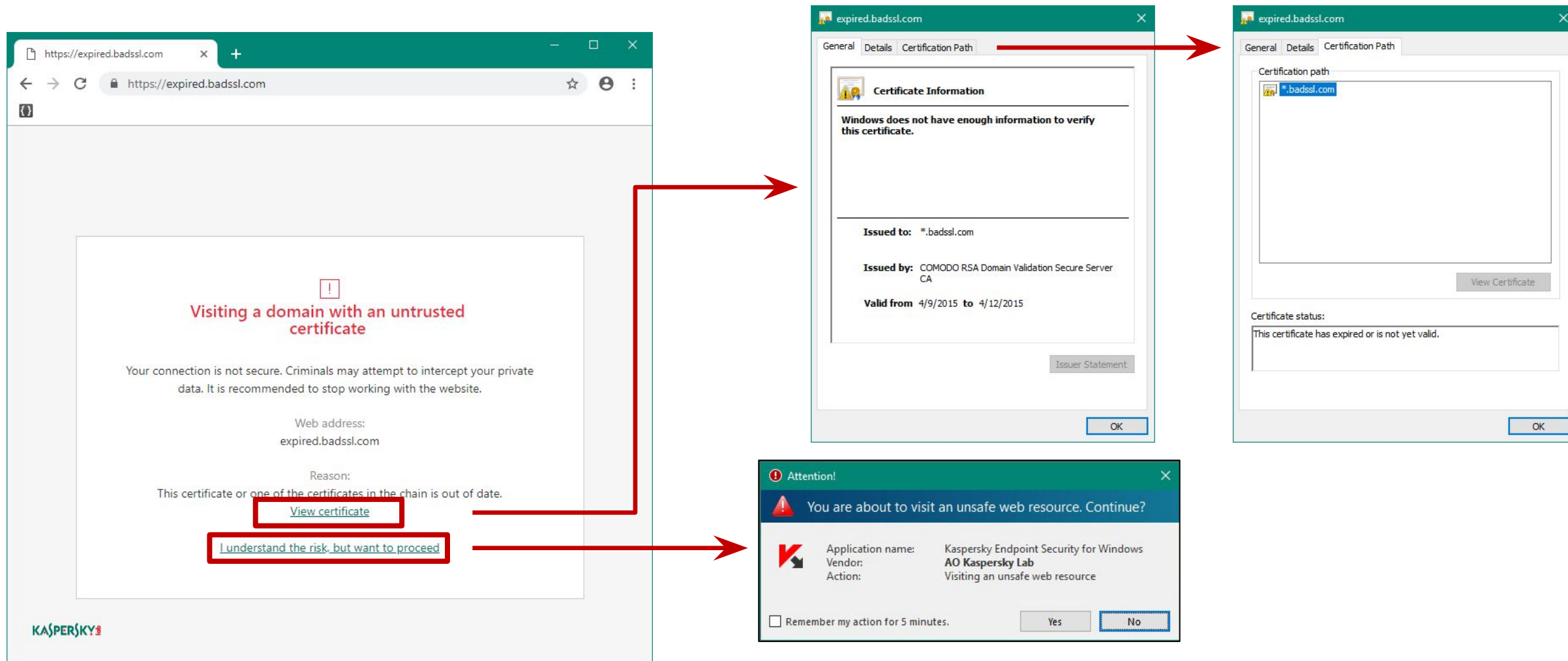
The image displays four windows from the Kaspersky Endpoint Security interface, illustrating how to configure settings to avoid interfering with program functionality while maintaining encrypted traffic scanning.

- Network settings:** Shows the 'Encrypted connections scan' section. The 'Enforce' toggle is turned on. Under 'When visiting a domain with an untrusted certificate', 'Allow' is selected. Under 'When secure connection scan errors occur', 'Add domain to exclusions' is selected. The 'Block SSL 2.0 connections (recommended)' checkbox is checked. A red arrow points from the 'Add domain to exclusions' option to the 'Trusted domains' window.
- Trusted domains:** A window showing a list of domains. The 'Add' button is highlighted with a red arrow pointing to the 'Add domain' dialog. The list contains two domains: `*.secure.eicar.org` and `*.eicar.org`, both with 'Enabled' status.
- Add domain:** A dialog box for adding a new domain. The 'Domain' field contains `*.secure.eicar.org`. The 'Status' is set to 'Enabled'.
- Trusted applications:** A window showing a list of applications. The 'Add' button is highlighted with a red arrow pointing to the 'Add domain' dialog. The list is currently empty.
- Application:** A window showing settings for a specific application. The 'Path or path mask to the application' is `C:\Program Files (x86)\ABC_Bank\client.exe`. The 'Do not scan network traffic' checkbox is checked. The 'Encrypted traffic only' radio button is selected. A red arrow points from the 'Do not scan network traffic' checkbox to the 'Application' window.

