

نصب و مدیریت Kaspersky Security Center

تهیه کنندگان:

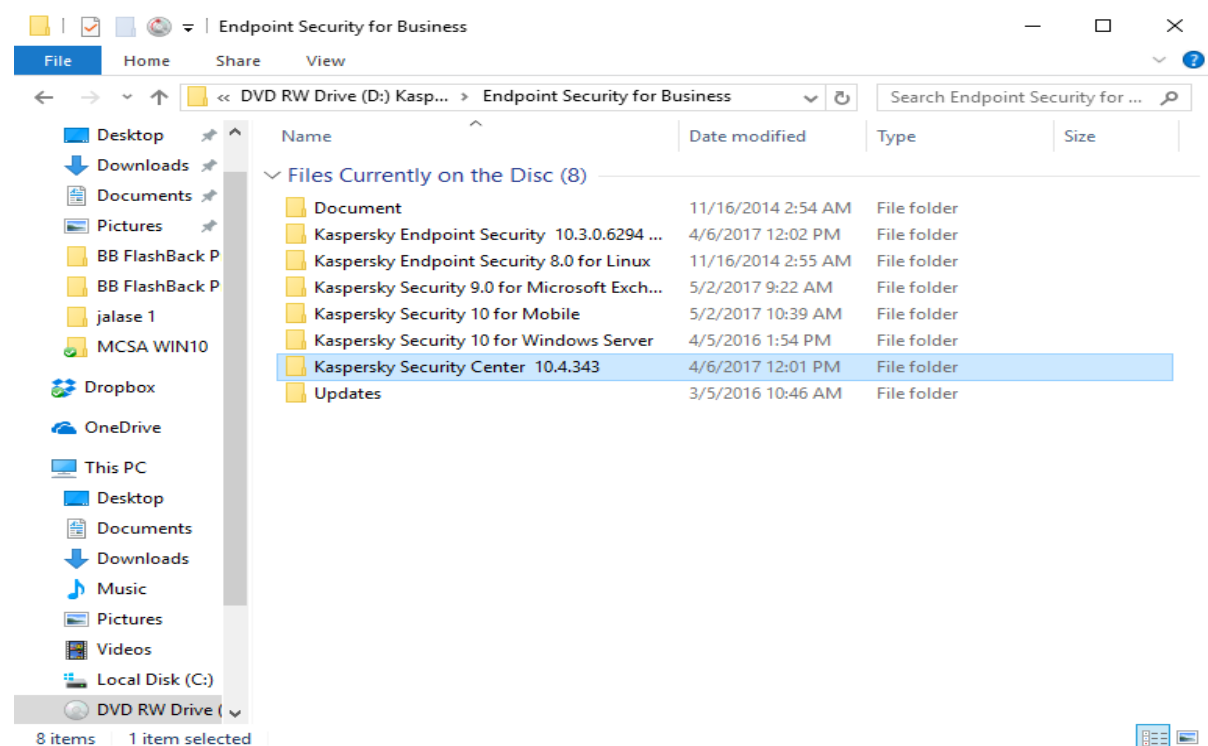
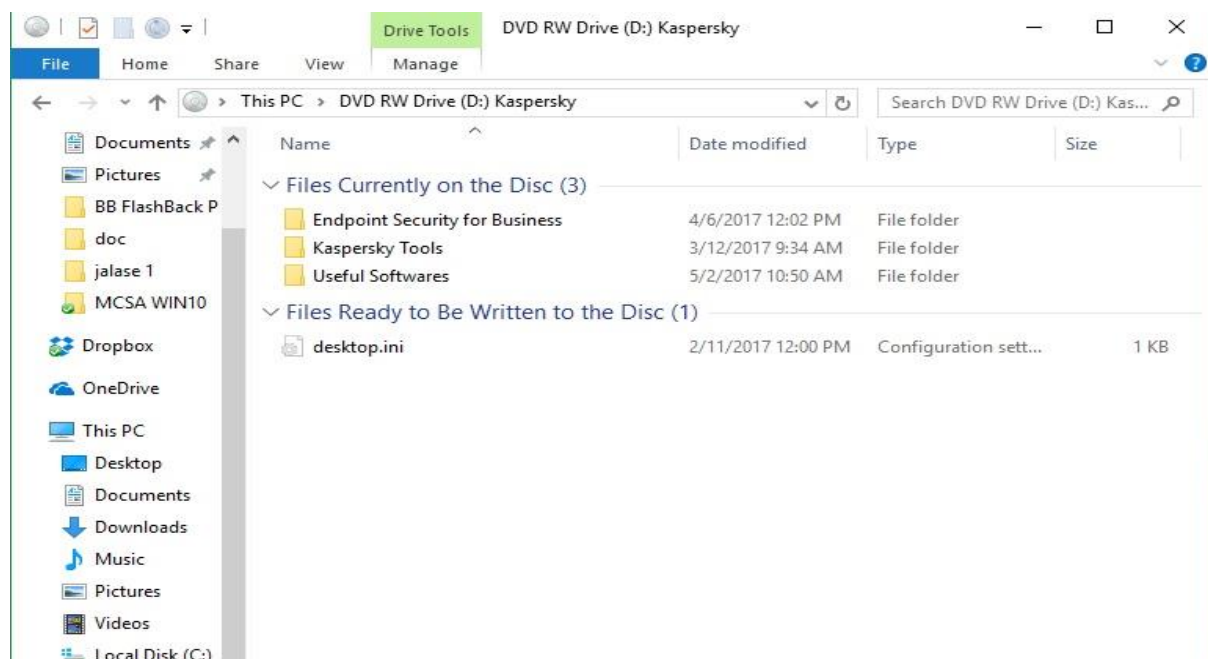
حسین ظفری

مرجان امیری

خرداد ماه 96

نصب سرور کسپرسکی (Kaspersky Security Center):

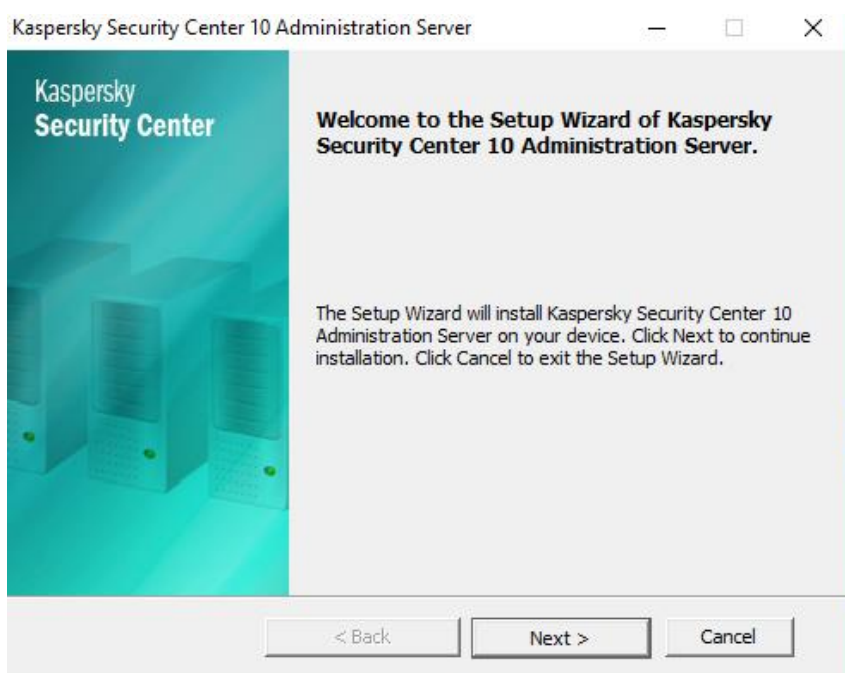
جهت نصب کنسول مرکزی آنتی ویروس، وارد DVD دریافتی شده و مانند تصاویر زیر از درون پوشه Endpoint Security for Business پوشه Kaspersky Security Center 10.4.343 را باز کرده و فایل اجرایی موجود در این مسیر را اجرا کنید.



با اجرای این فایل، ویزاردی برای شما باز خواهد شد که با اجرای Install Kaspersky Security Center 10 فایل های موجود بر روی بسته از حالت فشرده خارج و بلافاصله فایل نصب اجرا خواهد گردید. مراحل نصب را بر اساس تصاویر ذیل ادامه دهید.



در این مرحله نصب اصلی کنسول آغاز می شود:



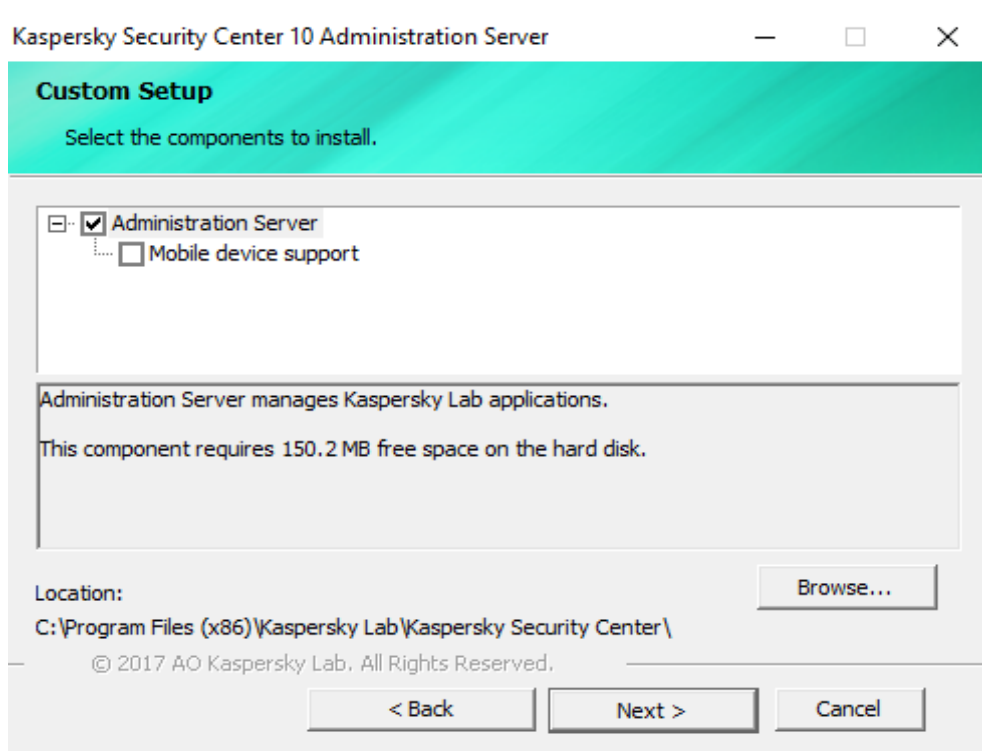


عملیات نصب را به صورت Custom ادامه دهید.

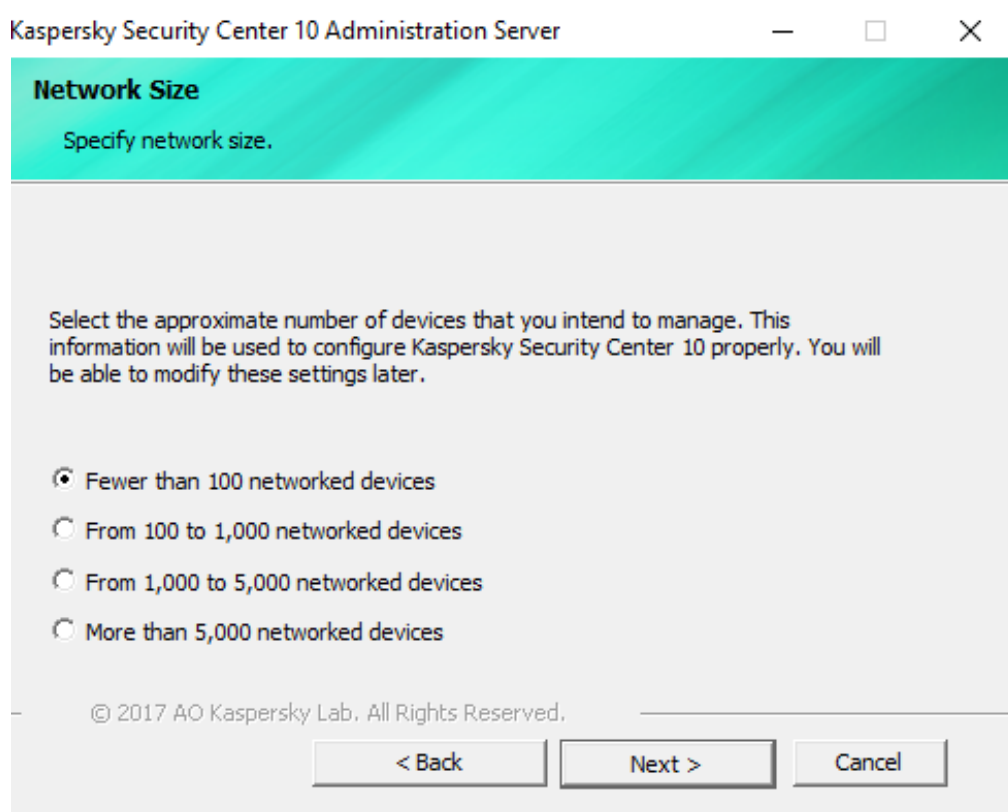


در این قسمت شما Component های مورد نیاز برای نصب Security Center را انتخاب می نمایید. در صورتیکه این سیستم سرور اصلی آنتی ویروس شما می باشد، نصب را به همین صورت انجام دهید. در زیر توضیح کوتاهی از Component های موجود خواهید دید.

- **Administration server**: این Component که اصلی ترین Component نصب Security Center می باشد، سرویسی است که مسئولیت مدیریت نرم افزارهای نصب شده کسپرسکی در شبکه را به عهده دارد. این سرویس در هنگام نصب احتیاج به یک پایگاه داده برای ذخیره اطلاعات دارد. همزمان با نصب این Component نرم افزار Network Agent نیز بر روی این سرور نصب می شود که وظیفه برقراری ارتباط بین کلاینت ها و سرور آنتی ویروس را بر عهده دارد، علاوه بر این پس از نصب این نرم افزار بر روی کلاینت ها وظیفه ی انتقال فایل ها و اطلاعات بر عهده آن خواهد بود.
- **Mobile devices support**: با انتخاب این قسمت، شما اجازه مدیریت آنتی ویروس نصب شده بر روی دستگاه های Mobile را نیز از طریق کنسول Security center خواهید داشت.



در این مرحله بزرگی شبکه خود را مشخص کنید. برای این منظور از تعداد لایسنس خود استفاده کنید.



Kaspersky Security Center 10 Administration Server

Network Size

Specify network size.

Select the approximate number of devices that you intend to manage. This information will be used to configure Kaspersky Security Center 10 properly. You will be able to modify these settings later.

- Fewer than 100 networked devices
- From 100 to 1,000 networked devices
- From 1,000 to 5,000 networked devices
- More than 5,000 networked devices

© 2017 AO Kaspersky Lab. All Rights Reserved.

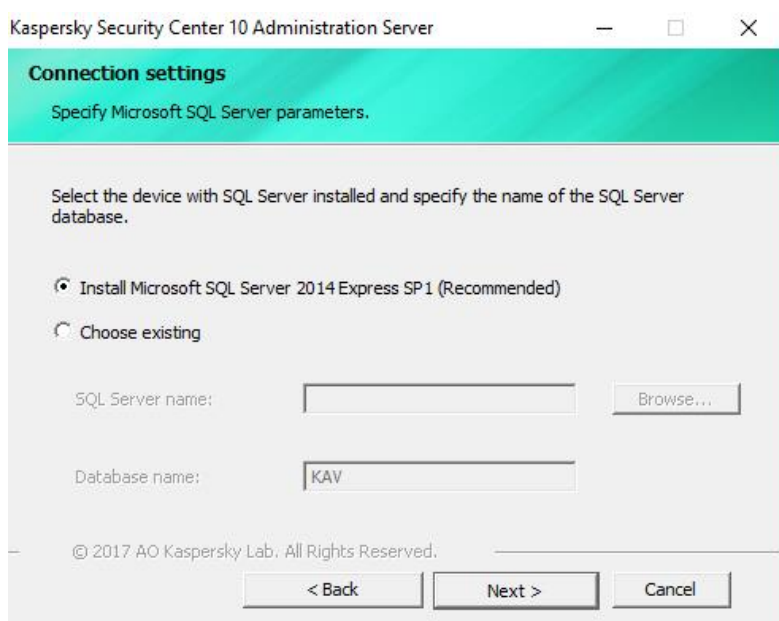
< Back Next > Cancel

در قسمت بعدی شما باید یک Account برای نصب سرویس انتخاب نمایید. در این قسمت تنظیمی انجام ندهید و به مرحله بعد بروید.

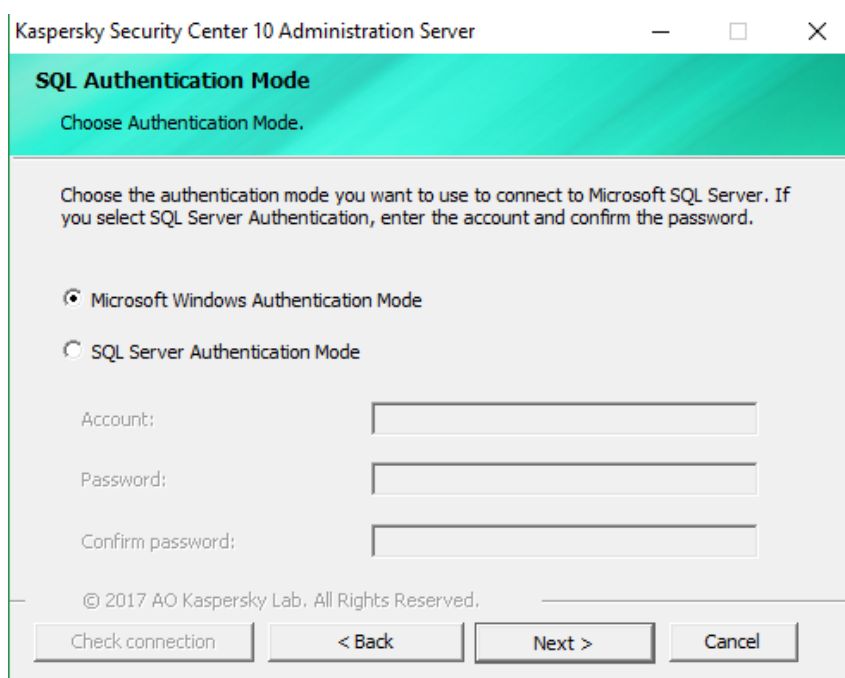


در این مرحله شما باید نوع پایگاه داده مورد نظر برای استفاده Security Center را مشخص کنید. پیشنهاد کسپرسکی استفاده از Microsoft SQL Server می باشد.

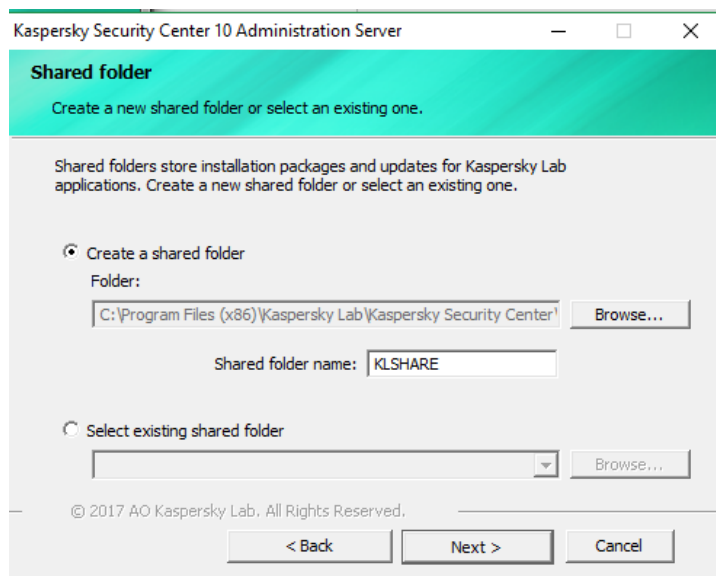
در این مرحله بگذارید خود کسپرسکی یک سرور SQL نسخه Express Edition برای شما نصب کند که این کار را به صورت اتوماتیک انجام میدهد، به مرحله بعد بروید.



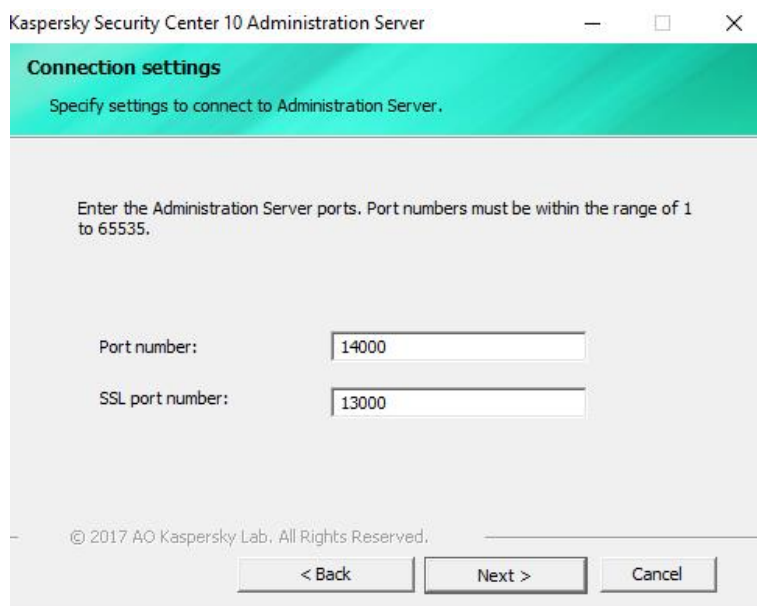
در این قسمت نحوه ی اتصال به SQL Server را مشخص کنید. اجازه دهید گزینه ی Windows Authentication Mode در حالت انتخاب باقی بماند.