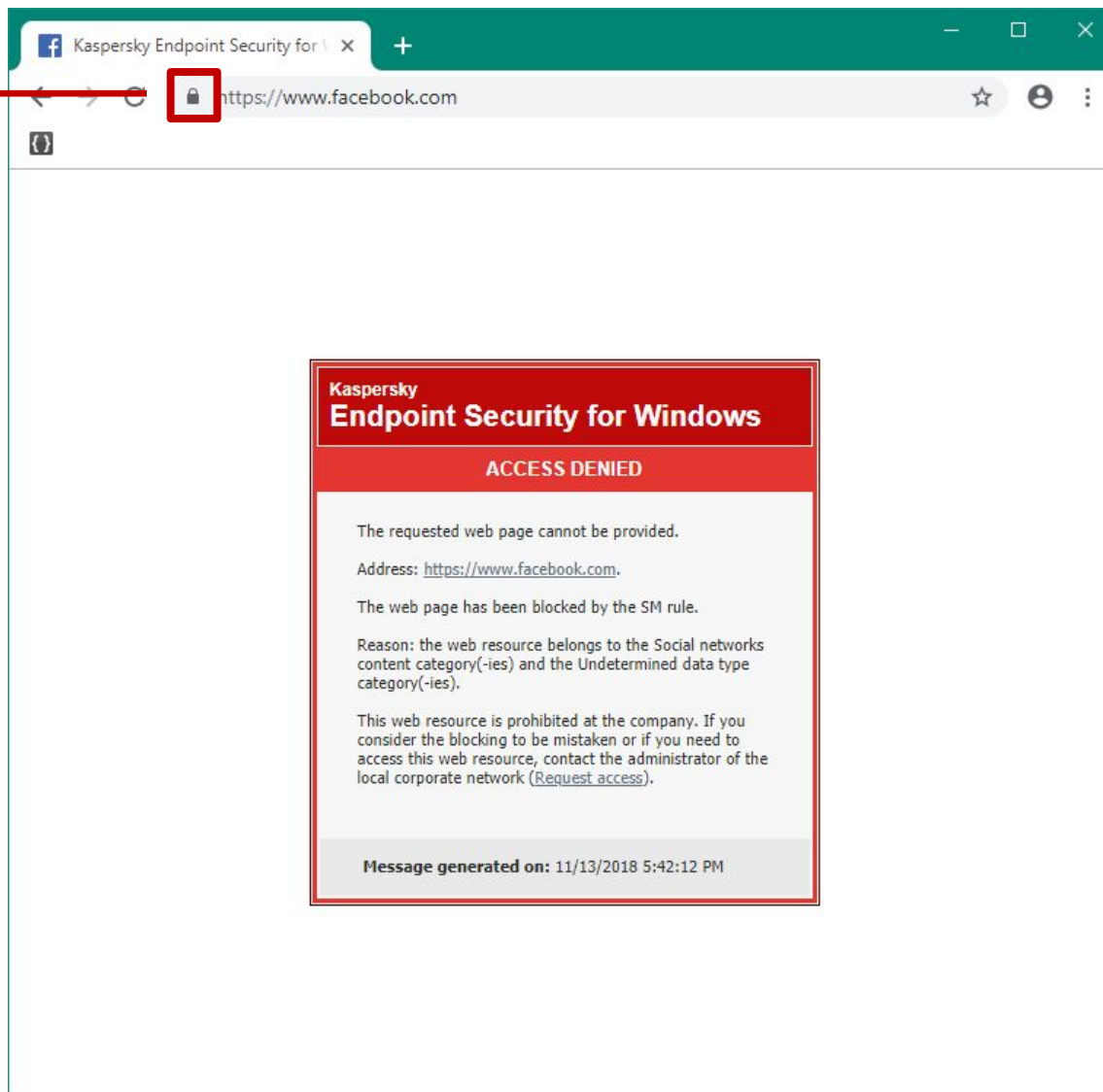
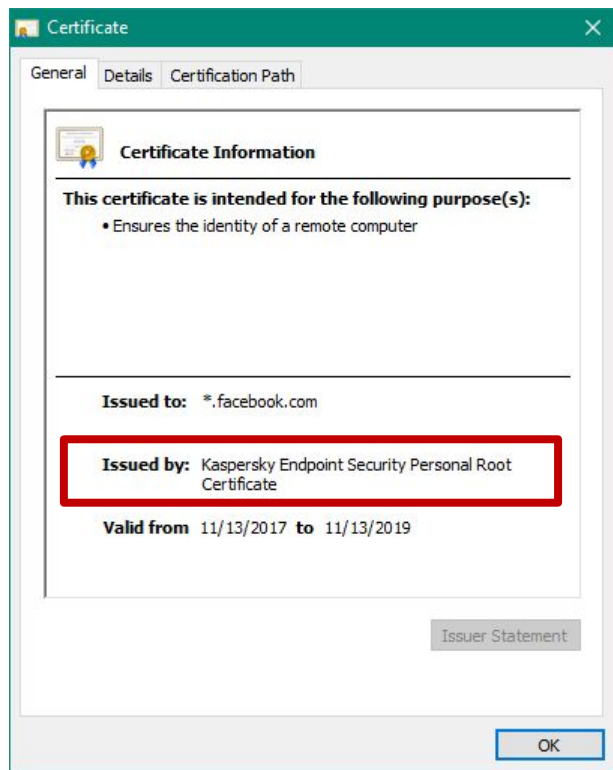
Не отключаете проверку зашифрованного трафика полностью

Настройте исключения для конкретных доменов и приложений

Проверка https-трафика: проблемы сертификата Веб-сайта



Web Control: проверка https-трафика



Web Control: новая категория

The image shows the Kaspersky Endpoint Security for Windows (11.1.0) interface. The main window displays the 'APPLICATION SETTINGS' tab, with 'Web Control' highlighted in the left sidebar. A red arrow points from 'Web Control' in the sidebar to the 'Web Control' settings window. In this window, 'Web Control' is enabled, and the 'Rule List' table is empty. A red arrow points from the '+ Add' button in the 'Rule List' to the 'Rule' configuration window. In the 'Rule' window, the 'Content categories' link is highlighted, and a red arrow points to the 'Content categories' dialog box. In this dialog box, the 'Cryptocurrencies and mining' category is highlighted with a red rectangle.

Kaspersky Endpoint Security for Windows (11.1.0)

High protection level.

GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY

Advanced Threat Protection
Essential Threat Protection
Security Controls
Endpoint Sensor
Local Tasks
General Settings

Web Control

Web Control ENABLED
This component allows you to control access to web resources.

Web Control Settings

Rule List

Rule name	State
No data	

Default rule

☒ Allow all except the rules list
☐ Deny everything except the rules list

Warning Blockage Message to administrator

Template of the warning message that appears when attempt

Rule

Rule name

Status

☒ Active
☐ Inactive

Action

☒ Allow
☐ Block
☐ Warn

Filter type

☐ By content categories
☐ By types of data

Content categories

Types of data

Addresses

☒ Apply to all addresses
☐ Apply to individual addresses and/or groups

+ Add Edit Delete

Address

Content categories

- ☐ Internet communication
 - ☐ Web-based email
 - ☐ Social networks
 - ☐ Chats and forums
 - ☐ Blogs
 - ☐ Dating sites
- ☐ Online stores, banks, payment systems
 - ☐ Online stores
 - ☐ Banks
 - ☐ Payment systems
- ☐ Cryptocurrencies and mining
- ☐ Computer games
- ☐ Religions, religious associations
- ☐ News media
- ☐ Banners
- ☐ Regional legal restrictions

OK

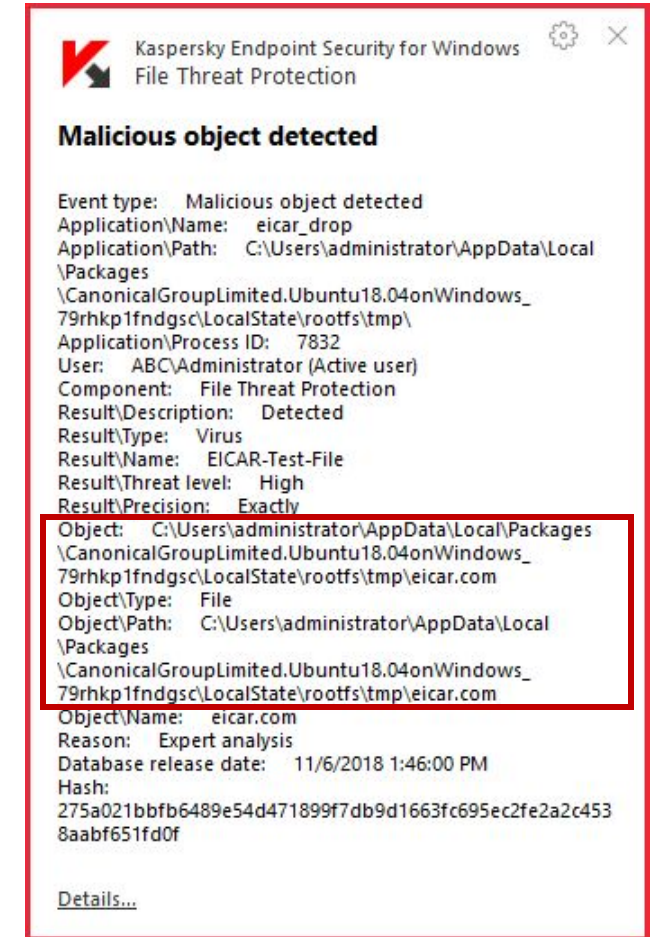
Как проверить защиту от веб-угроз



1. Проверьте, что Защита от веб-угроз проверяет https трафик
2. Выключите проверку шифрованного трафика для программы PowerShell