کنسول کسپرسکی برای ذخیره ی فایل های به روز رسانی وبسته های نصب و ... از یک پوشه ی به اشتراک گذاشته شده استفاده می کند. این پوشه به صورت پیش فرض در مسیر نصب کنسول قرار می گیرد. این پوشه KLshare نام دارد. در این قسمت هم تغییری ندهید و به مرحله بعدی بروید.



برای ارتباط بین کلاینت و سرور، Network Agent از دو درگاه 13000 و 14000 استفاده می کند. درگاه پیش فرض برای اتصال 13000 می باشد که یک درگاه امن (SSL) است.



در مرحله بعد، شما باید نحوه ی ارتباط Network Agent نصب شده بر روی کلاینت ها با سرور را مشخص کنید.

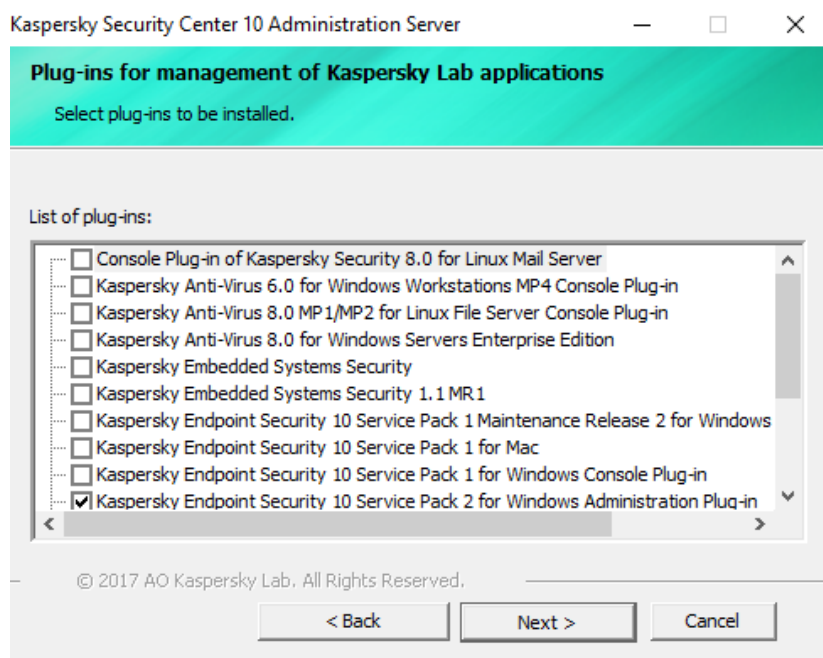
برای ارتباط با سرور، Network Agent می تواند از سه روش زیر استفاده کند:

- **IP Address**: بهترین حالت، استفاده از این گزینه می باشد. توجه داشته باشید و توجه داشته باشید که حتما IP را در این قسمت انتخاب کنید.
- **DNS Name**: زمانی که کنسول در شبکه ی Domain راه اندازی می شود، بهترین حالت استفاده از DNS می باشد. زیرا اگر IP سرور تغییر کند و یا حتی Range شبکه عوض شود، می توان با تغییر کوچکی در سرور DNS ارتباط کلاینت ها با سرور را مجدداً برقرار کرد.
- **Net Bios Name**: در این قسمت نام خود سرور را انتخاب میکنیم.

کسپرسکی به صورت پیش فرض از **IP Address** جهت برقراری ارتباط استفاده می کند.



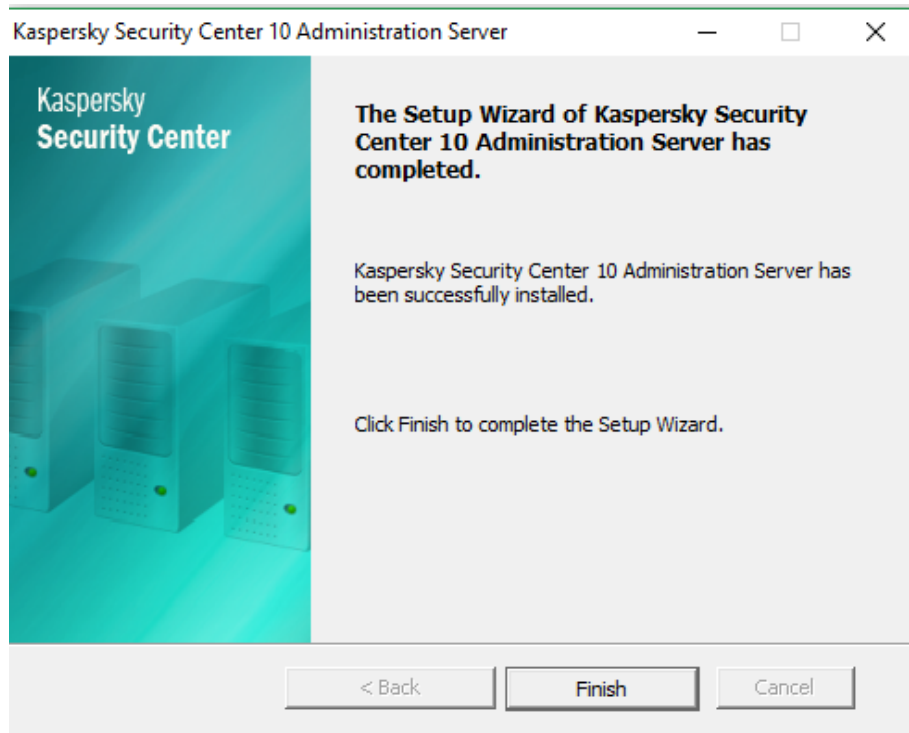
در قسمت بعد شما میتوانید Plugin های آنتی ویروس هایی از کسپرسکی را که میخواهید بر روی سیستم هایتان نصب کنید را انتخاب نمایید تا در زمان نصب کنسول آن ها نیز نصب شوند.



در ادامه بر روی گزینه Install کلیک نمایید تا نصب شروع شود.

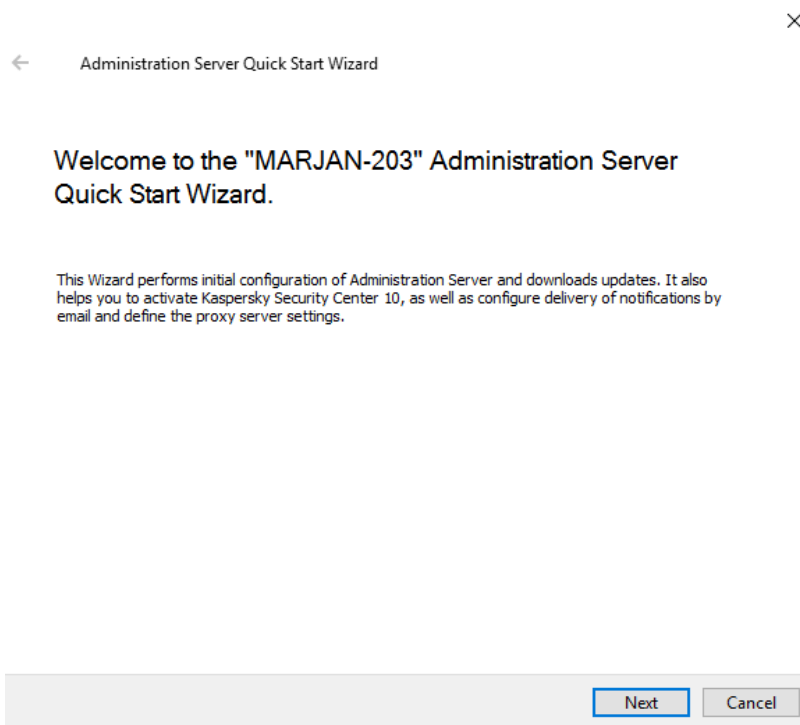


در انتهای نصب بر روی گزینه Finish کلیک کنید.

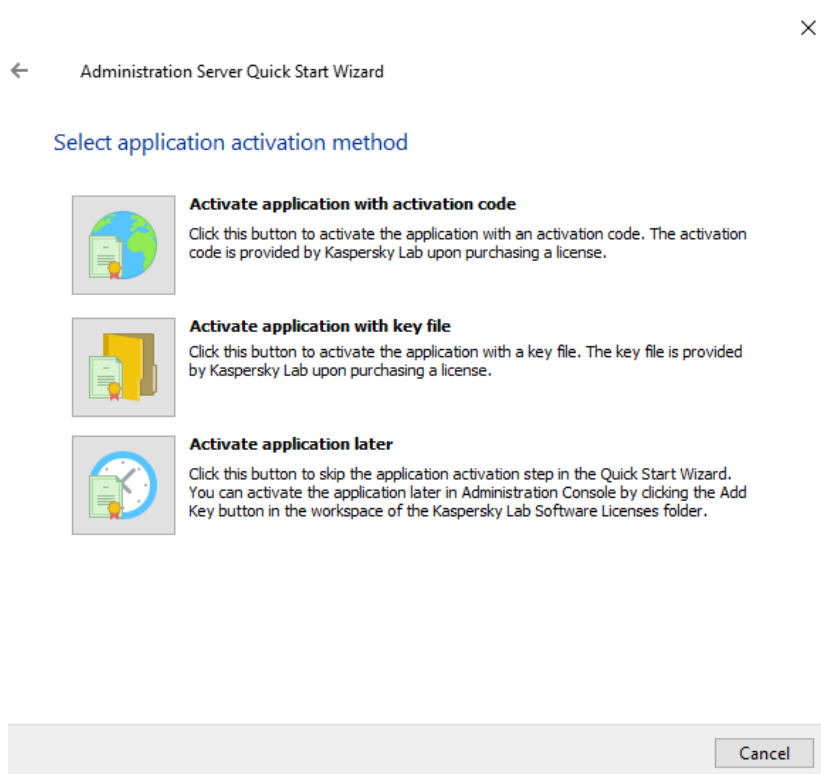


Quick Start Wizard

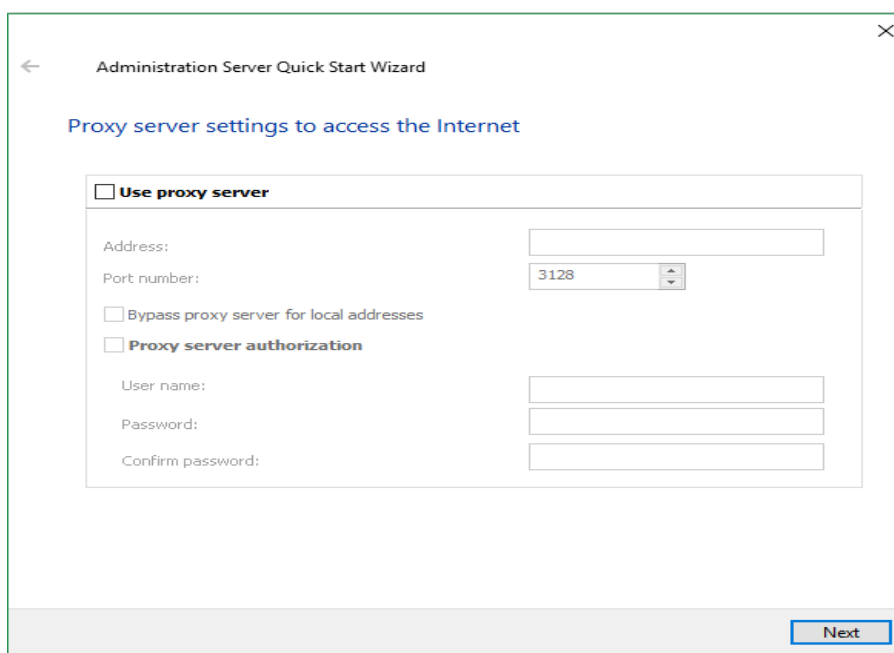
بازدن دکمه Finish در مرحله قبل پنجره Quick Start Wizard باز می شود Next را بزنید.



در مرحله بعد گزینه Activate application later را انتخاب نمایید تا به مرحله بعد بروید.



در این مرحله در صورتیکه سرور برای دسترسی به اینترنت از Proxy استفاده می کند، می بایست گزینه Use Proxy Server را فعال کنید و سپس IP Address و پورت آن را وارد کنید. در غیر این صورت به بخش بعدی بروید.



Administration Server Quick Start Wizard

Proxy server settings to access the Internet

Use proxy server

Address:

Port number:

Bypass proxy server for local addresses

Proxy server authorization

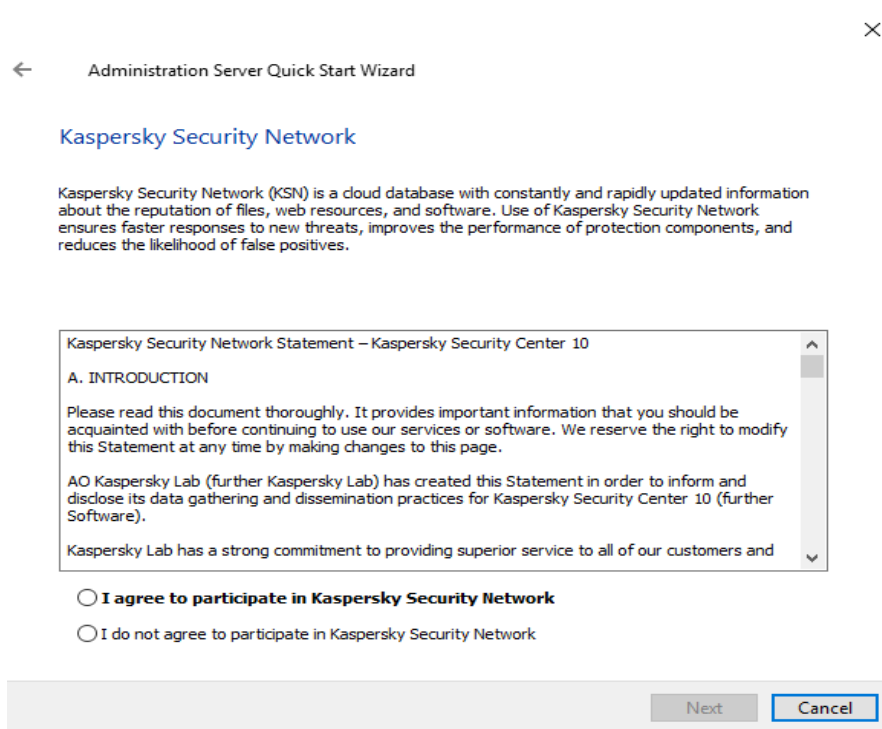
User name:

Password:

Confirm password:

Next

در قسمت بعدی که KSN است به دلیل اینکه سرور های کسپرسکی ادارات امور شعب و شعبه ها اینترنت ندارند شما نمیتوانید از این ابزار استفاده نمایید. بنابراین گزینه I do not accept to participate in kaspersky security network را انتخاب نمایید و به مرحله بعدی بروید.



Administration Server Quick Start Wizard

Kaspersky Security Network

Kaspersky Security Network (KSN) is a cloud database with constantly and rapidly updated information about the reputation of files, web resources, and software. Use of Kaspersky Security Network ensures faster responses to new threats, improves the performance of protection components, and reduces the likelihood of false positives.

Kaspersky Security Network Statement – Kaspersky Security Center 10

A. INTRODUCTION

Please read this document thoroughly. It provides important information that you should be acquainted with before continuing to use our services or software. We reserve the right to modify this Statement at any time by making changes to this page.

AO Kaspersky Lab (further Kaspersky Lab) has created this Statement in order to inform and disclose its data gathering and dissemination practices for Kaspersky Security Center 10 (further Software).

Kaspersky Lab has a strong commitment to providing superior service to all of our customers and

I agree to participate in Kaspersky Security Network

I do not agree to participate in Kaspersky Security Network

Next Cancel

در صورتیکه تمایل داشته باشید Notification های مربوط به کنسول برای شما ایمیل شود، می توانید آدرس ایمیل دریافت کننده، آدرس SMTP Server و پورت مربوط به SMTP Server را در این پنجره وارد کنید تا از این پس پیغام ها برای شما ارسال شود.

×

← Administration Server Quick Start Wizard

Configure the method of email notification sending

Recipients (email addresses):

SMTP servers:

SMTP server port:

Use ESMTP authorization

User name:


Password:

Confirm password:

بعد از ساخته شدن Task و Policy های مورد نیاز از قبیل Virus Scan و Update این قسمت به پایان میرسد.

×

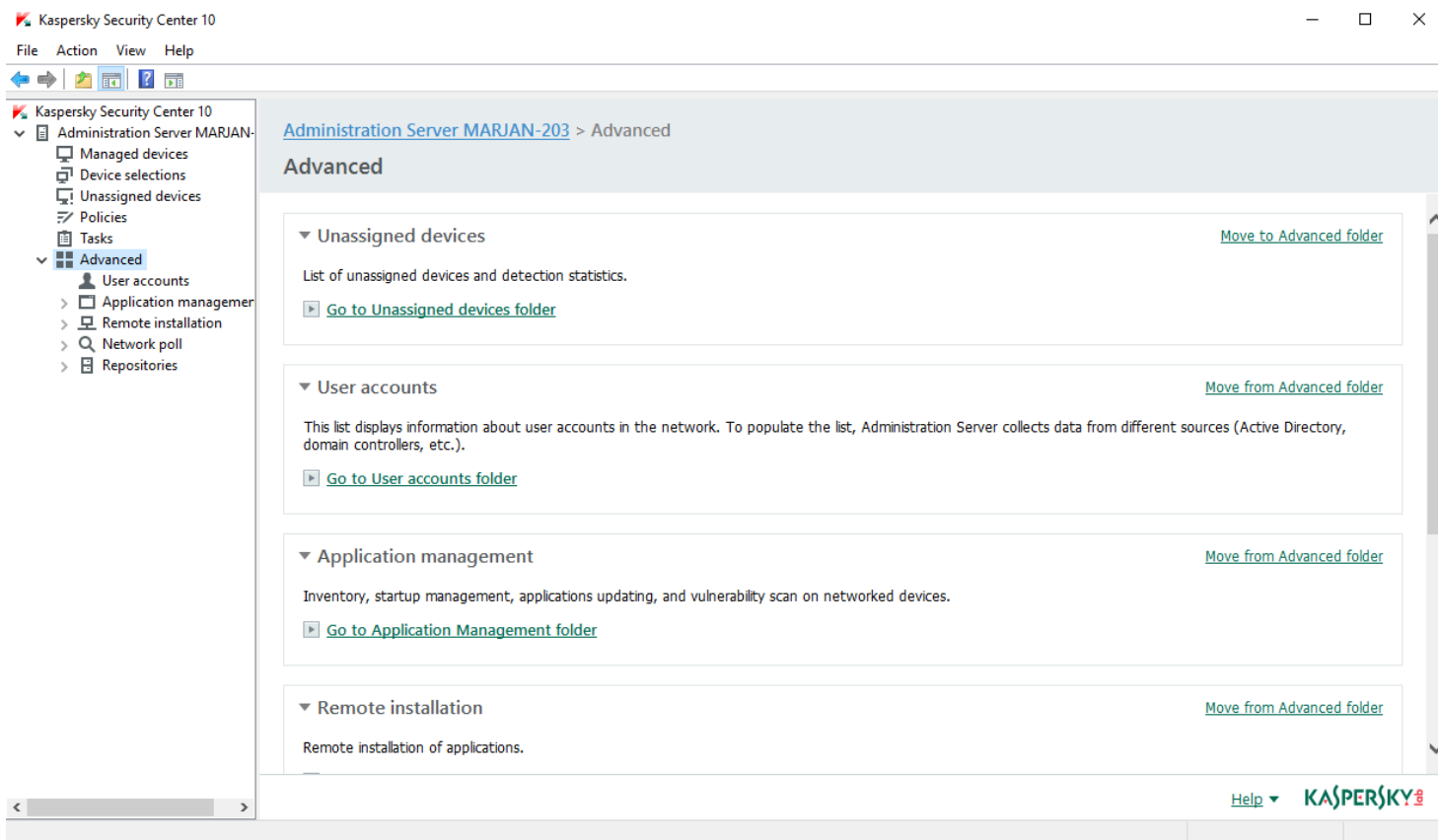
← Administration Server Quick Start Wizard

 You have successfully completed the Quick Start Wizard.

Run Protection Deployment Wizard

معرفی Tree کنسول:

همان طور که مشاهده می کنید tree کنسول شامل چندین بخش است که همه آنها زیر مجموعه Administration Server هستند.



Managed devices:

گروه اصلی و یا به اصطلاح Parent کنسول کسپرسکی می باشد، به صورت پیش فرض کلیه ی سیستم های شبکه پس از نصب Network Agent در این گروه قرار می گیرند و در صورت ایجاد گروه بندی های جدیدی همه گروه ها نیز در زیر مجموعه ی این گروه قرار می گیرند.

این قسمت خود شامل چهار تب است:

Devices:

در این قسمت کامپیوتر های موجود در گروه Managed devices نمایش داده می شوند. برای اضافه کردن کامپیوتر جدید می توانید Add Devices را انتخاب کنید یا از داخل قسمت Unassigned Devices سیستم های مورد نظر را با موس به گروه مورد نظر منتقل کنید.

Policies:

جهت تنظیم policy برای Server ها و client ها از این تب استفاده می کنیم.