Kaspersky Endpoint Security 11.1: поддержка Windows Subsystem for Linux (WSL)

```
vb@ABC-Test: /tmp
vb@ABC-Test:~$ cd /tmp/
vb@ABC-Test:/tmp$ ls
eicar_drop_kl_edu.cpp  eicar_dropper
vb@ABC-Test:/tmp$ eicar_dropper
eicar_dropper: command not found
vb@ABC-Test:/tmp$ g++ eicar_drop_kl_edu.cpp -o eicar_drop
vb@ABC-Test:/tmp$ eicar_drop
eicar_drop: command not found
vb@ABC-Test:/tmp$ ls
eicar_drop  eicar_drop_kl_edu.cpp  eicar_dropper
vb@ABC-Test:/tmp$ ./eicar_drop
  +hdNNd+  :hNNmhs-
    oNMMMM/      -mMMMMy`
  /MMsdMN:/osyss+:dMN/MMy      DEMO eicar dropper 0.1
  oMM-/MMMMmdhhmMMMMs`NMd
  `mNNMMh/` DEMO :sNNMMM:
    /MMM+  EICAR  -mMMY
  /MNhoMMMMMMdyssyhMMMMMMyyMy
  `/smMMm`-/-oyyNMyyss+:. yMMmy/.
    :MM+      yMM      .MMs
    oMM-      yMM      MMy
  :sssdMM:    yMM      `MMssso
  /hhhhMMY    yMM      /MMdhhy
    sMM:      yMM      `NMm
    `mMM/     yMM      .mMM-
  .sNNMMh-    yMM      `sMMMMNy:
  :NMd+`-hMMms/dMM/ohMMm/ :yMMo
  ..      .+hMMMMMMNds-
    `...`
vb@ABC-Test:/tmp$
```



Как проверить защиту от файловых угроз



1. Проверить, что Kaspersky Endpoint Security умеет обнаружить вредоносные файлы, которые запускаются в Windows Subsystem for Linux
2. Изучите события защиты от файловых угроз

Что нового в Kaspersky Security Center 11

- Операционные системы
- New Web Console
- Изменения в интерфейсе MMC-консоли администрирования
- Поддержка DIFF-файлов обновлений
- Изменения в работе Агентов обновлений
- Обратная совместимость плагинов KES
- Улучшения в RBAC



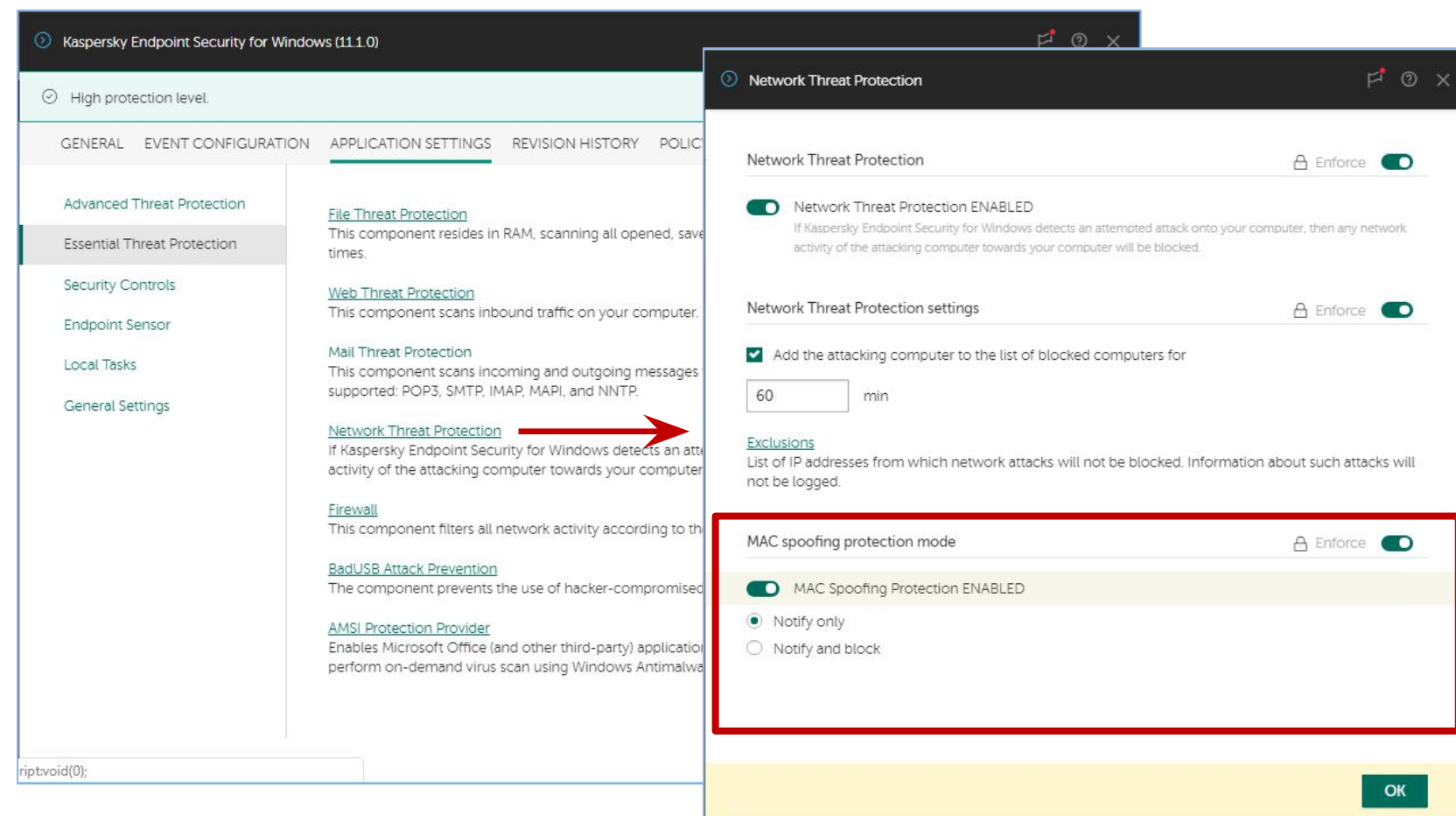
Что нового в Kaspersky Endpoint Security 11.1

- Операционные системы
- Новые компоненты KES
- Компонент AMSI Protection Provider
- Компонент Adaptive Anomaly Control
- Проверка зашифрованного трафика
- Защита от MAC Spoofing**
- Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: защита от MAC Spoofing

Предотвращает подмену адресов в ARP-таблице, принимая только те ответы, для которых был отправлен запрос

После выполнения ARP-запроса все ответы кроме первого игнорируются



Что нового в Kaspersky Security Center 11

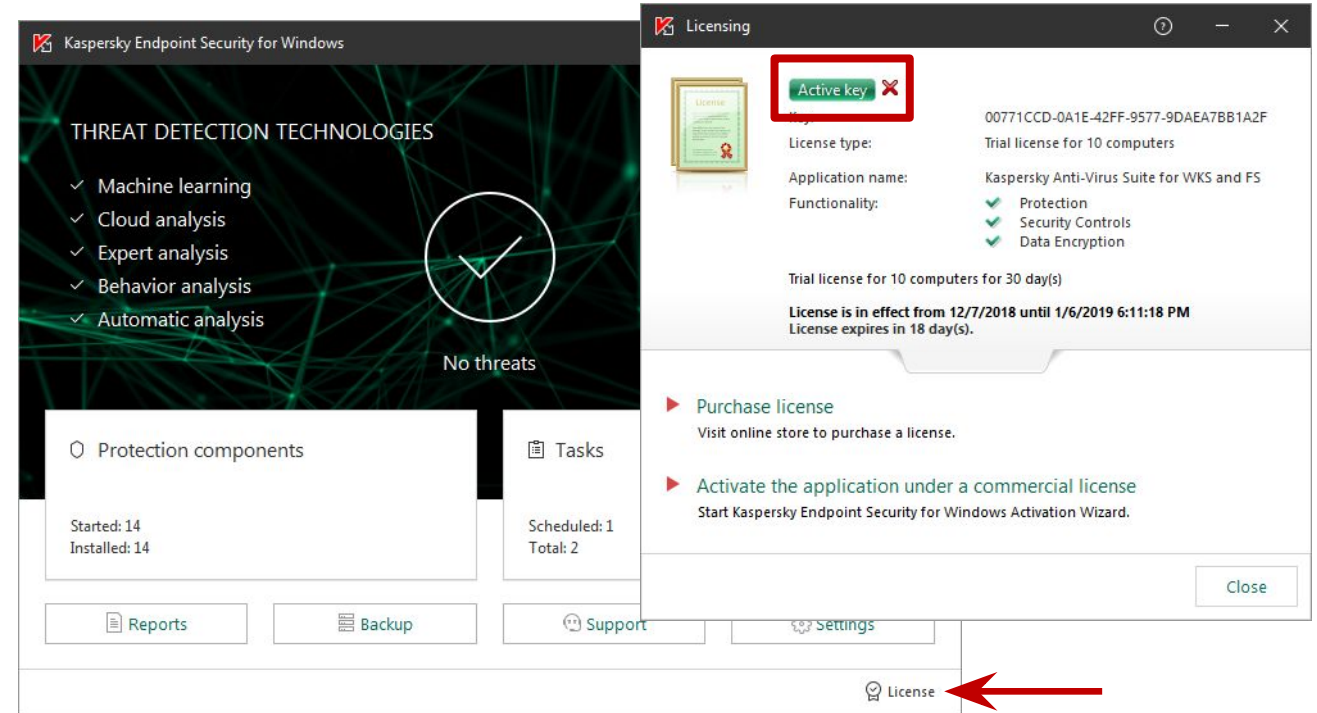