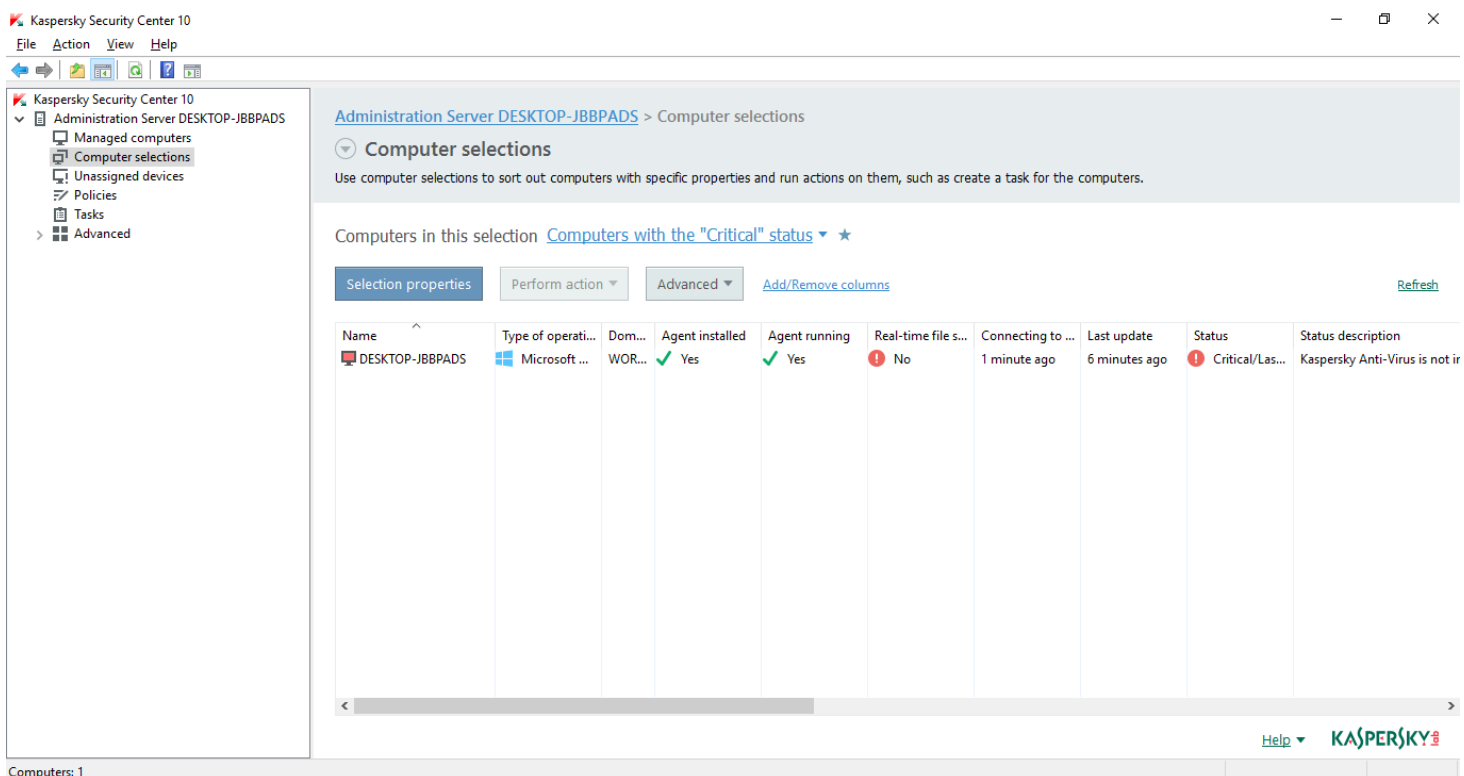
Tasks:

شامل Task های Update و Virus Scan و Find vulnerabilities است و جهت ایجاد Task برای Server ها و Client ها از این تب استفاده می کنیم. در این قسمت Task های مربوط به Security Center نیز قرار می گیرند که به صورت معمول شامل Task های Download updates the repository جهت دریافت فایل های به روز رسانی از سایت کسپرسکی و Back up Administration Server data جهت تهیه نسخه ی پشتیبان از تمامی تنظیمات Security Center می باشد. همچنین تسک های نصب ریموت که فقط مخصوص شبکه های دامین میباشد نیز در این بخش تنظیم میشوند.

در این قسمت باید در داخل تسک Download updates to the repository در بخش Settings و سپس در بخش Update Source سورس آپدیت سرور کسپرسکی شعب و سرپرستی را بر روی گزینه Master Server قرار دهید.

Computer Selection:

در این بخش میتوانید از کلاینت هایی که یک ارور خاص را دارند را کلی مشاهده نمایید.



Administration Server DESKTOP-JBBPADS > Computer selections

Computer selections

Use computer selections to sort out computers with specific properties and run actions on them, such as create a task for the computers.

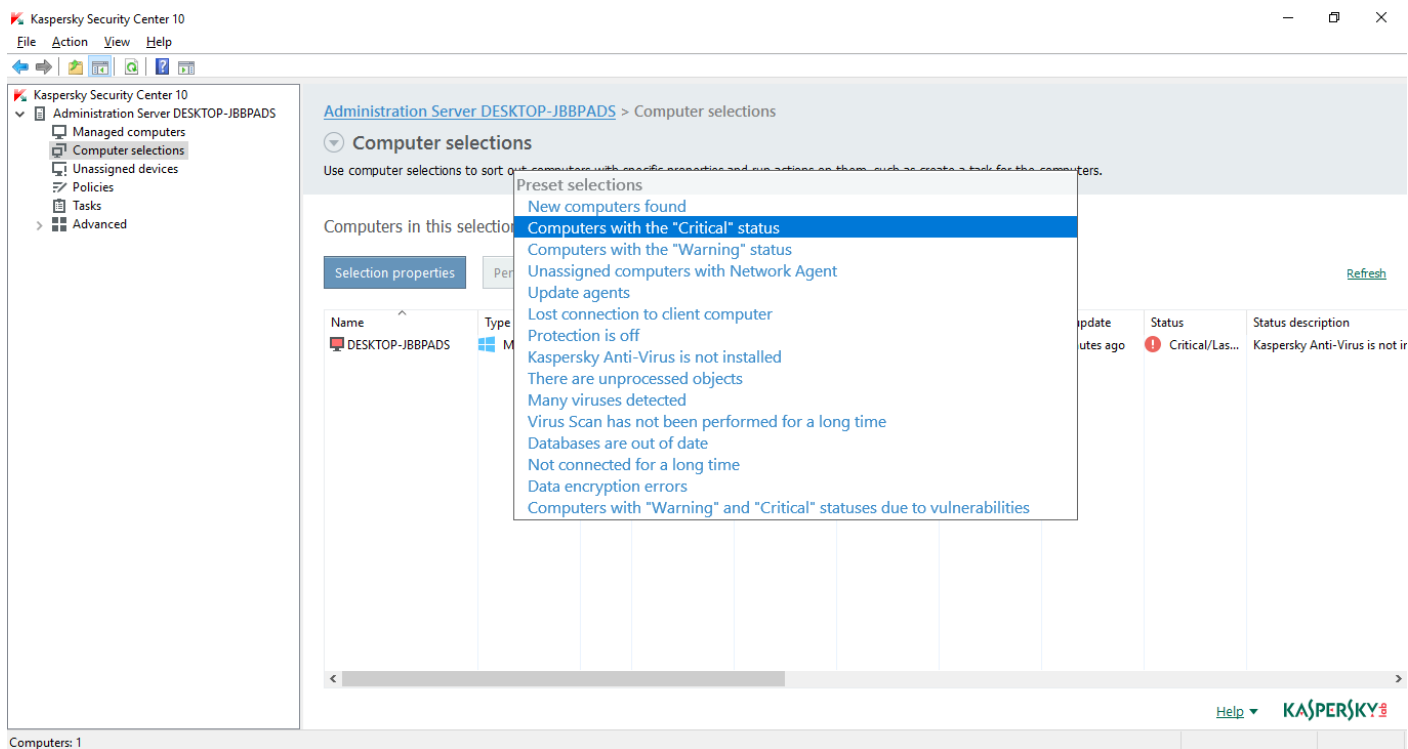
Computers in this selection [Computers with the "Critical" status](#) ★

Selection properties Perform action Advanced Add/Remove columns Refresh

Name	Type of operati...	Dom...	Agent installed	Agent running	Real-time file s...	Connecting to ...	Last update	Status	Status description
DESKTOP-JBBPADS	Microsoft ...	WOR...	Yes	Yes	No	1 minute ago	6 minutes ago	Critical/Las...	Kaspersky Anti-Virus is not ir

Computers: 1

به طور مثال می‌توانید سیستم‌هایی که آپدیت نشده‌اند را با کلیک بر روی گزینه Database are out of date در سراسر شبکه مشاهده نمایید. به تصویر زیر نگاه نمایید.



نحوه ایجاد گزارش در کنسول Kaspersky :

برای اینکار بر روی Administration Server کلیک نمایید و در تب Report گزینه Create a report را انتخاب نمایید و بعد از تعیین نام نوع گزارش را انتخاب نمایید.

Administration Server MARJAN-203 (IeDco\marjan.am)

Monitoring Statistics Reports Events [Server settings](#)

[Create a report template](#) [Configure report delivery](#) [Refresh](#)

[Add/Remove columns](#)

Name	Type	Description	Creat...
Database usage report	Database usage report	Kaspersky Lab anti-virus database usage re...	6/7/...
Errors report	Errors report	Report on main errors in Kaspersky Lab ap...	6/7/...
Hardware report	Hardware report	Report contains information about equipm...	6/7/...
Incompatible applicat...	Incompatible applicatio...	Report on incompatible security applicatio...	6/7/...
Kaspersky Lab softwa...	Kaspersky Lab software ...	Report on Kaspersky Lab software versions	6/7/...
Key usage report	Key usage report	Report on status of keys on devices	6/7/...
Protection deployme...	Protection deployment ...	Report on network deployment of Kaspers...	6/7/...
Protection status report	Protection status report	This report contains information about the...	6/7/...
Report about errors in...	Report about errors in e...	Report about errors in encryption of files a...	6/7/...
Report on blockage o...	Report on blockage of a...	Report on blockage of access to encrypted ...	6/7/...
Report on blocked runs	Report on blocked runs	This report contains information about blo...	6/7/...
Report on device users	Report on device users	This report displays the accounts of users ...	6/7/...
Report on effective us...	Report on effective user...	Rights of the user specified in the report pr...	6/7/...
Report on encryption ...	Report on encryption st...	This report displays the encryption statuses...	6/7/...
Report on file operati...	Report on file operation...	File operations on removable drives	6/7/...
Report on hardware r...	Report on hardware regi...	This report contains information about the...	6/7/...
Report on installed ap...	Report on installed appl...	Report on all installed applications	6/7/...
Report on key usage ...	Report on key usage by ...	Report on statistics of the use of keys by vir...	6/7/...
Report on most heavil...	Report on most heavily ...	Top 10 most heavily infected devices	6/7/...

Database usage report

Properties

Type: Database usage report
 Description: Kaspersky Lab anti-virus database usage report
 Created: 6/7/2017 3:28:54 PM

Actions

[Show report](#)
[Save](#)
[Deliver reports](#)
[Properties](#)
[Delete](#)

Help

Reports: 27

← New report template wizard

Defining report template name

Name:

[Next](#) [Cancel](#)

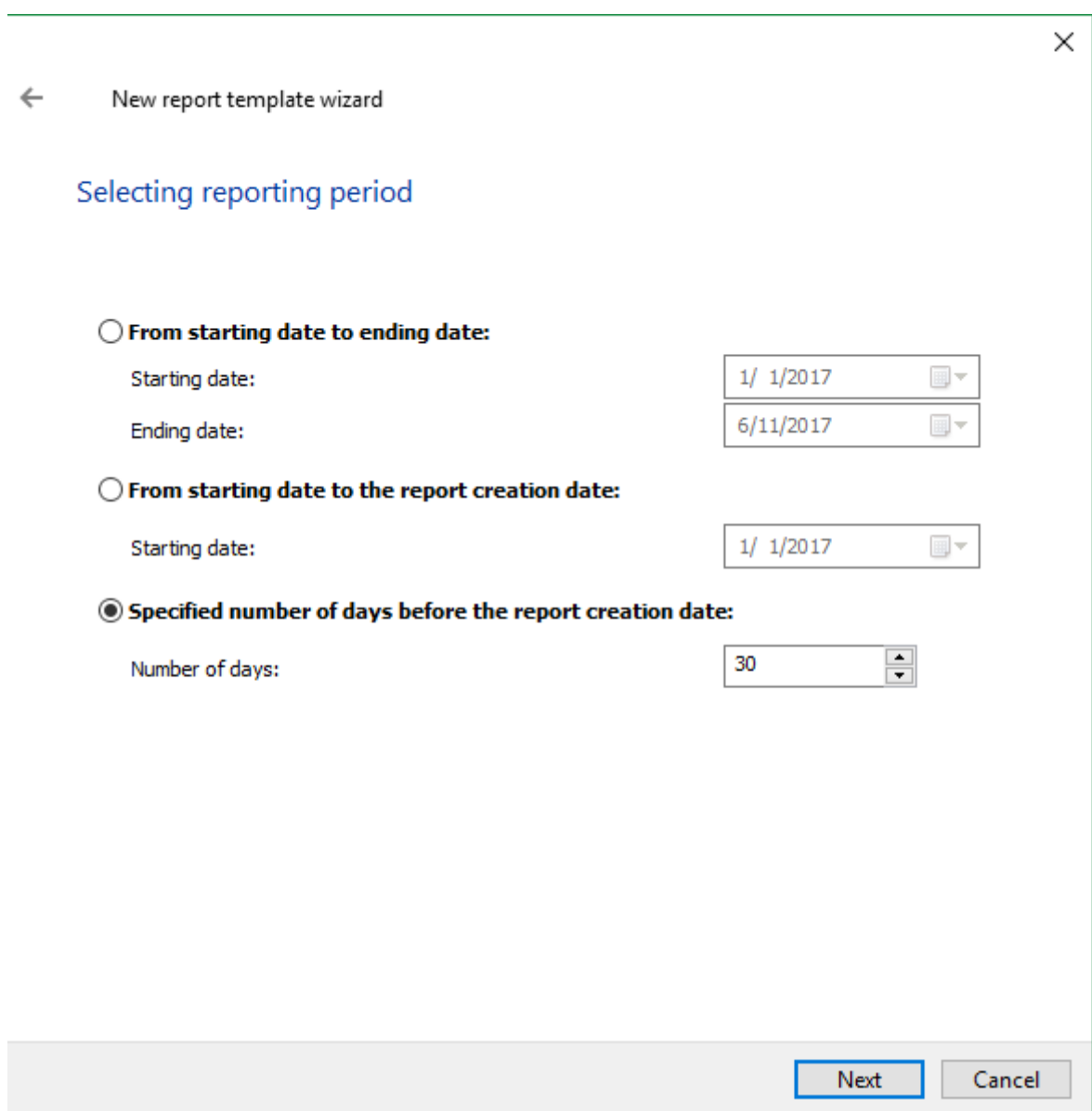
← New report template wizard ×

Selecting the report template type

- Protection status**
 - Protection status report
 - Errors report
 - Event report
 - Report on activity of update agents
- Deployment**
 - Key usage report
 - Kaspersky Lab software version report
 - Incompatible applications report
 - Protection deployment report
 - Report on key usage by virtual Server
- Update**
 - Database usage report
 - Report on versions of Kaspersky Lab software module updates
- Statistics of threats**
 - Viruses report
 - Report on most heavily infected devices
 - Network attack report

Next Cancel

در این مرحله می توانید یک محدوده ی زمانی برای گرفتن گزارش تهیه نمایید، به عنوان مثال 30 روز گذشته.

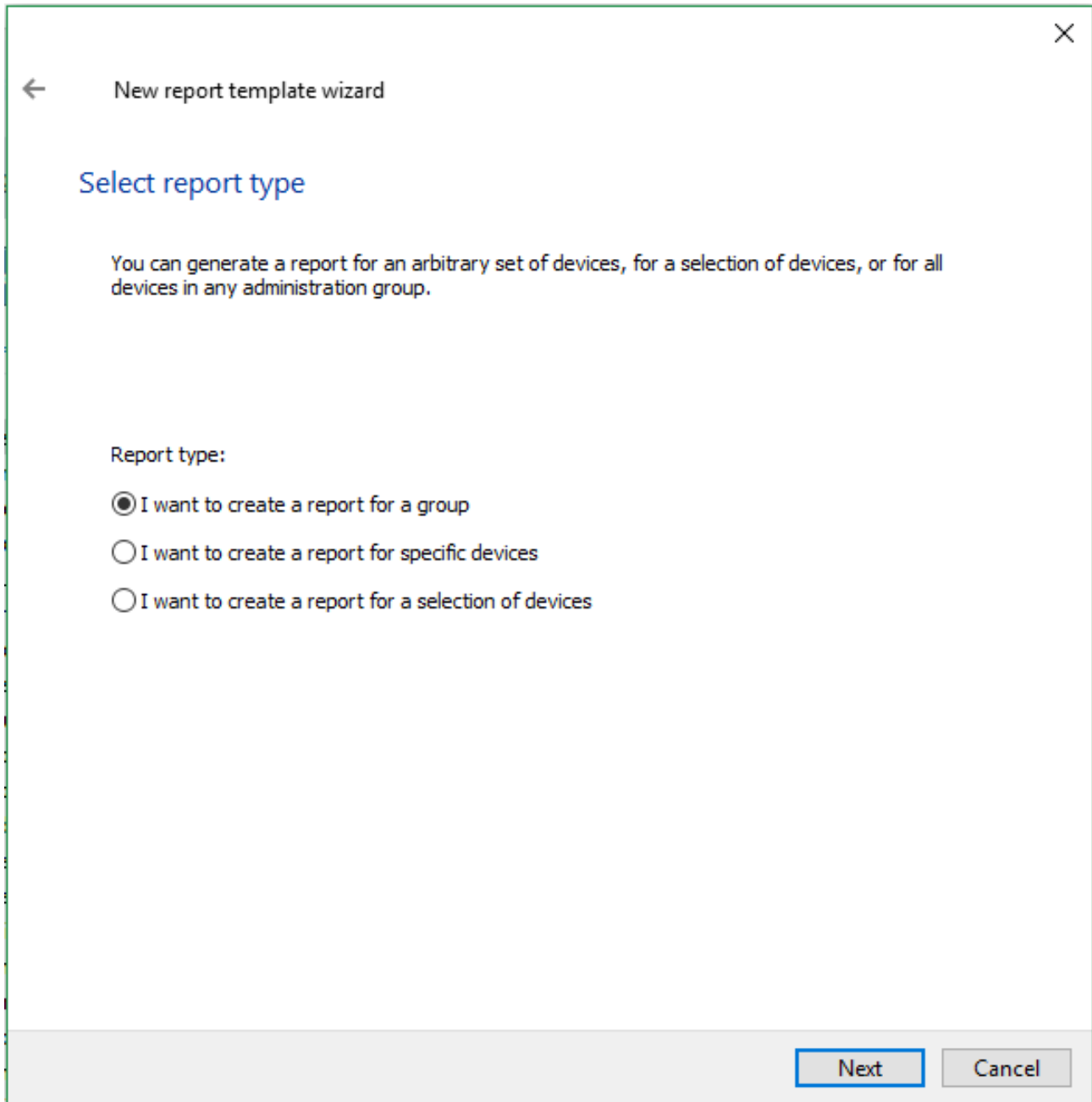


The screenshot shows a dialog box titled "New report template wizard" with a close button (X) in the top right corner. The main heading is "Selecting reporting period". There are three radio button options:

- From starting date to ending date:
 - Starting date: 1/ 1/2017
 - Ending date: 6/11/2017
- From starting date to the report creation date:
 - Starting date: 1/ 1/2017
- Specified number of days before the report creation date:
 - Number of days: 30

At the bottom right, there are two buttons: "Next" and "Cancel".

در این پنجره می توانید این گزارش را برای گروه خاصی از سیستم ها ایجاد کنید.



← New report template wizard

Select report type

You can generate a report for an arbitrary set of devices, for a selection of devices, or for all devices in any administration group.

Report type:

- I want to create a report for a group
- I want to create a report for specific devices
- I want to create a report for a selection of devices

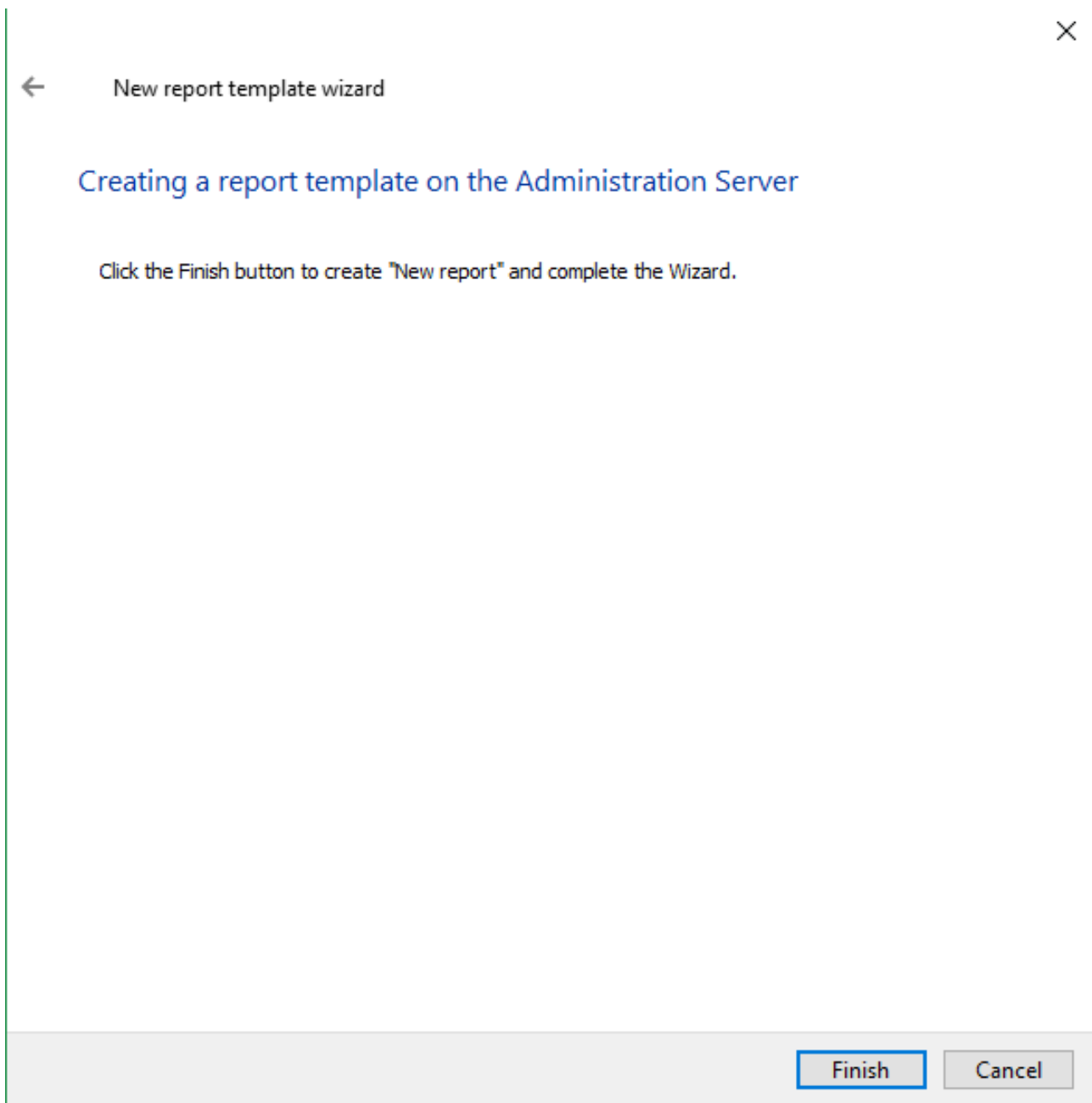
Next Cancel

×

← New report template wizard

Select group

Target group for report:






















همان طور که مشاهده می کنید گزارش ساخته شده در لیست Report ها اضافه شده است.