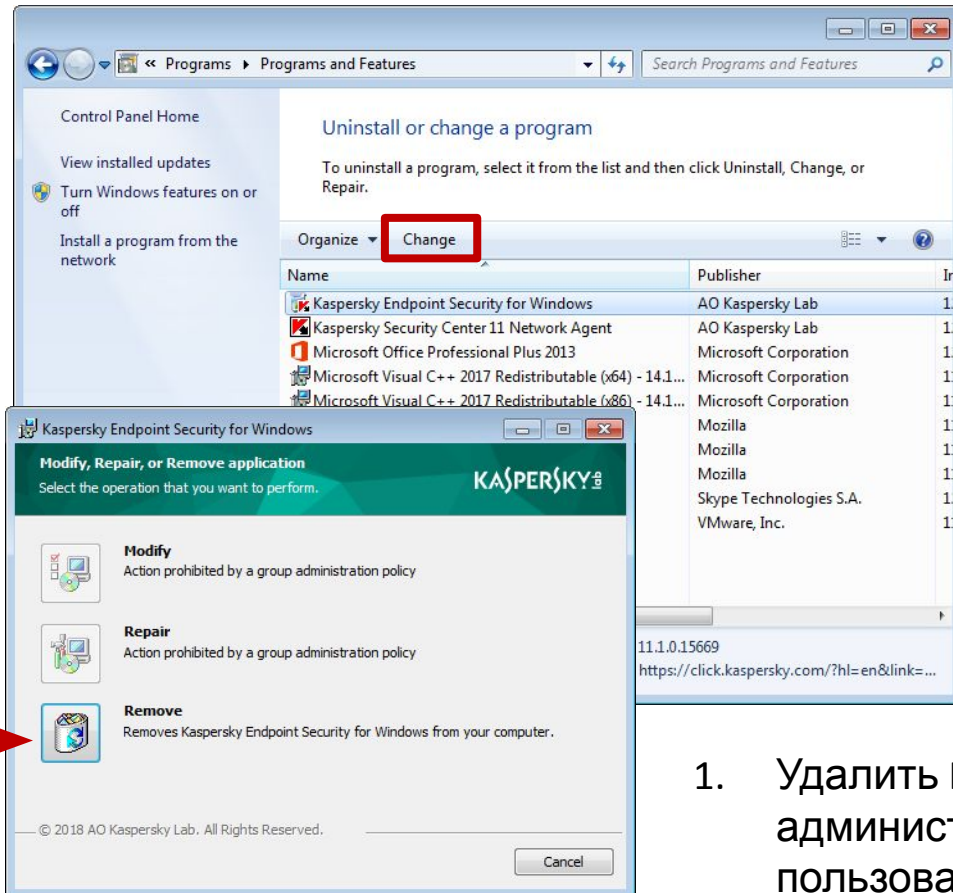
Операционные системы
New Web Console
Изменения в интерфейсе MMC-консоли администрирования
Поддержка DIFF-файлов обновлений
Изменения в работе Агентов обновлений
Обратная совместимость плагинов KES
Улучшения в RBAC



Что нового в Kaspersky Endpoint Security 11.1

Операционные системы
Новые компоненты KES
Компонент AMSI Protection Provider
Компонент Adaptive Anomaly Control
Проверка зашифрованного трафика
Защита от MAC Spoofing
Role Based Access Control for KES