Monitoring
Statistics
Reports
Events

Create a report template

Configure report delivery

[Add/Remove columns](#)

Name	Type	Description
 Database usage report	Database usage report	Kaspersky
 Errors report	Errors report	Report or
 Hardware report	Hardware report	Report cc
 Incompatible applications report	Incompatible applicatio...	Report or
 Kaspersky Lab software version report	Kaspersky Lab software ...	Report or
 Key usage report	Key usage report	Report or
 New report	Network attack report	Report cc
 Network attack report	Network attack report	Report cc
 Protection deployment report	Protection deployment ...	Report or
 Protection status report	Protection status report	This repo
 Report about errors in encryption of files and folders	Report about errors in e...	Report ab
 Report on blockage of access to encrypted files	Report on blockage of a...	Report or
 Report on blocked runs	Report on blocked runs	This repo
 Report on device users	Report on device users	This repo
 Report on effective user permissions	Report on effective user...	Rights of
 Report on encryption status of data storage drives	Report on encryption st...	This repo
 Report on file operations on removable drives	Report on file operation...	File oper
 Report on hardware registry	Report on hardware regi...	This repo
 Report on installed applications	Report on installed appl...	Report or

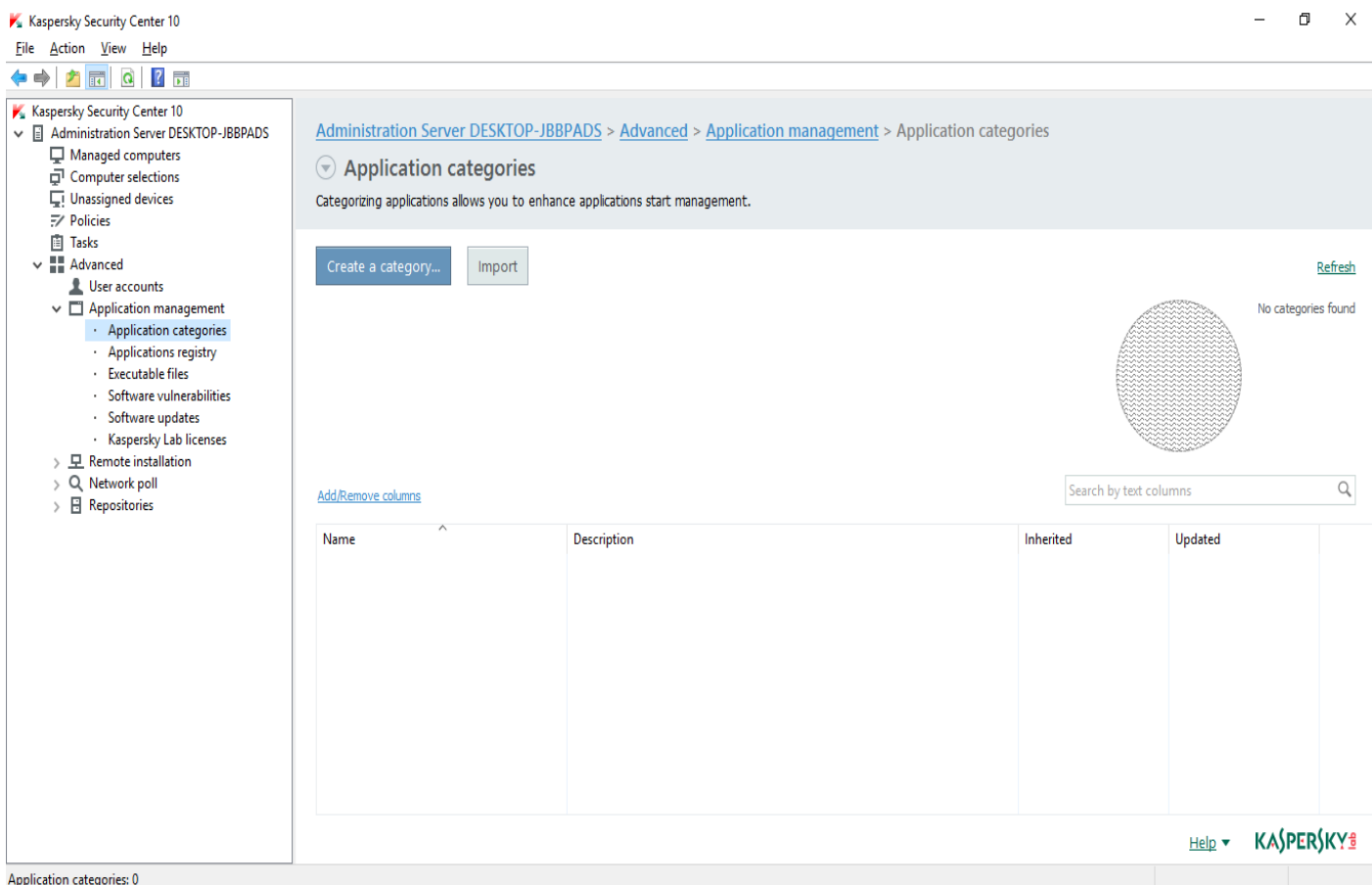
Advanced:

این بخش شامل چندین قسمت است. مانند، ساختن category، مشاهده برنامه های نصب شده، فایل های اجرایی داخل شبکه و لایسنس ها و آپدیت سیستم عامل ها است.

Application categories:

در این بخش شما می توانید دسته بندی های مختلفی بر روی application های نصب شده روی سیستم های داخل شبکه انجام دهید، این قابلیت ها شامل دسترسی یا عدم دسترسی تعدادی از application به کاربران می باشد. در قسمت Policy در بخش Start of application control می توانید از این Category ها استفاده کنید. به صورت پیش فرض در این قسمت هیچ Category از قبل تعریف نشده است. جهت تعریف یک Category مطابق مراحل زیر عمل کنید:

ابتدا بر روی گزینه Create a category کلیک کنید.



Kaspersky Security Center 10 Administration Server DESKTOP-JBBPADS > Advanced > Application management > Application categories

Application categories

Categorizing applications allows you to enhance applications start management.

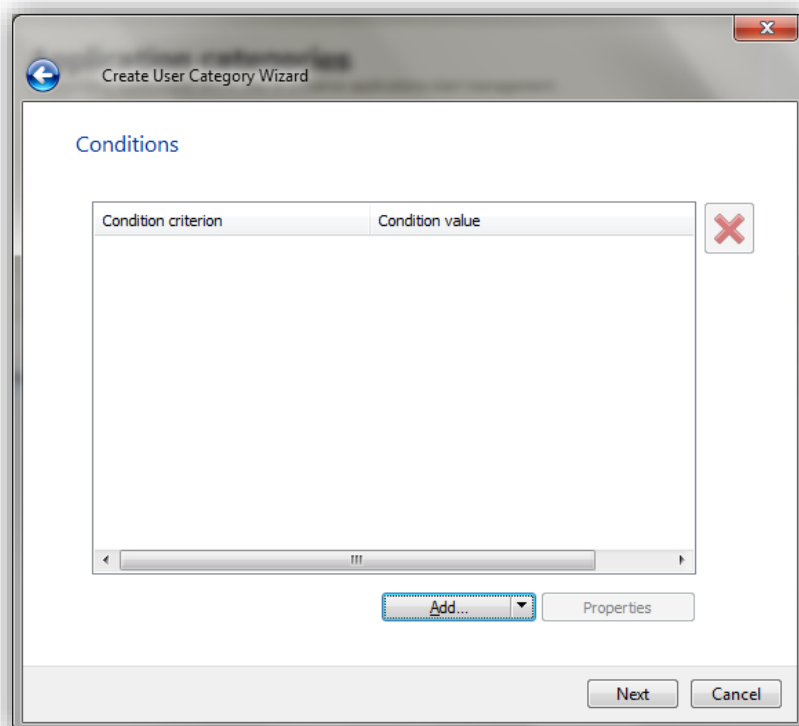
Create a category... Import Refresh

No categories found

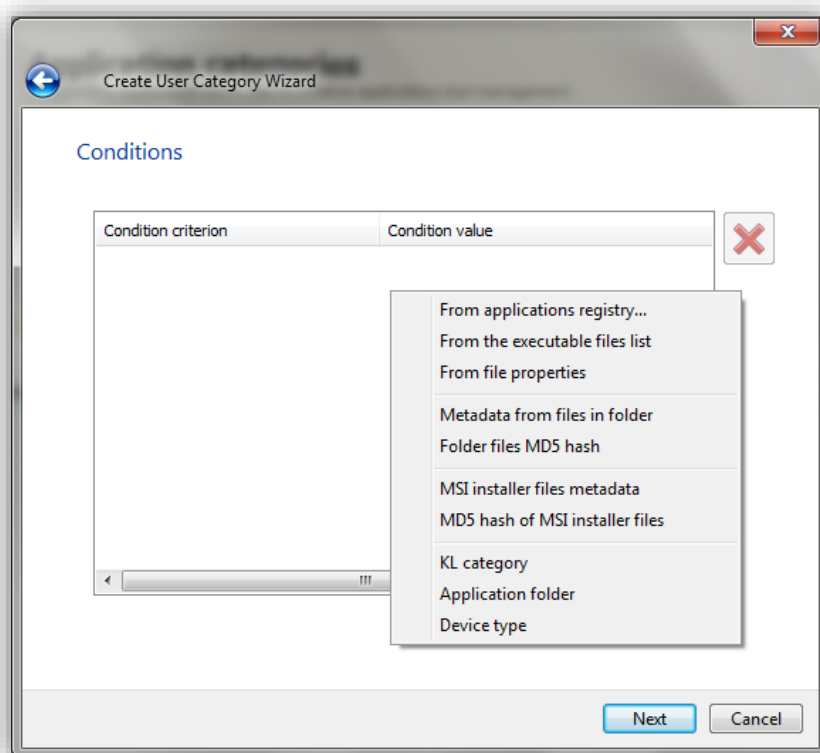
Add/Remove columns

Name	Description	Inherited	Updated

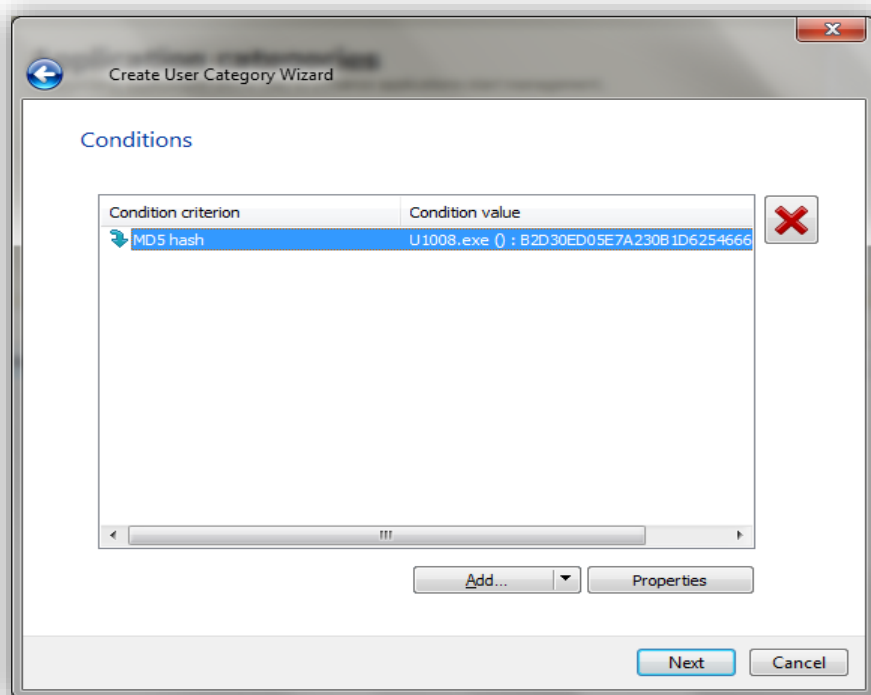
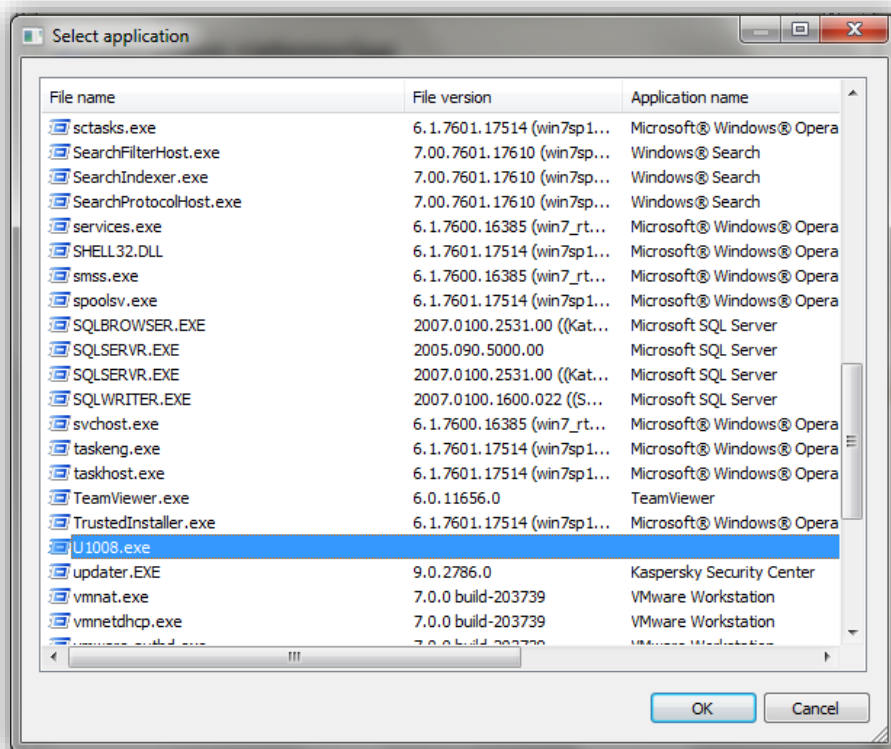
Application categories: 0



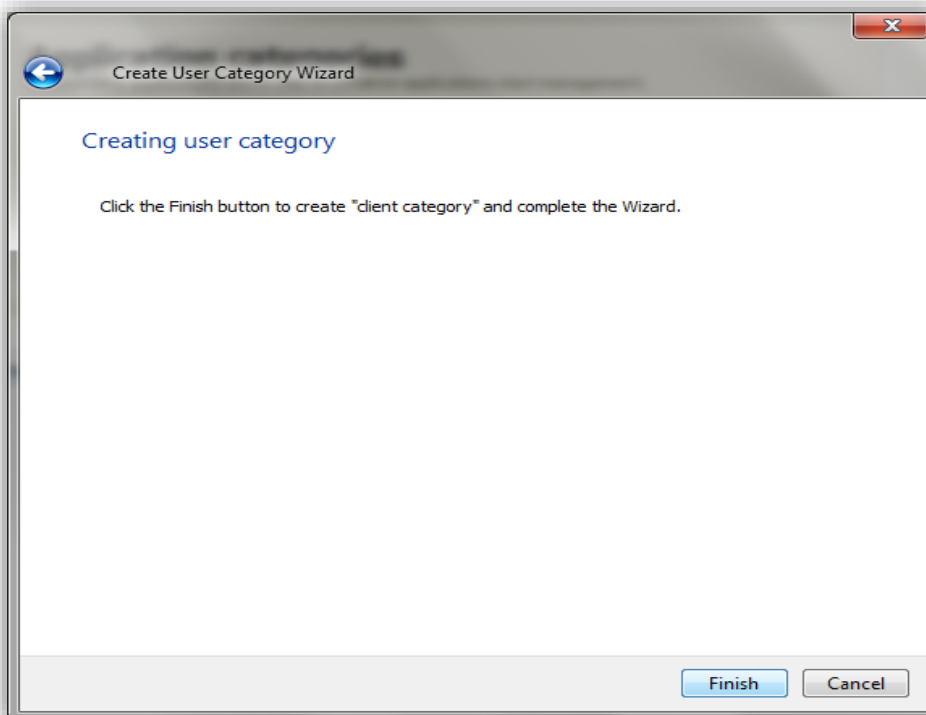
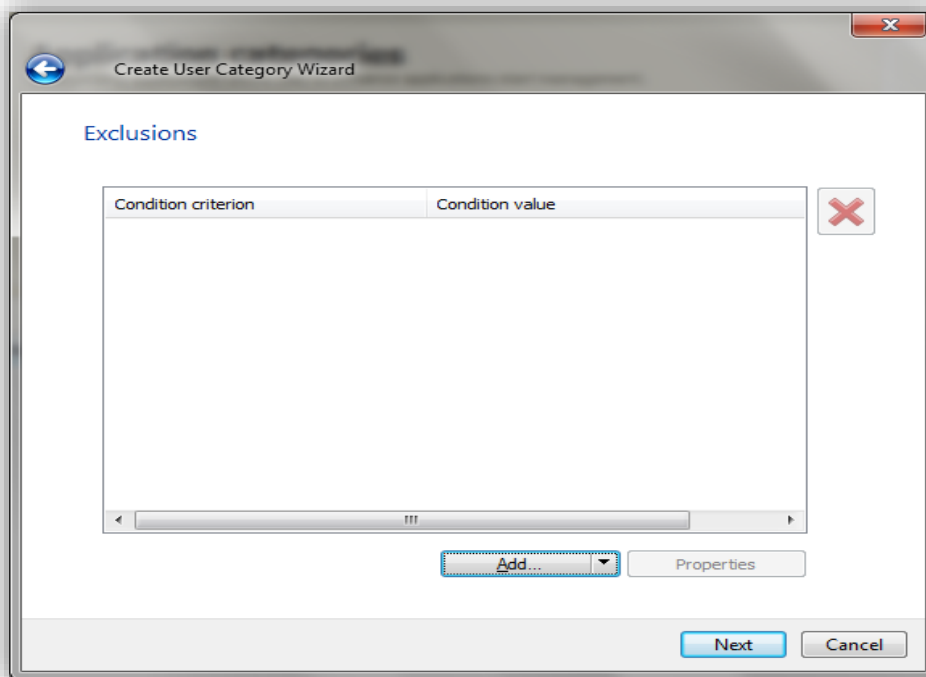
جهت اضافه کردن Application مورد نظر بر روی دکمه Add کلیک نمایید، لیست باز شونده کنار دکمه ی Add این امکان را به شما می دهد تا شیوه ی اضافه کردن application ها در category مورد نظر را انتخاب کنید. در این مثال بر روی لیست باز شونده کلیک می کنیم و روش انتخاب را بر اساس From the executable files list تنظیم می کنیم و در پنجره ای که باز می شود executable file مورد نظر خود را انتخاب می کنیم.



پس از انتخاب این گزینه لیستی از فایل های اجرایی موجود بر روی سیستم های داخل شبکه نمایش می یابد. برای مثال در این پنجره فایل اجرایی فیلتر شکن U1008.exe را انتخاب می کنیم.



با کلیک بر روی دکمه Add می توانید Application مورد نظر خود را از این لیست مستثنی کنید.



Application registry:

در این قسمت (به شرط وجود Network Agent بر روی سیستم های موجود در شبکه) می توانید کلیه ی Application های نصب شده بر روی سیستم های شبکه را مشاهده نمایید.

Administration Server DESKTOP-JBBPADS > Advanced > Application management > Applications registry

Applications registry

Categorizing applications allows you to enhance applications start management. [Properties](#)

[Show applications registry properties window](#) [Report on installed applications](#) [Refresh](#)

No filter specified, records total: 11

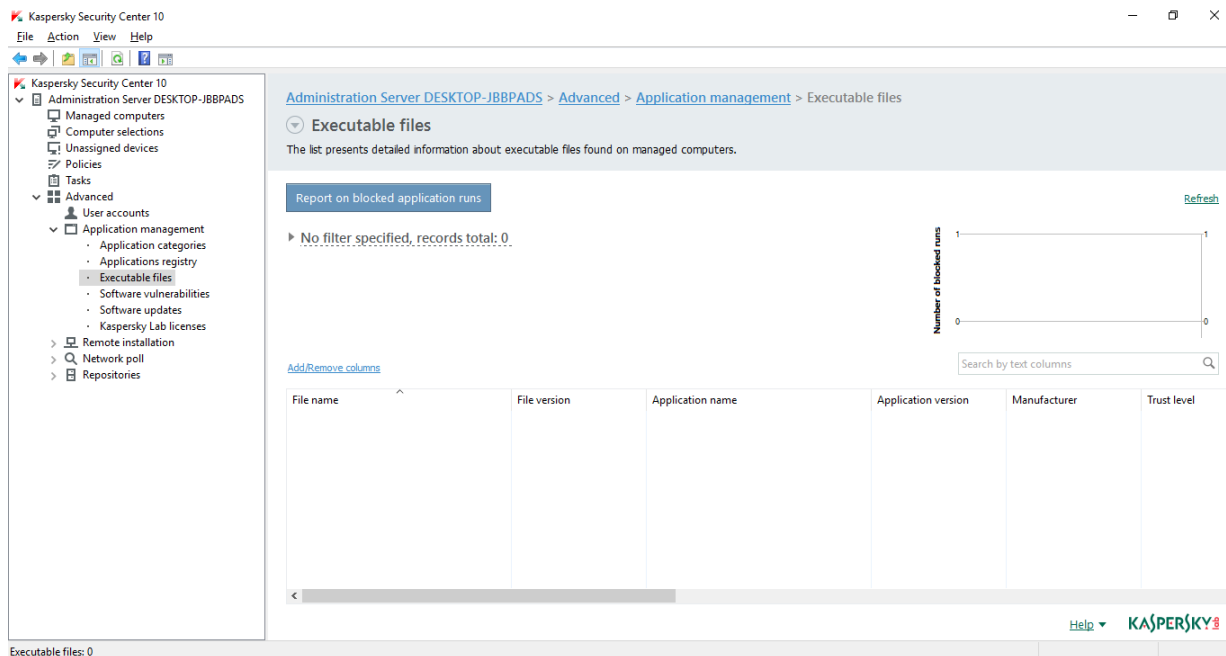
[Add/Remove columns](#)

Name	Version	Manufacturer	Num...	Comments	Technical
Plug-in for management of mobile iOS devices	10.3.407.0	AO Kaspersky Lab	1		
Plug-in for Exchange ActiveSync	10.3.407.0	AO Kaspersky Lab	1		
Oracle VM VirtualBox Guest Additions 5.1.22	5.1.22.0	Oracle Corporation	1		
Microsoft SQL Server VSS Writer	10.52.4000.0	Microsoft Corporation	1		http://go
Microsoft SQL Server Browser	10.52.4000.0	Microsoft Corporation	1		http://go
Microsoft SQL Server 2008 Setup Support Files	10.1.2731.0	Microsoft Corporation	1		http://go
Microsoft SQL Server 2008 R2 Setup (English)	10.52.4000.0	Microsoft Corporation	1		http://go
Microsoft SQL Server 2008 R2 Native Client	10.52.4000.0	Microsoft Corporation	1		http://go
Microsoft SQL Server 2008 R2	17.3.6816.0313	Microsoft Corporation	1		http://go
Microsoft OneDrive	10.3.407	AO Kaspersky Lab	1		http://go
Kaspersky Security Center 10 Administration Server	10.3.407	AO Kaspersky Lab	1		http://su

Applications in database: 11

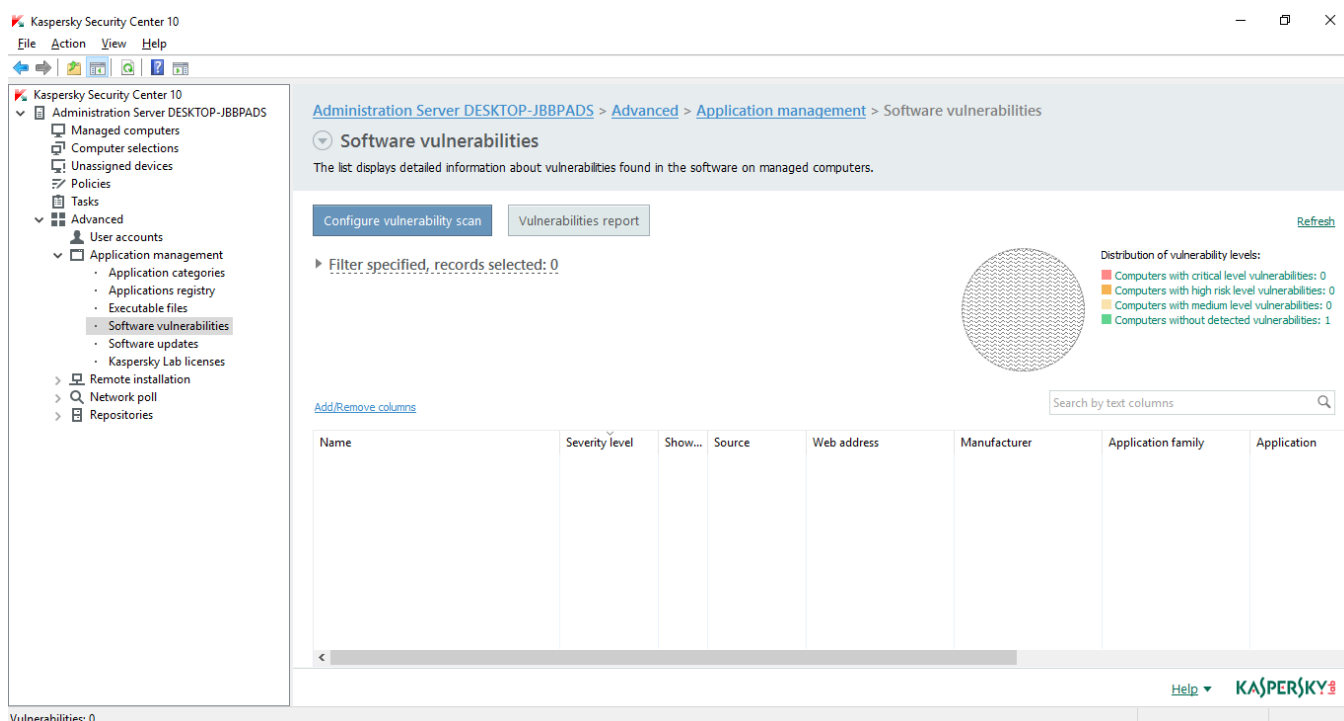
Executable Files:

در این قسمت از کنسول فایل های اجرایی که بر روی سیستم های داخل شبکه وجود دارد نمایش داده می شود.



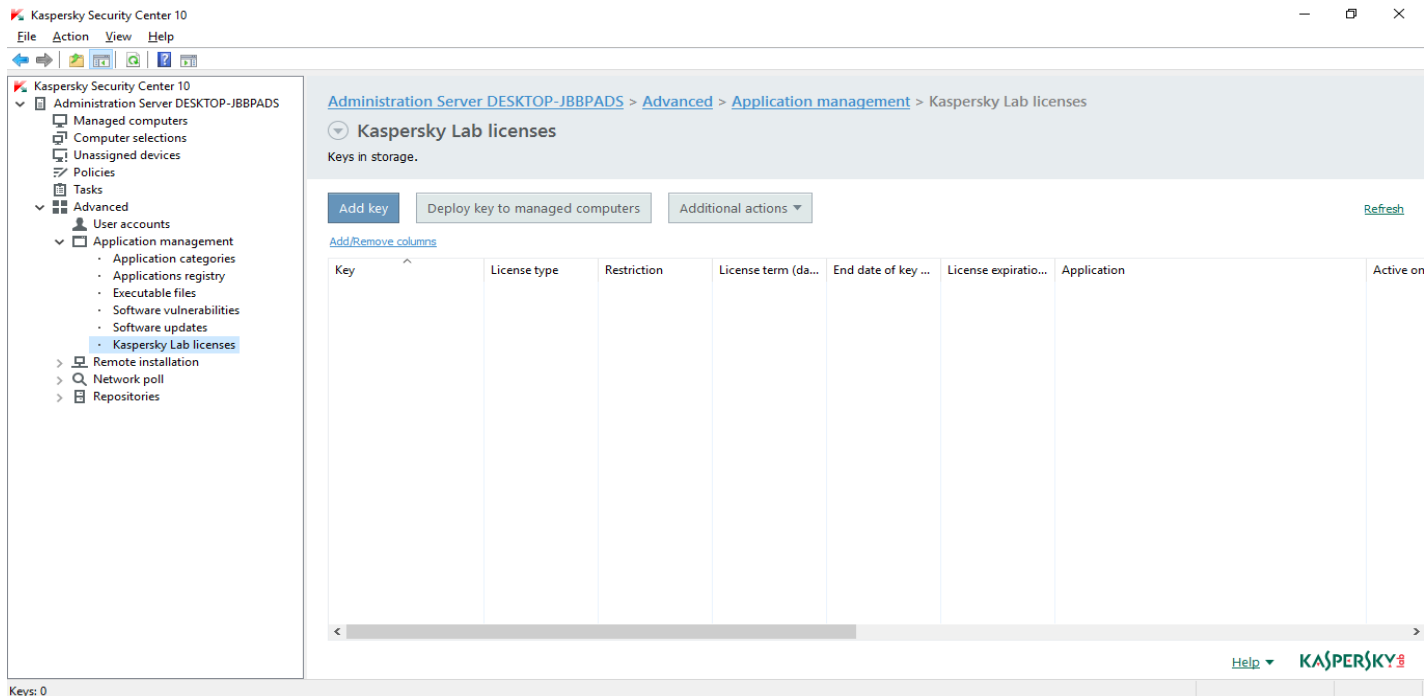
Software vulnerabilities:

این قسمت از کنسول آسیب پذیری های شناسایی شده در نرم افزارهای نصب شده بر روی سیستم های داخل شبکه را نمایش می دهد.

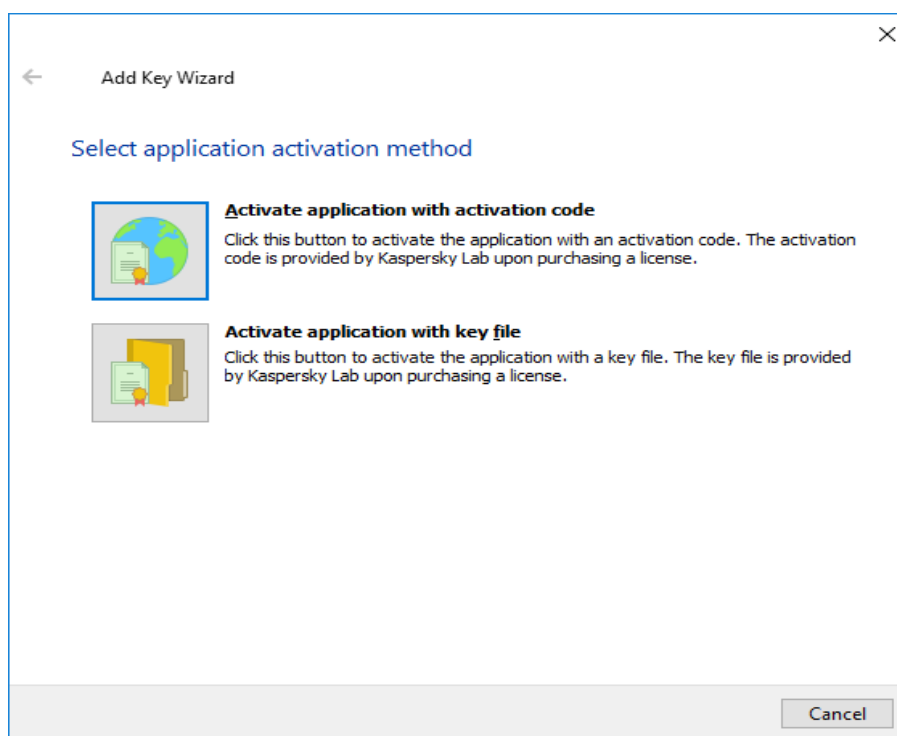


Kaspersky Lab licenses:

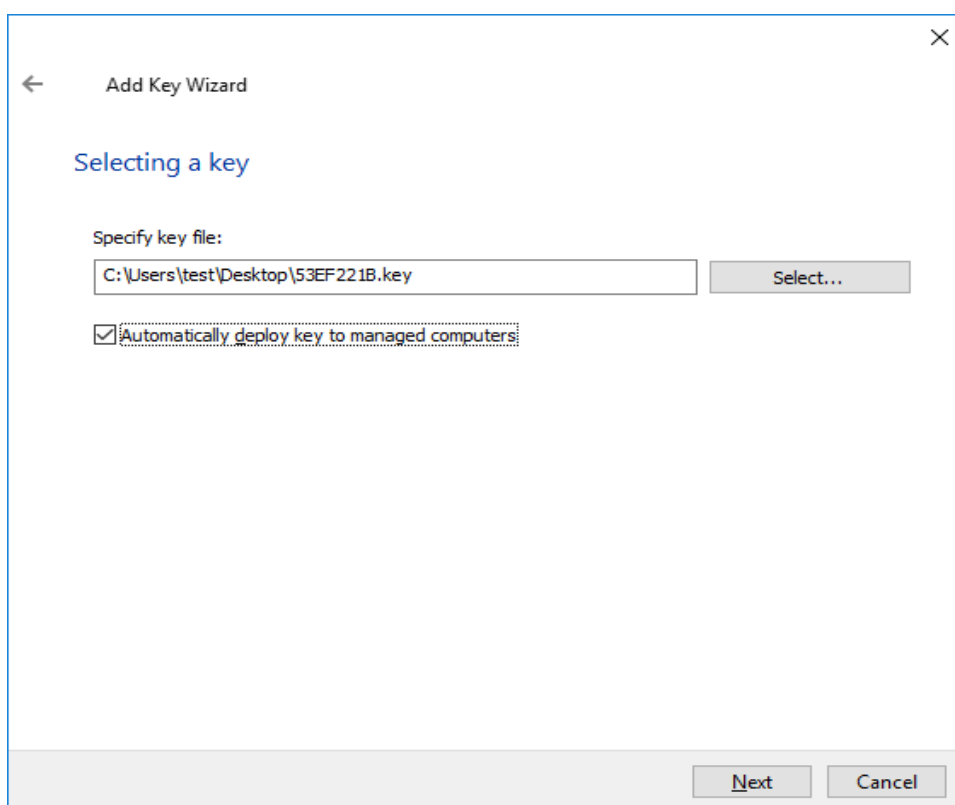
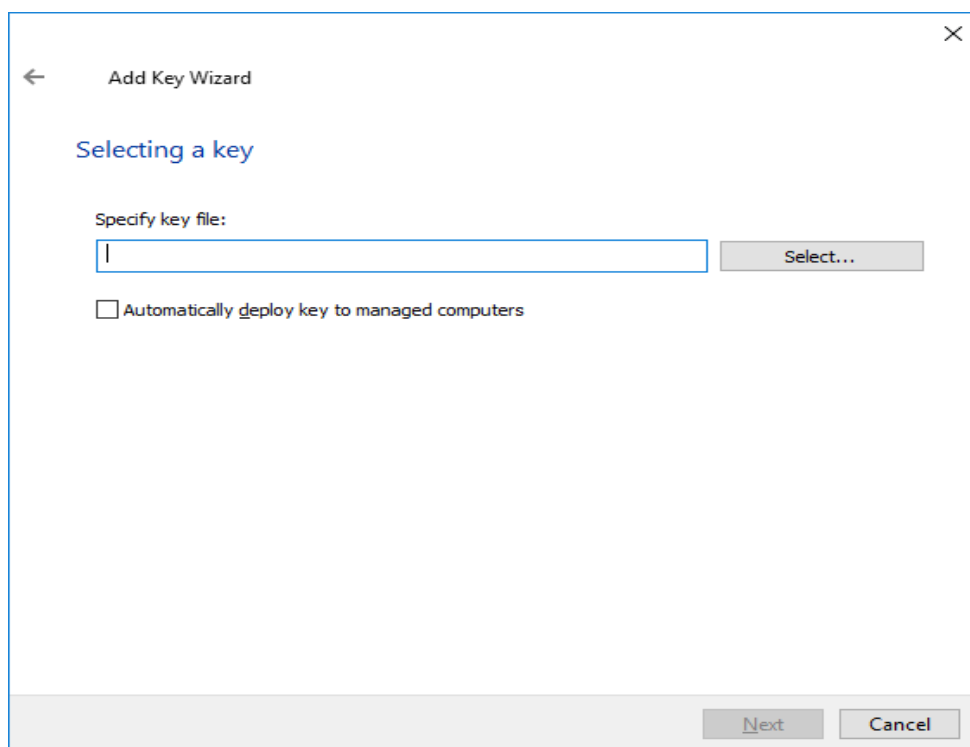
در این قسمت میتوانید لایسنس های کسپرسکی خود را اضافه نمایید تا بعد از نصب آنتی ویروس ها بر روی سیستم های دیگر، لایسنس به صورت اتوماتیک بر روی آن ها قرار گیرد.



برای اضافه کردن لایسنس ها ابتدا بر روی گزینه **Add key** کلیک نمایید پس از باز شدن صفحه زیر، بر روی گزینه **Activate application with key file** کلیک نمایید.



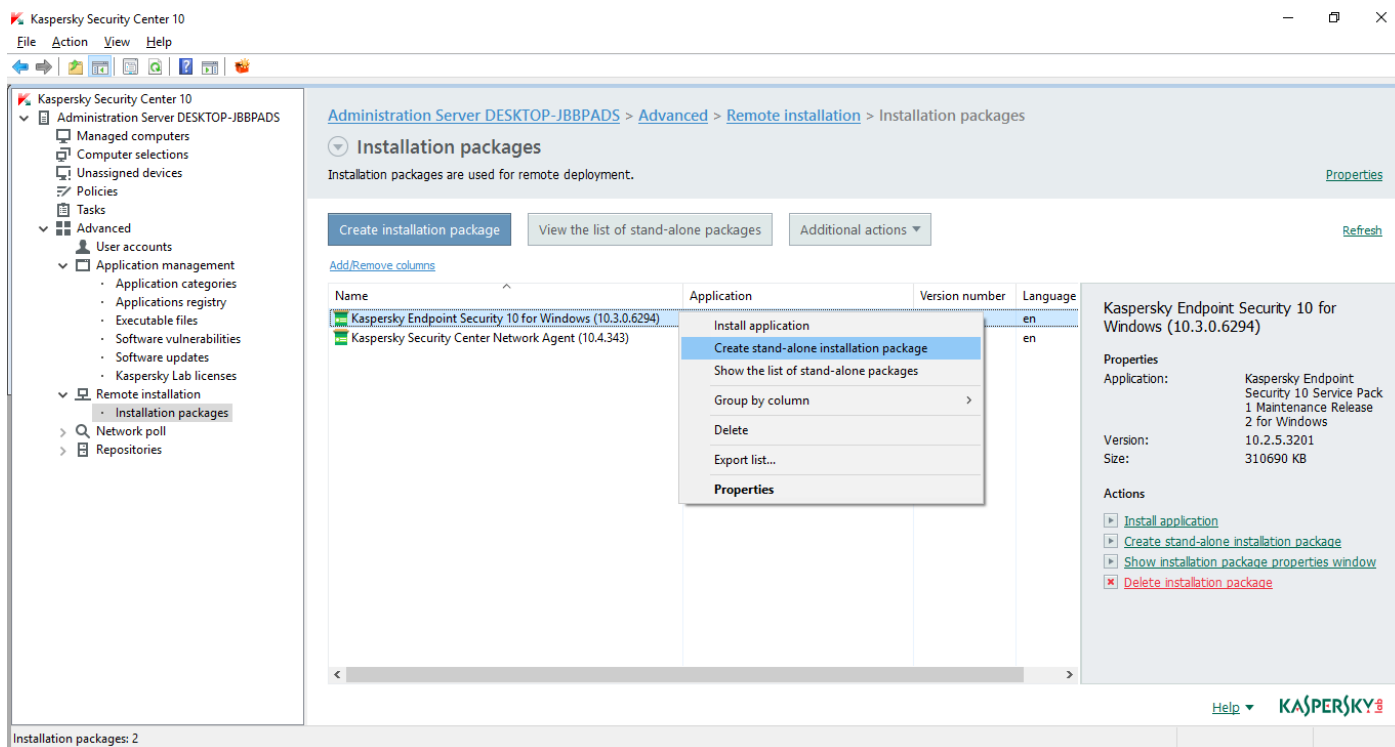
سپس در مرحله بعد فایل لایسنس خود را Browse کنید و تیک گزینه Automatically deploy key را نیز بزنید. این کار را برای هر دو فایل لایسنس انجام دهید.



Remote installation:

- **Installation packages:** برای نصب هر گونه نرم افزاری (چه نرم افزار های کسپرسکی و چه نرم افزار های غیر از آن) ابتدا باید Package مربوط به آن نرم افزار در این قسمت ساخته شود، البته Package های مربوط به نصب نرم افزار های کسپرسکی با نصب کنسول Security center به صورت پیش فرض ساخته می شود و نیازی به ساختن دوباره آن ها نمی باشد.

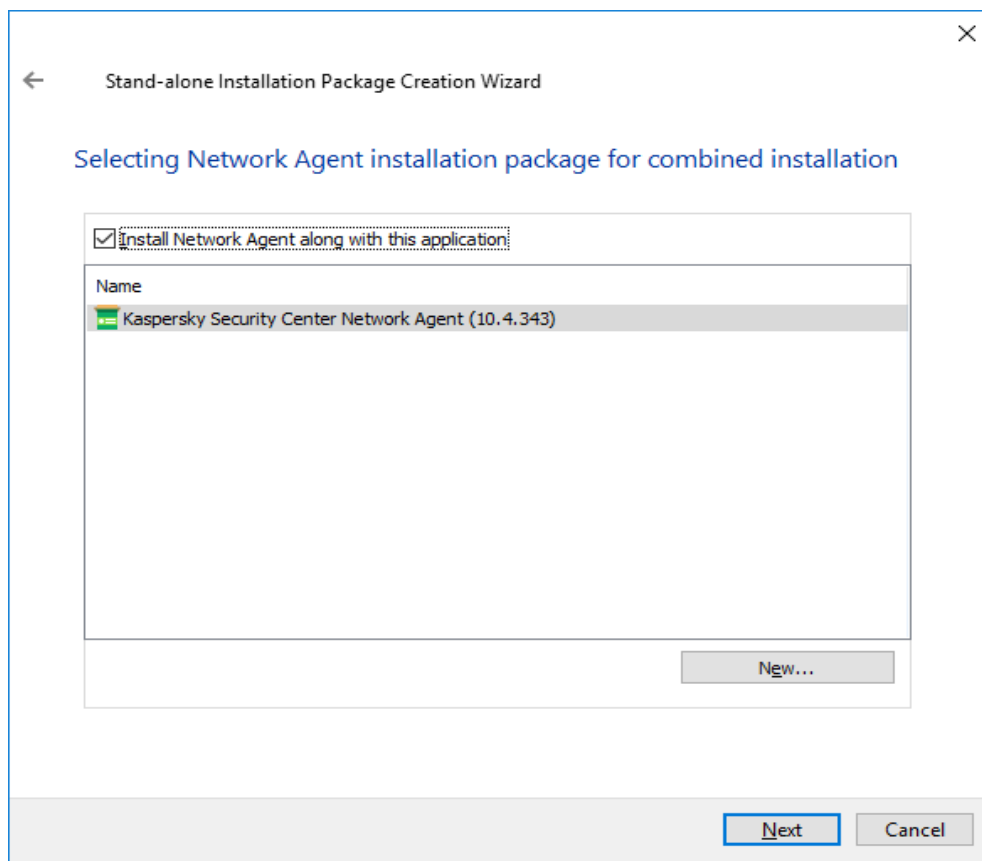
برای نصب بروی کلاینت ها ابتدا باید از پکیج آنتی ویروس موجود در این قسمت یک پکیج نصب به نام Stand-alone بسازید. ابتدا مطابق تصویر زیر بر روی پکیج Kaspersky Endpoint Security راست کلیک کنید و بر روی گزینه Create stand-alone installation package کلیک نمایید.