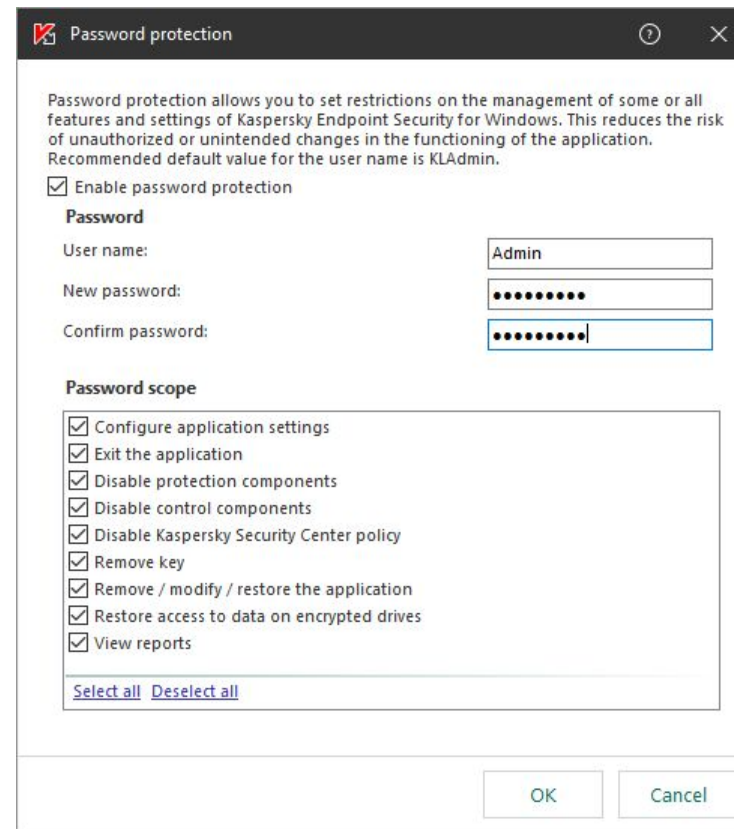
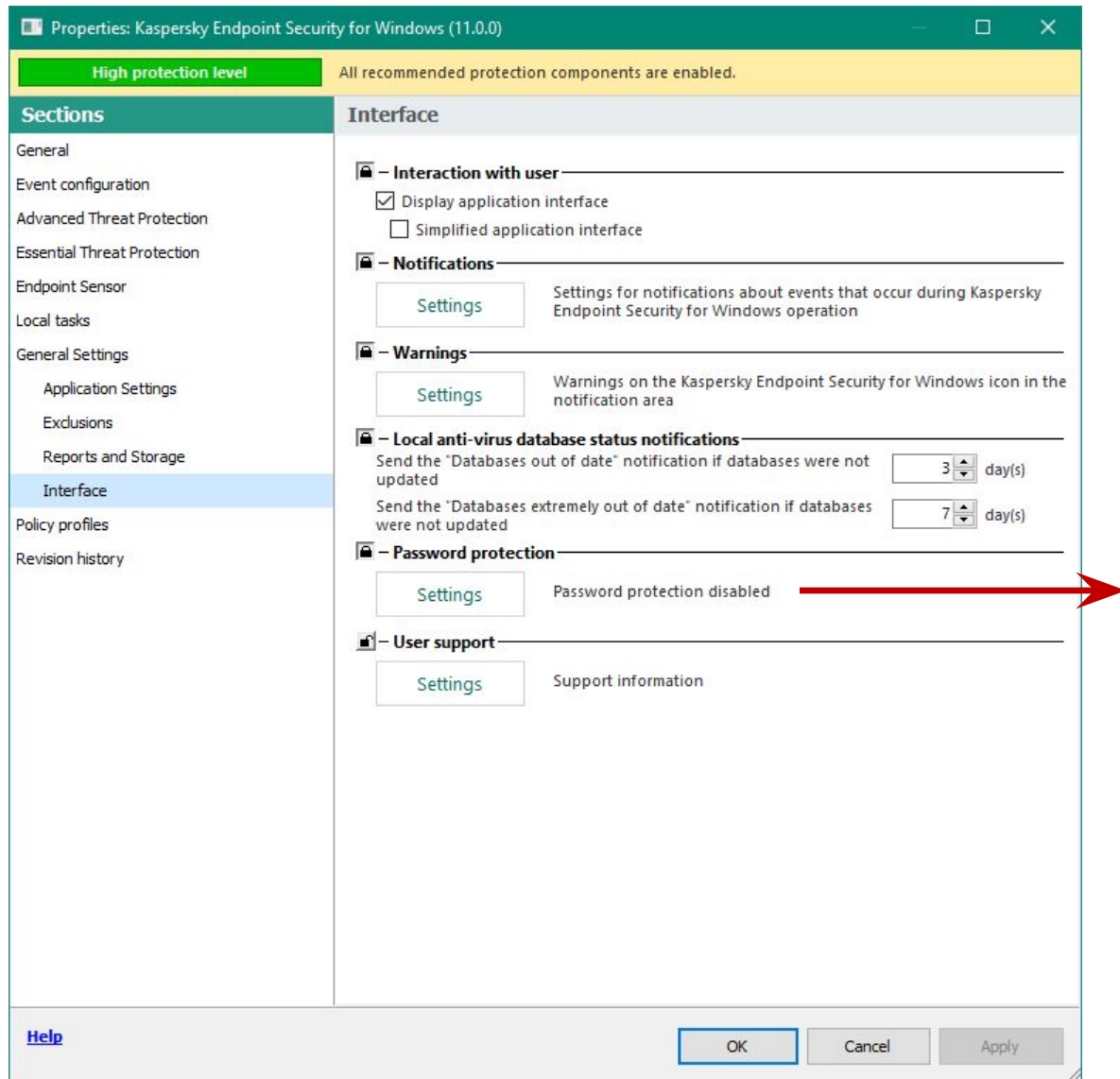
Как пользователь может помешать защите?