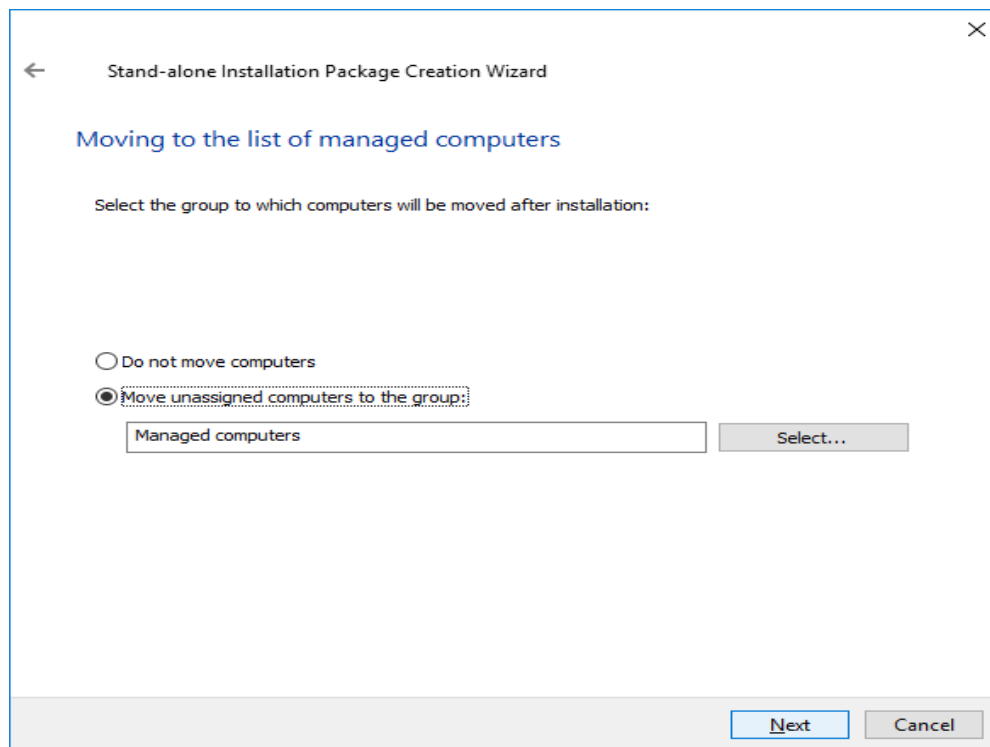
The screenshot shows the Kaspersky Security Center 10 Administration Console. The main window displays the 'Installation packages' section under 'Advanced > Remote installation'. A table lists installed packages, and a context menu is open over the 'Kaspersky Endpoint Security 10 for Windows (10.3.0.6294)' package, with the option 'Create stand-alone installation package' highlighted. The properties panel on the right shows details for the selected package, including its name, application, version number, language, and actions like 'Install application', 'Create stand-alone installation package', 'Show installation package properties window', and 'Delete installation package'.

Name	Application	Version number	Language
Kaspersky Endpoint Security 10 for Windows (10.3.0.6294)	Install application		en
Kaspersky Security Center Network Agent (10.4.343)	Show the list of stand-alone packages		en

سپس در صفحه جدید پکیج Network Agent را انتخاب نمایید و به مرحله بعد بروید.

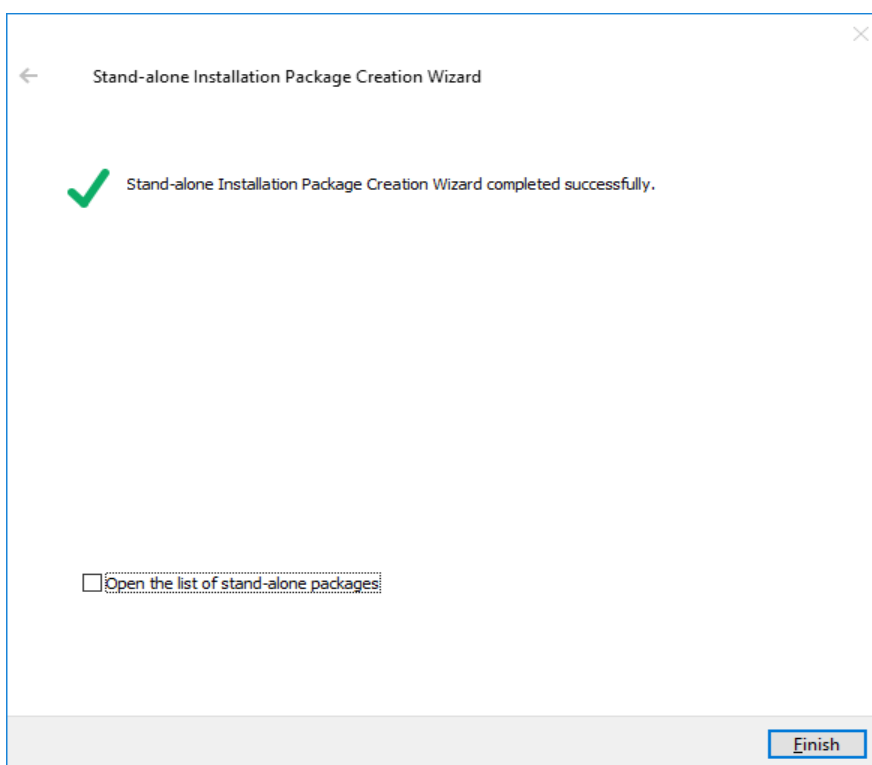
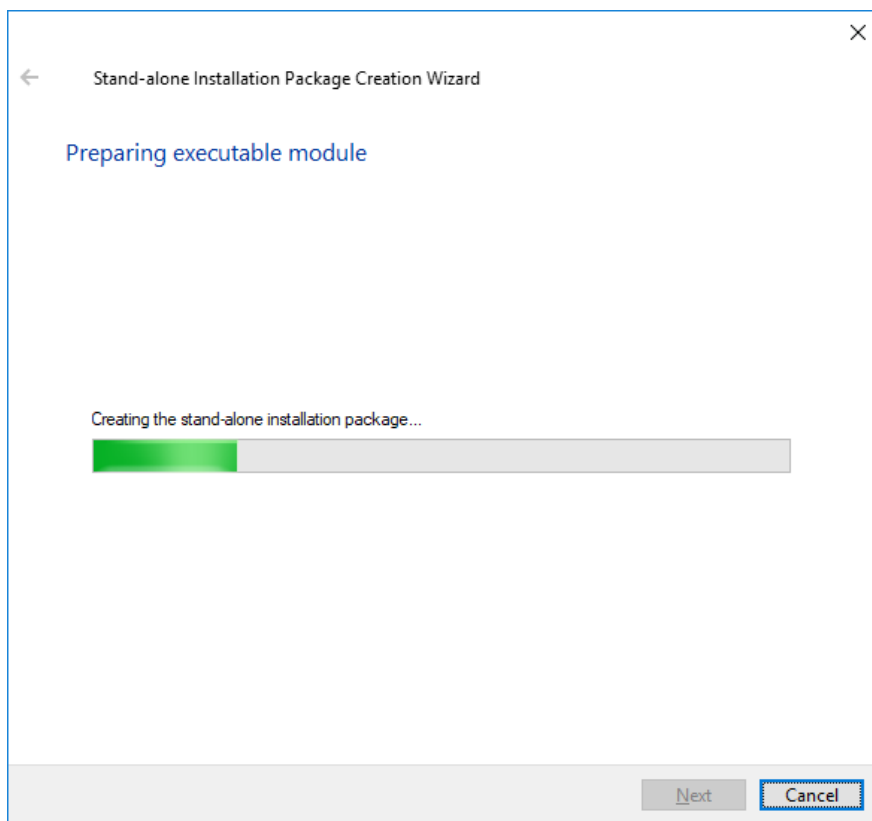


در مرحله بعدی تغییری ندهید و به مرحله بعد بروید.



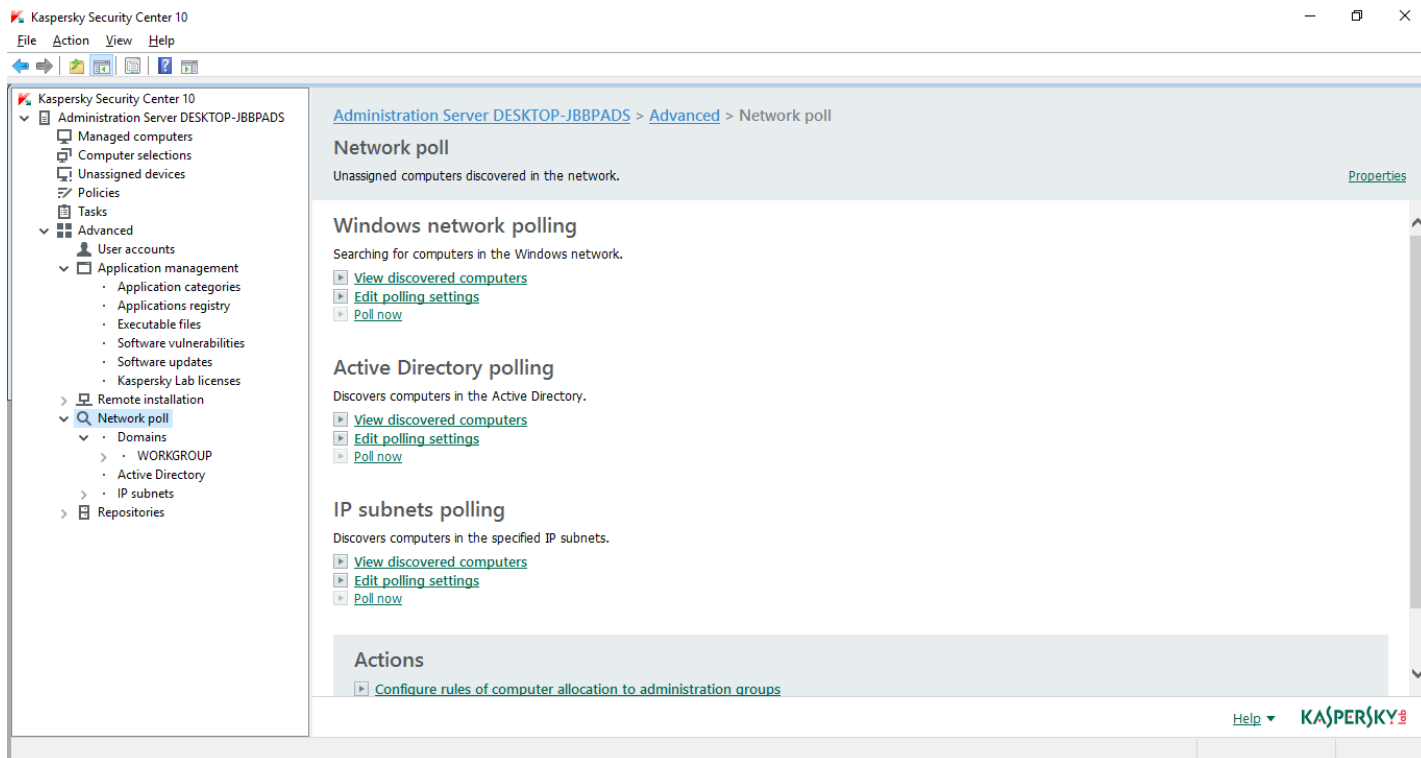
سپس اجازه دهید تا پکیج فوق ساخته شود. پس از ساخت این پکیج در share سرور کسپرسکی در مسیر زیر قرار میگیرد.

\\Kaspersky server IP\KLshare\pkginst\



Network Poll:

در این قسمت شما میتوانید مطابق تصویر زیر در سه بخش مختلف Domain و Active Directory و IP Subnet سیستم های داخل شبکه را شناسایی کنید و آن ها را به داخل Managed devices انتقال دهید.



این قسمت خود شامل چندین زیر شاخه است :

- **Kaspersky Lab updates and patches**: شامل نمایشی از پایگاه داده و مازول های آپدیت و آخرین تاریخ به روز رسانی این اجزا (تاریخ Create شدن و receive شدن فایل های به روز رسانی) می باشد
- **Quarantine**: در صورتیکه آنتی ویروس برنامه ای را مشکوک به ویروس ببیند آن را قرنطینه می کند و اطلاعات آن فایل قرنطینه شده را به Security Center ارسال می کند.
- **Backup**: زمانی که آنتی ویروس ها بر روی سیستم ها فایلی را ویروسی شناسایی کنند در ابتدا سعی می کنند آلودگی را از روی فایل برطرف کنند (Disinfect)، در صورتی که موفق به رفع آلودگی نشوند، فایل مذکور به صورت کامل پاک خواهد شد. در هر صورت، قبل از اینکه آنتی ویروس عملیاتی بر روی فایل های آلوده انجام دهد یک نسخه ی پشتیبان از آن فایل تهیه می شود تا در صورت لزوم بتوان آن فایل را Restore نمود. اطلاعات نسخه های پشتیبان تهیه شده از فایل ها در این محل ذخیره می شود.
- **Unprocessed files**: در این بخش فایل های ویروسی شناسایی شده توسط آنتی ویروس سیستم ها که هنوز پردازشی روی آنها صورت نگرفته نمایش داده می شود.

Policy های مربوط به سرور و کلاینت

Policy ها به طور عموم در جهت تنظیمات کاربردی و حفاظتی بروی سیستم های شما استفاده می شود

در شاخه ی Managed computer یک Policy برای Server ها و Workstation ها جهت تنظیمات و تغییرات اجزای آنتی ویروس بر روی سیستم ها یا فعال و غیرفعال کردن قسمت هایی بر روی آنتی ویروس و همچنین اعمال محدودیت تغییر بر روی آنتی ویروس توسط کار بران وجود دارد.

تنها مکان برای تعریف Policy داخل گروه های موجود می باشد، به ازای هر گروه یک Policy در قسمت Policies مربوط به آن گروه تعریف می شود.

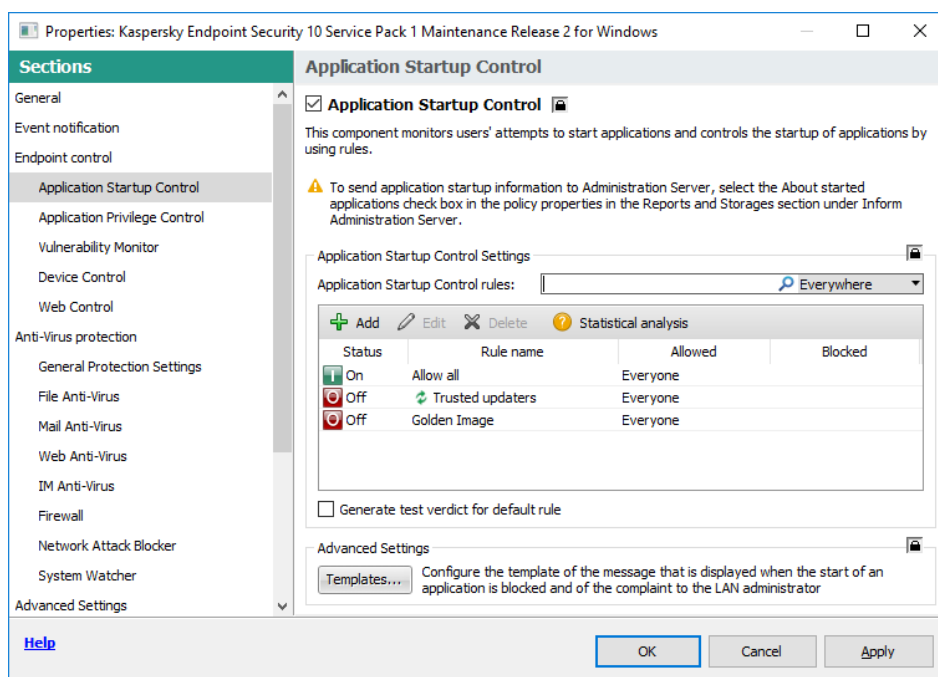
وارد Policies در قسمت Managed computer شوید.

جهت تغییر تنظیمات Policy بر روی سیستم ها، وارد تب Policies در Managed computer شوید، سپس بر روی Protection policy راست کلیک نمایید و گزینه ی Properties را انتخاب کنید. در این قسمت تمامی تنظیمات مربوط به آنتی ویروس قرار دارد که بر اساس نیاز می توانید آنها را تغییر دهید.

همان طور که در این قسمت مشاهده می کنید لیست تمام Component های محافظت مربوط به نوع نرم افزار برای شما نمایش داده خواهد شد شما می توانید با فعال یا غیر فعال کردن هر Component، آن Component را بر روی آنتی ویروس سیستم ها فعال یا غیر فعال کنید، همچنین در کنار هر قسمت یک قفل موجود می باشد با یکبار کلیک کردن بر روی قفل حالت قفل تغییر خواهد کرد، این قفل دسترسی کاربران را مشخص می کند هر قسمتی که قفل باز داشته باشد توسط کاربر قابل تغییر می باشد. در ادامه چند نمونه از این Component ها را توضیح خواهیم داد.

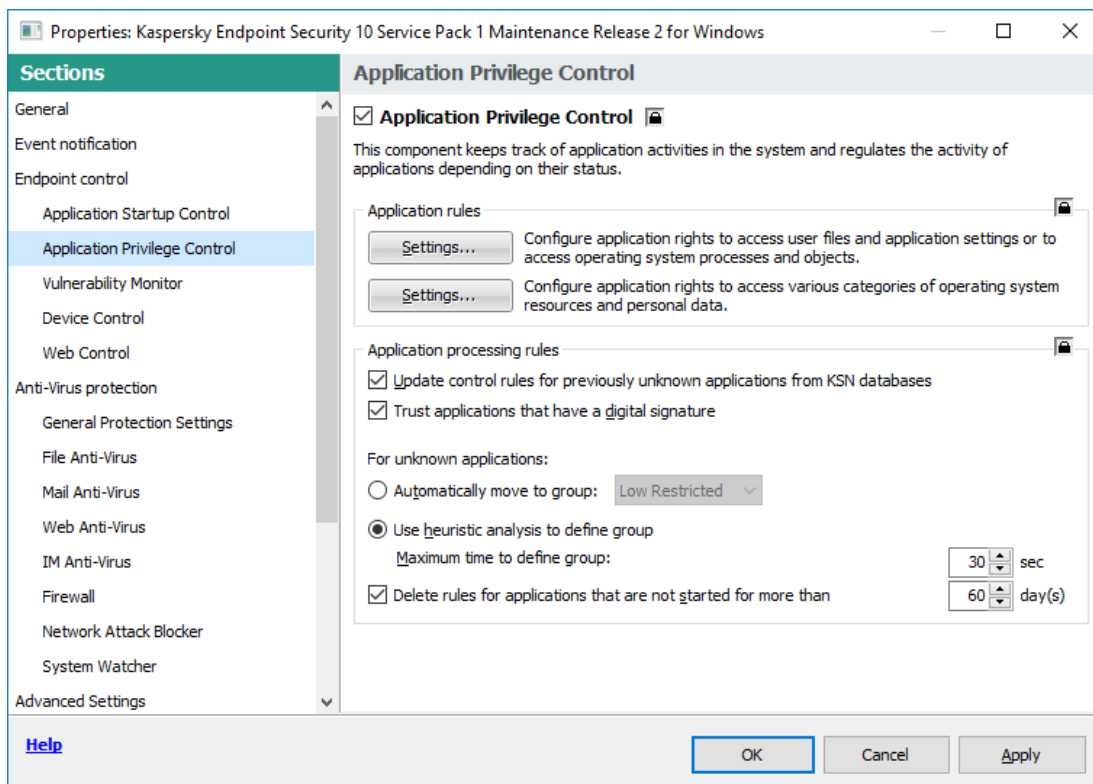
Application startup control

این Component راه اندازی Application های داخل شبکه را کنترل می کند. شما در این قسمت می توانید مشخص کنید چه Application هایی توسط چه اشخاصی اجازه ی اجرا شدن داشته باشند و یا چه اشخاصی نتوانند آن را اجرا کنند. برای اجرای این قابلیت شما در ابتدا باید در Applications and vulnerabilities یک Category ایجاد کنید که در قسمت های قبلی توضیح به طور کامل داده شده است. سپس برای استفاده از این قابلیت شما با زدن دکمه Add، Category ساخته شده را روی می کنید در این قسمت اجازه دسترسی و یا عدم دسترسی را برای کاربران تعیین نمایید.