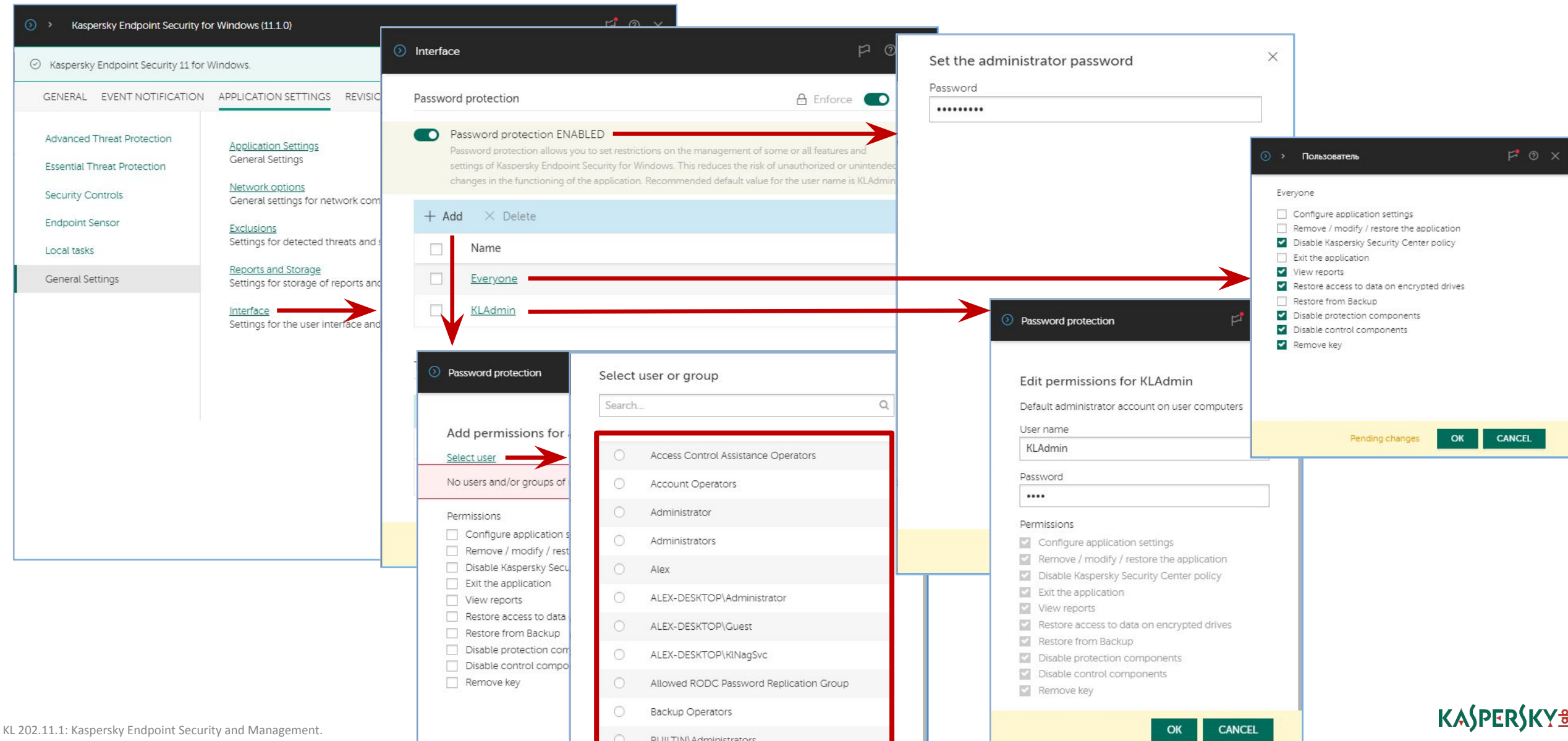
1. Удалить Kaspersky Endpoint Security или Агент администрирования. Без Агента не применяется политика и пользователь сможет менять настройки
2. Удалить лицензию: компоненты остановятся
3. Выйти из Kaspersky Endpoint Security: защита остановится



Kaspersky Endpoint Security 11.0: доступ по паролю к локальному интерфейсу KES



Kaspersky Endpoint Security 11.1: доступ по паролю к локальному интерфейсу KES



Kaspersky Endpoint Security 11.1: поддержка миграции

- При обновлении версии KES больше не нужно расшифровывать зашифрованные диски, если он зашифрован с помощью Kaspersky Full Disk Encryption
- Улучшена поддержка миграции с Windows 7 / 8 / 8.1 на Windows 10

Kaspersky Endpoint Security 11.1: ИТОГО

- Появились новые компоненты:
 - AMSI Protection Provider
 - Adaptive Anomaly Control
- Реализована проверка HTTPS-трафика
- Реализована поддержка Windows Subsystem for Linux (WSL)
- Реализована защита от MAC Spoofing
- Изменена модель доступа по паролю к локальному интерфейсу KES
- Реализована поддержка Kaspersky Full Disk Encryption при обновлении версий
- Улучшена поддержка миграции с Windows 7 / 8 / 8.1 на Windows 10
- Появилась новая категория Web Control, связанная с криптовалютами и майнингом



Лабораторная работа №9

Как проверить защиту сетевых папок от программ-вымогателей

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



Лабораторная работа №10

Как проверить защиту от сетевых атак

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