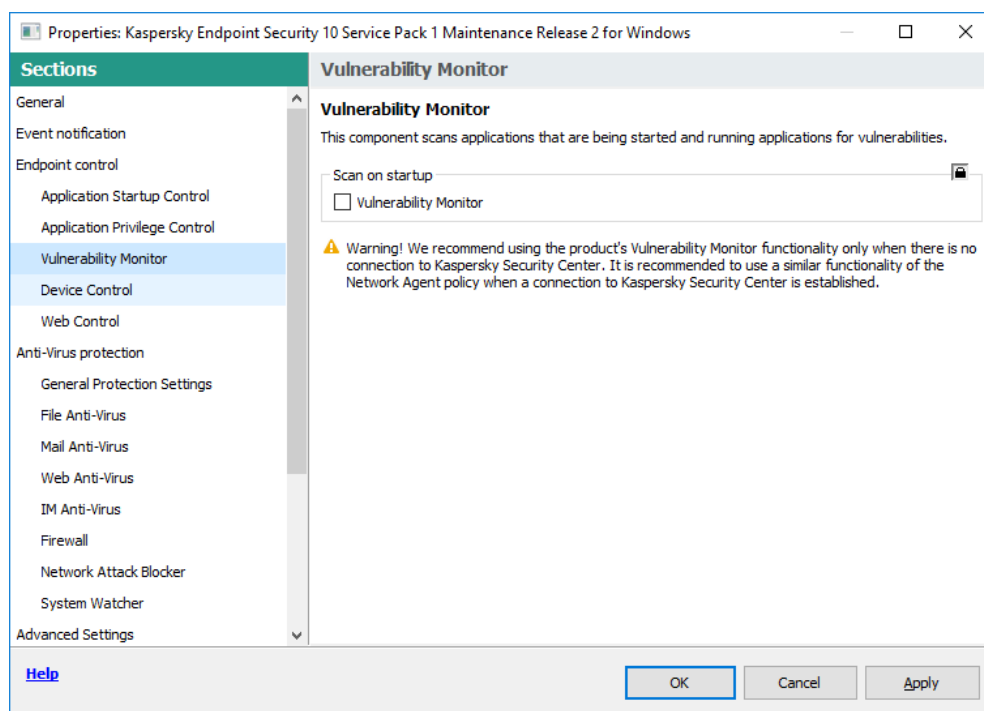
Application Privilege Control

این Component وضعیت و فعالیت Application ها را بر روی سیستم پیگیری می کند و پس از چک کردن وضعیت هر Application و اختصاص دادن آن به یکی از گروه های Trusted, Untrusted, High restricted, Low restricted اجازه فعالیت را بر اساس گروه بندی انجام شده به آن Application می دهد. برای این کار بروی Setting در قسمت Application control رفته Application control Rule و نرم افزار های مد نظر خود را در هر سطحی که لازم میدانید اضافه کنید.



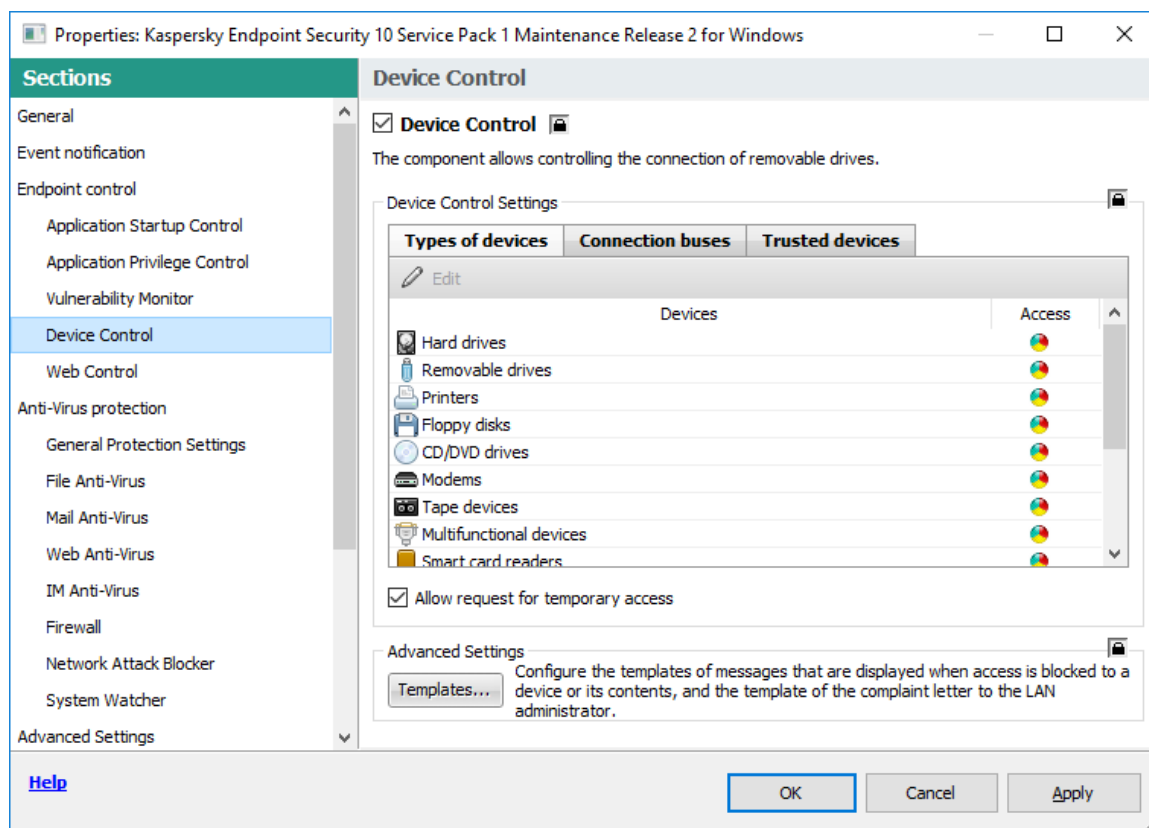
Vulnerability Monitor

فعال بودن این گزینه سبب می شود زمانی که Application ای شروع به کار می کند و یا در حال اجرا شدن است آنتی ویروس کسپرسکی آسیب پذیری این Application را بررسی کند، در صورتیکه این گزینه فعال نباشد بررسی آسیب پذیری به صورت اتومات انجام نمی گیرد و در صورت نیاز می بایست find Vulnerabilities را از داخل Managed computer اجرا کنید.



Device Control

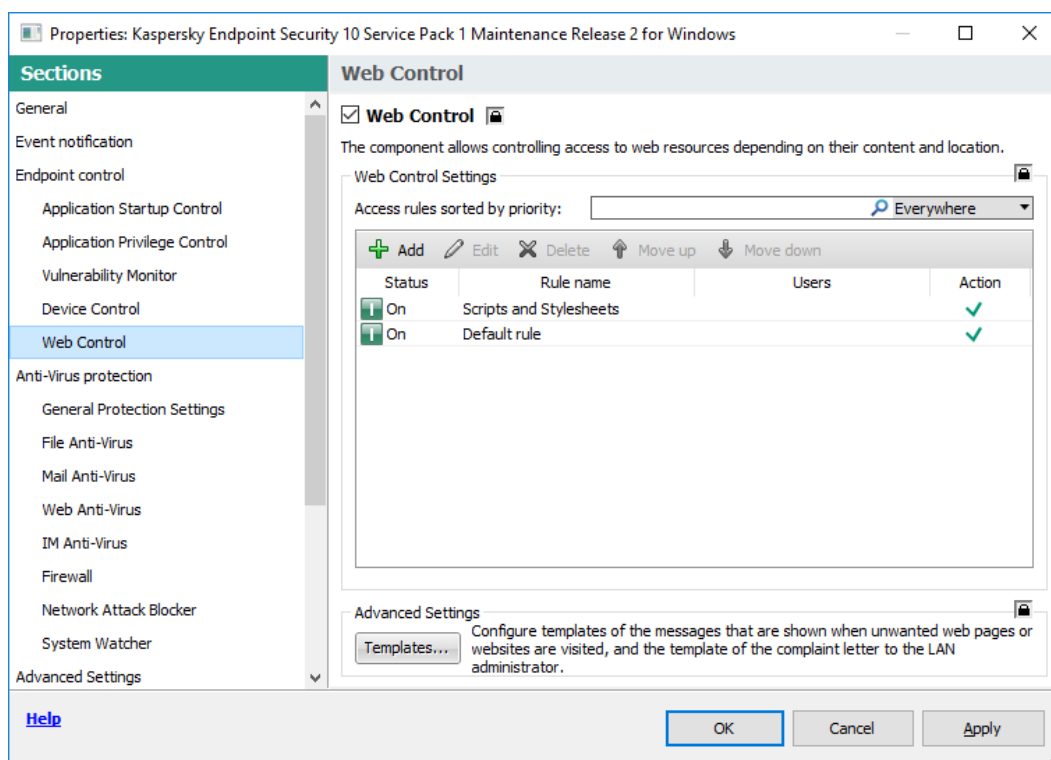
این Component به شما اجازه می دهد تا Removable Device ها را بر روی سیستم های داخل شبکه مدیریت کنید. به طور مثال شما می توانید از این طریق دسترسی به Flash Memory و یا CD\DVD-ROM را روی سیستم های کاربران ببندید.



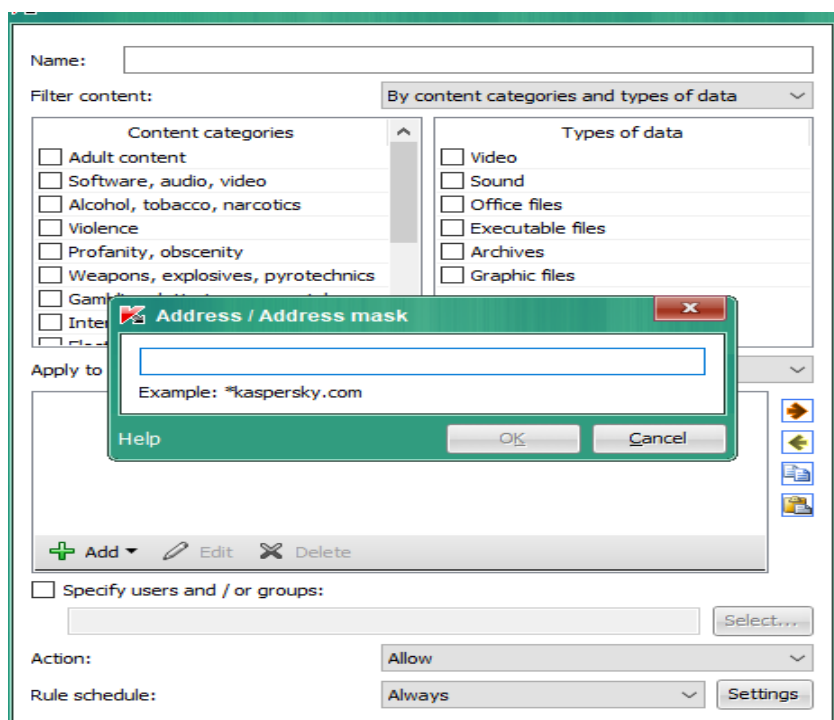
بر روی Removable drives کلیک کرده و به صورت پیش فرض در قسمت Access ، Depend On bus می باشد که می توانید Allow یا block را انتخاب نمایید و یا می توانید برای تعیین دسترسی برای تعدادی از کاربران دکمه Edit را بزنید و با اضافه کردن کاربران دسترسی Read ,Write مشخص کنید.

Web Control

این Component این امکان را به شما می دهد تا از طریق آن دسترسی کاربران به وب سایت های خاصی را براساس Content و یا بر اساس نوع داده (به طور مثال video, sound,....) و یا بر اساس URL ، مدیریت کنید.

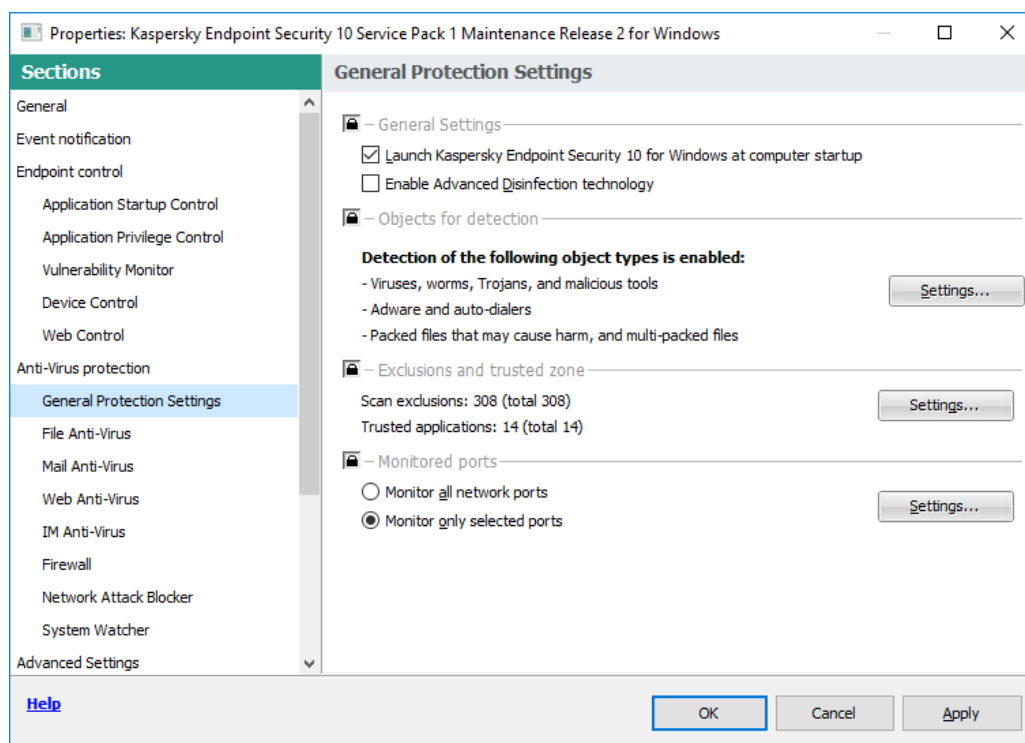


بروی گزینه Add کلیک کرده در قسمت filter Content، همانطور که مشاهده می کنید بر اساس محتوا می توانید سایت های مد نظرتان را فیلتر نمایید . در صورتی که بخواهید آدرس سایت خاصی را فیلتر نمایید در قسمت apply to address حالت To individual address را انتخاب و دکمه Add را می زنید و مانند نمونه سایت را وارد می نمایید. در صورتی که برای گروه یا کاربران خاص میخواهید این فیلترینگ را انجام دهید در قسمت Specify User and Group می توانید خاصیت Allow یا Block را تنظیم نمایید.



Anti-Virus protection

General Protection Setting

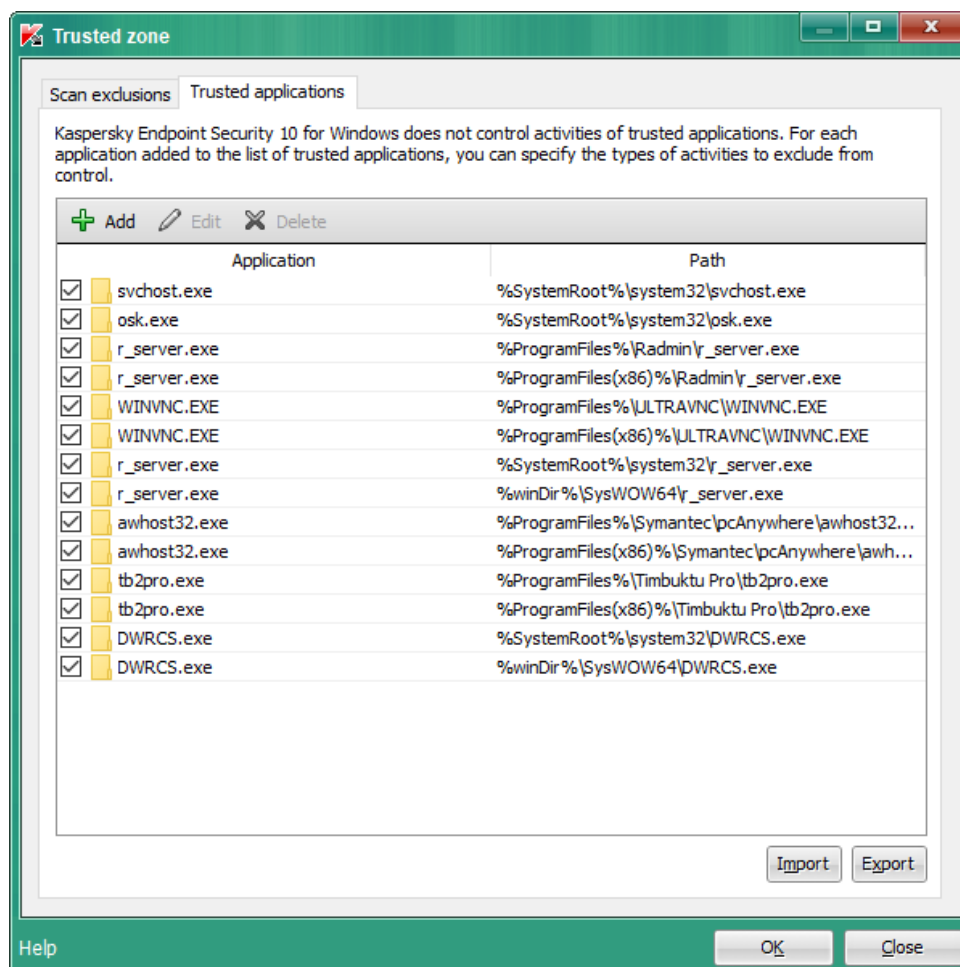


امکان بسیار خوبی که این Component در اختیار شما می گذارد این است که در قسمت Exclusions and trusted zone می توانید یک Application یا یک Folder را Exclude کنید که چه Component هایی از آنتی ویروس بر روی آن فعال نباشد (و یا حتی تمامی Component های آنتی ویروس بر روی آن غیر فعال باشد).

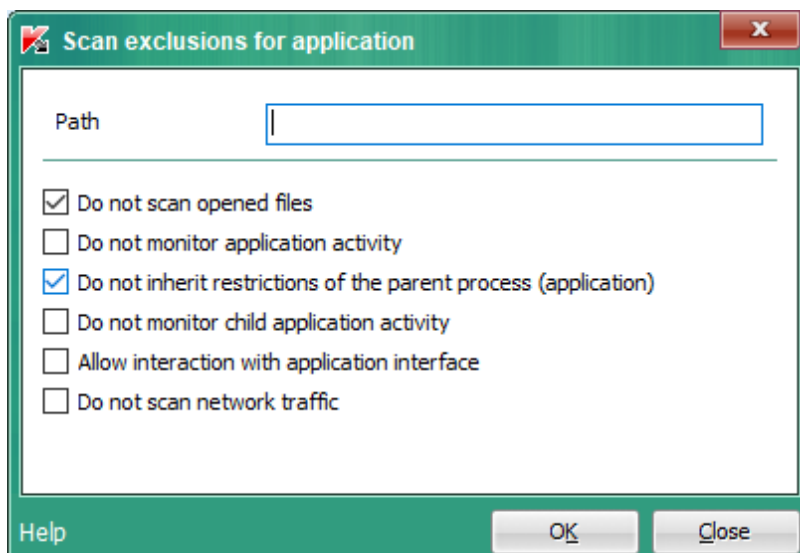
از این ویژگی زمانی استفاده می شود که به طور مثال نرم افزاری که تحت شبکه کار می کند پس از نصب آنتی به کندی کار کند و یا به عنوان ویروس شناخته شود یا به نحوی جلوی یکسری فعالیت های آن گرفته شود و موجب شود قسمتی از آن کار نکند. همچنین در مواردی که Crack های یک نرم افزار به عنوان ویروس شناخته می شود، از این ویژگی استفاده می شود.

جهت تنظیم این قسمت روی setting کلیک نمایید، سپس وارد تب Trusted application شوید.

در این قسمت می توانید یک application را Add کنید تا دیگر Component های آنتی ویروس بر روی آن کار نکند. برای اینکار این بار مسیر مورد نظر را در قسمت Application rules وارد می کنیم.

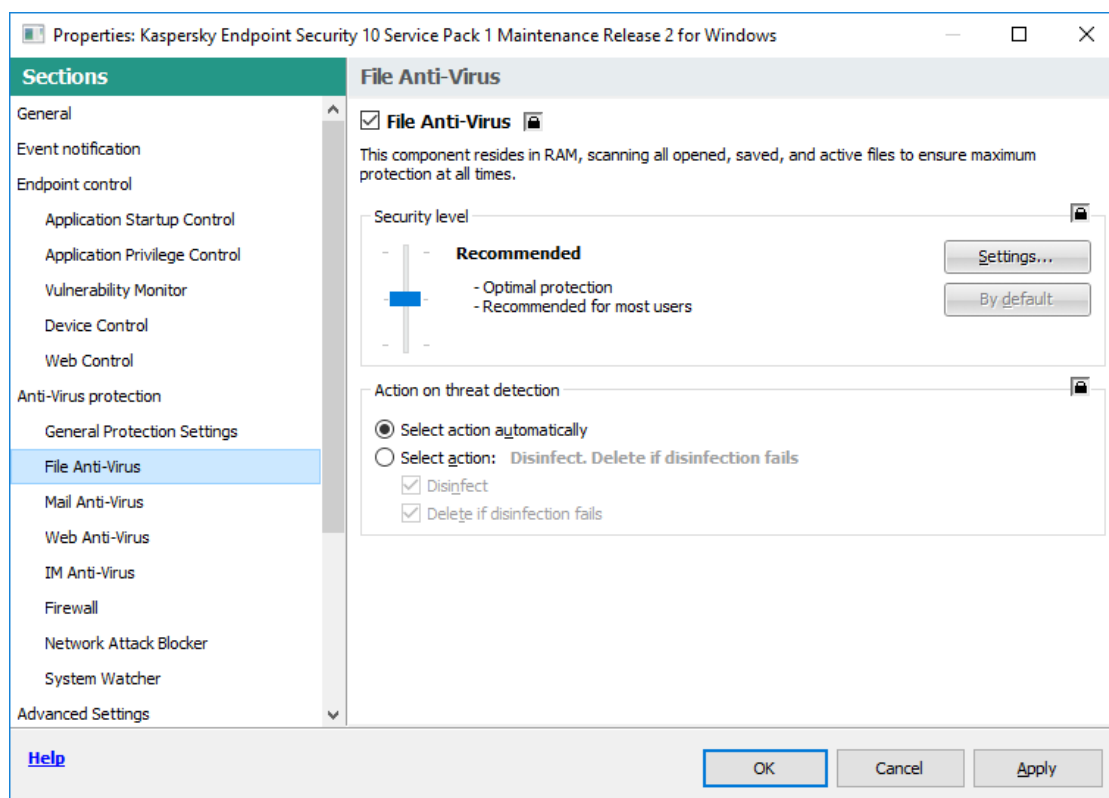


گزینه ی Add را انتخاب کنید و سپس مسیر Application مورد نظر را در قسمت Application وارد کنید و در قسمت Action تعیین کنید چه عملیاتی بر روی این Application صورت گیرد.



در صورتی که بروی تعداد خاصی client مدنظرتان باشد با زدن تیک Do not scan network traffic بروی Any در قسمت IP addresses کلیک کرده و گزینه specify را زده و IP های کامپیوتر های مدنظر را وارد نمایید.

File Antivirus

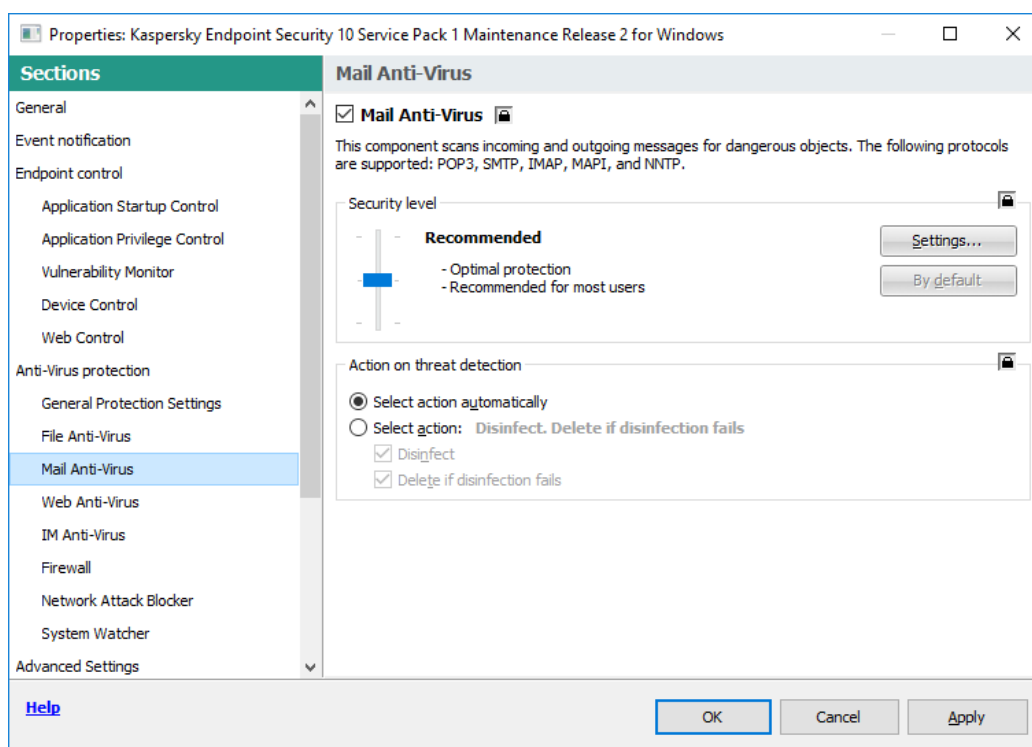


همان طور که مشاهده می کنید قفل ها به صورت پیش فرض بسته است و بنا به نیاز می توانید آنها را باز کنید، با گذاشتن یا برداشتن تیک گزینه Enable File Anti-virus می توانید این Component را روی سیستم ها فعال یا غیر فعال کنید. در قسمت Security level سطح امنیتی این Component را تعیین می کنیم و در قسمت Action نحوه ی برخورد با

ویروس های پیدا شده را مشخص می کنید که آیا آنتی ویروس جهت انجام عملیات خود از کاربران سوالی مبنی برچگونگی برخورد آنتی ویروس با ویروس های شناسایی شده بپرسد یا خیر. پیشنهادها ما تنظیم Action روی گزینه ی Select action است و تیک گزینه های Disinfect و Delete if disinfection fails را بزنید.

Disinfect: با انتخاب این گزینه در صورتیکه تنها قسمتی از فایل آلوده شده باشد، آنتی ویروس تنها قسمت آلوده را پاک می کند (حذف ویروس)

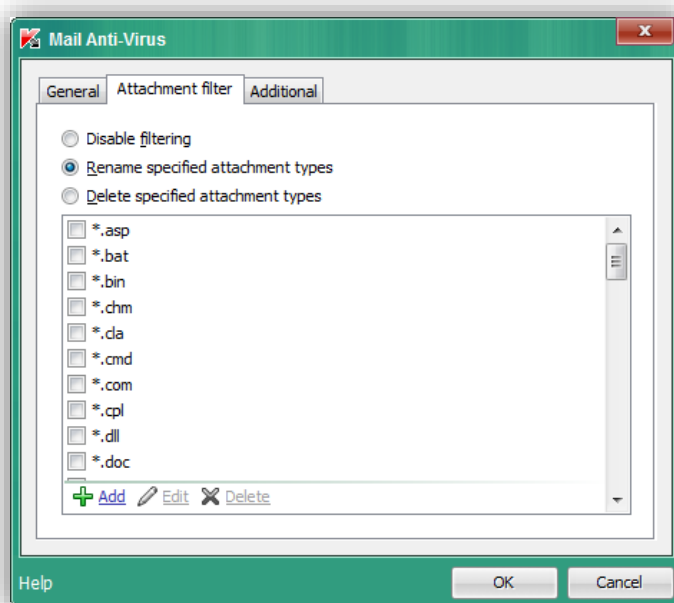
Delete if disinfection fails: در صورتیکه عملیات Disinfect انجام نشود آنتی ویروس کل فایل را پاک خواهد نمود.



Mail Anti-virus

در این بخش نیز Action را در حالت Select action می گذاریم و قفل ها نیز به حالت بسته باقی می ماند در قسمت setting نیز می توانید یک سری تنظیمات را بنا به نیازتان customize کنید.

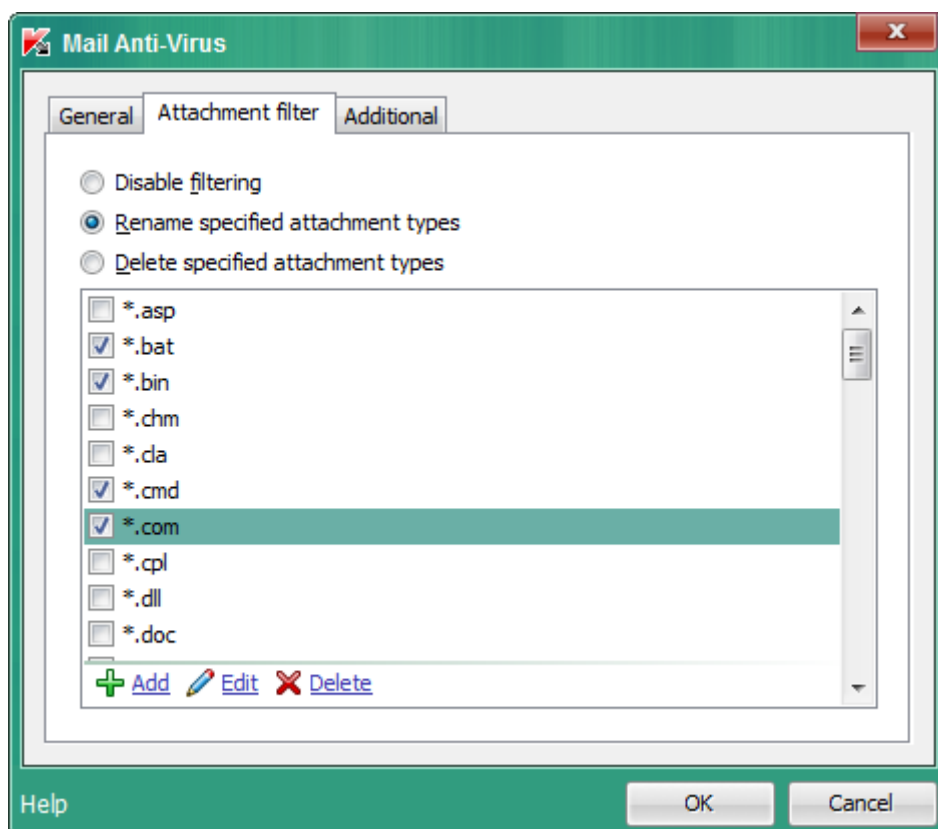
به طور مثال ممکن است یک سری فایل های آلوده به همراه ایمیل ها وارد شبکه ی شما شوند، برای جلوگیری از آلودگی سیستم ها می توانیم در تب Attachment filter یکسری تنظیمات را روی این ایمیل ها اعمال نماییم. برای اینکار روی گزینه ی setting کلیک نمایید و در پنجره ای که باز می شود وارد لبه attachment filter شوید.



با انتخاب گزینه ی Disable filtering ، هیچ Filtering روی ایمیل ها اعمال نمی شود.

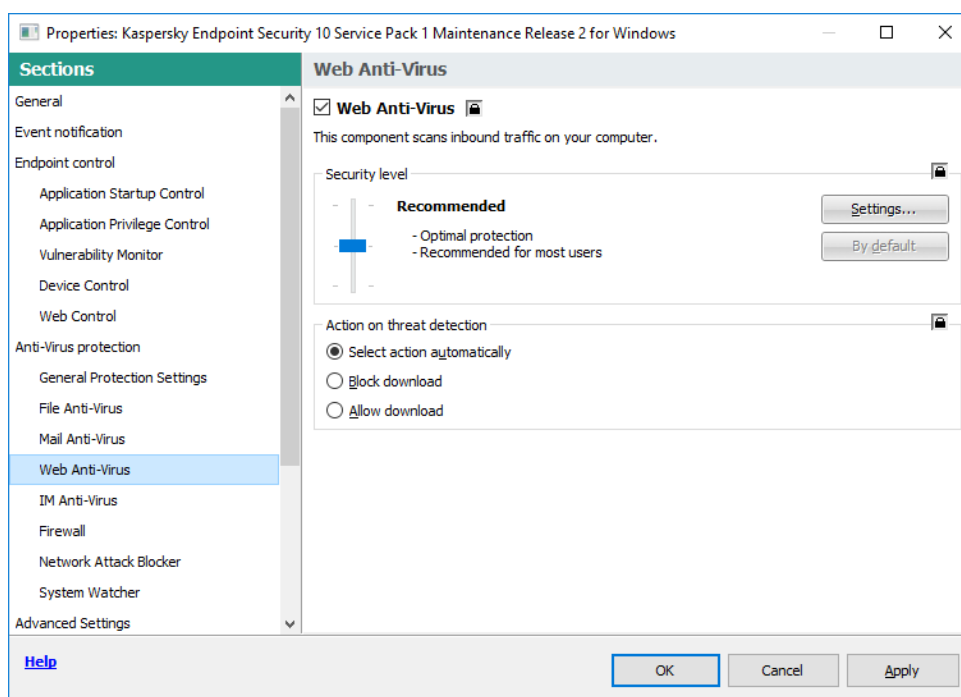
همچنین با انتخاب گزینه ی Rename specified attachment type ، در صورت دریافت ایمیلی همراه Attachment ی با پسوند های انتخاب شده در لیست ، این پسوند تغییر نام خواهد داد (در واقع فایل ویروسی همراه ایمیل، دارای Script ی است که پس از Rename شدن قادر به اجرا نمی باشد).

در صورتی که بخواهید Attachment ی با پسوند های خاصی هنگام دریافت به صورت اتوماتیک Delete شوند می توانید با انتخاب گزینه ی Delete selected attachment types و انتخاب پسوند های مورد نظر از لیست مربوطه آنها را delete کنید.

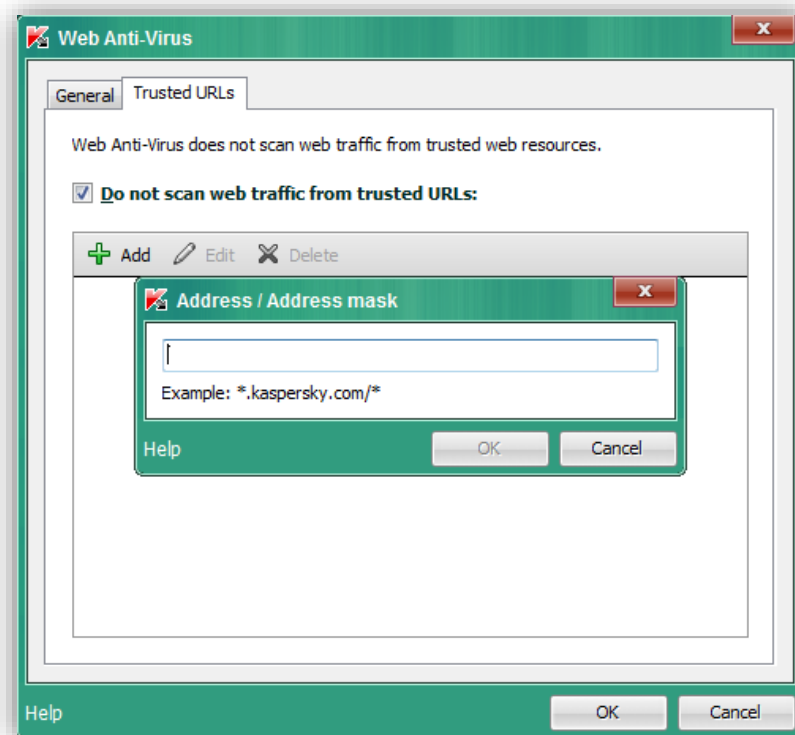


Web Anti-virus

برای Web آنتی ویروس Action را به حالت Block می گذاریم و در قسمت setting می توانیم URL های Trust مورد نظر خود را مطابق نمونه تعریف کنیم.

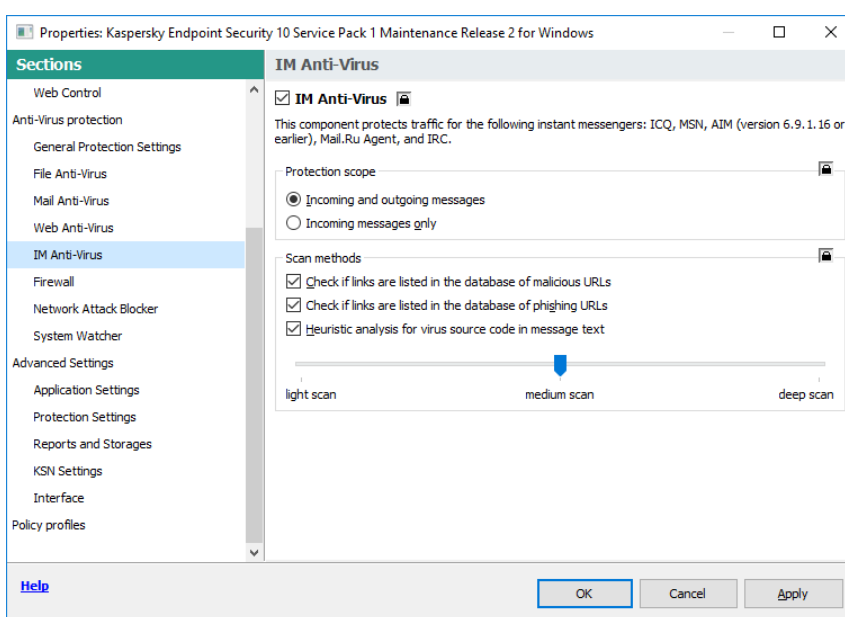


برای اینکار وارد قسمت settings شوید و وارد تب Trusted URLs شوید و مطابق نمونه URL مورد نظر خود را وارد کنید.



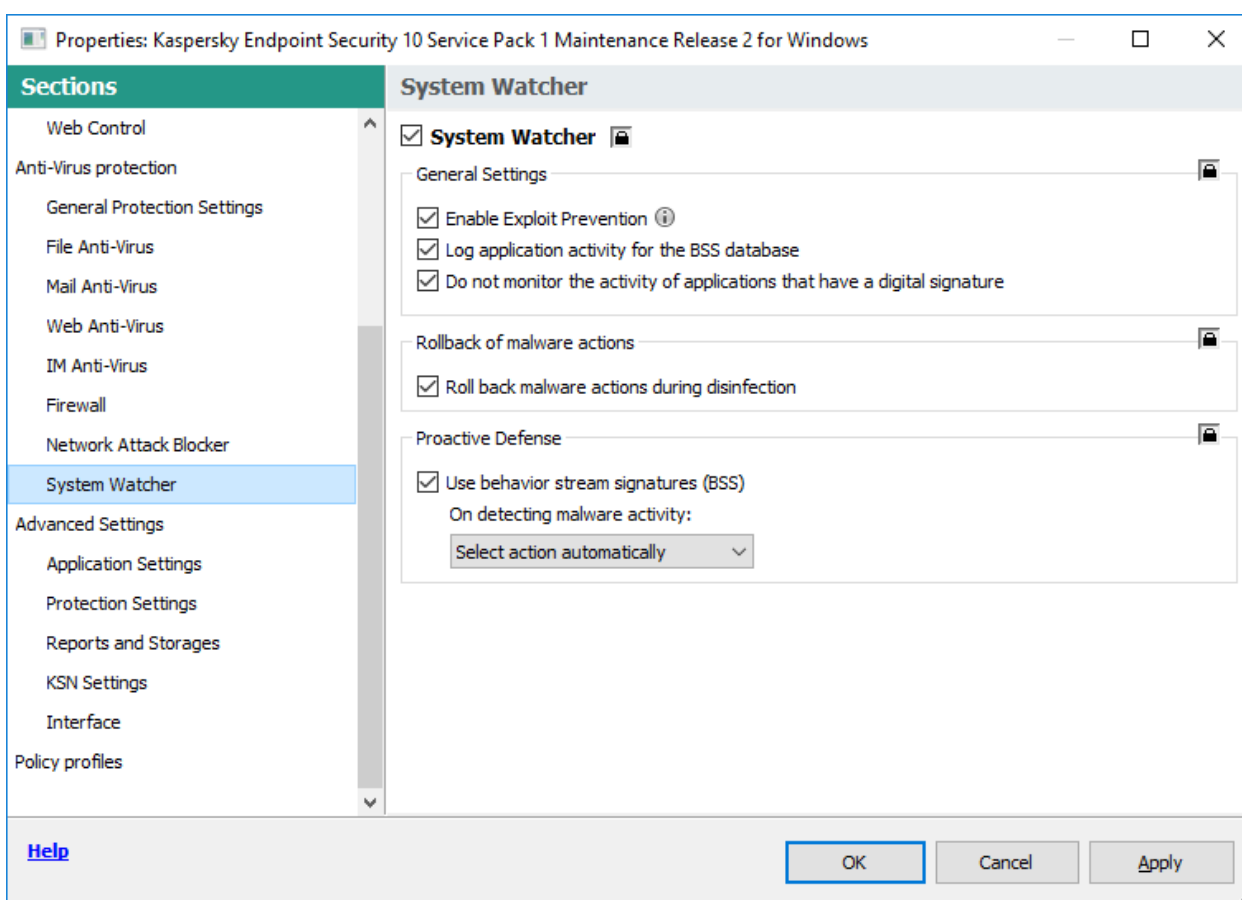
IM Anti-Virus

این Component ترافیک های ورودی و خروجی مربوط به Messenger های ICQ, MSN, AIM, Mail.Ru Agent, IRC را حفاظت می کند.



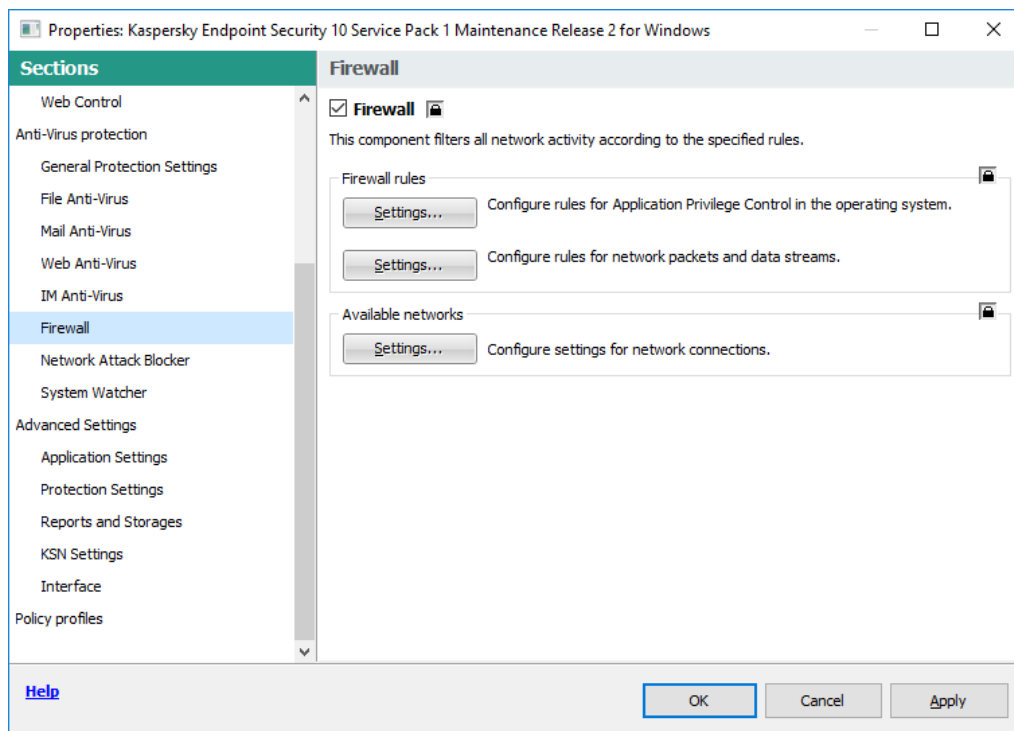
System Watcher

این component یک حفاظت پیشگیرانه در برابر تهدیداتیست که در database آنتی ویروس هنوز نا شناخته است. در واقع این Component با مانیتور کردن فعالیت Application ها داخل سیستم های شبکه، اطلاعات جزئی تری برای سایر Component های آنتی ویروس جهت حفاظتی عمیق تر، فراهم می آورد.

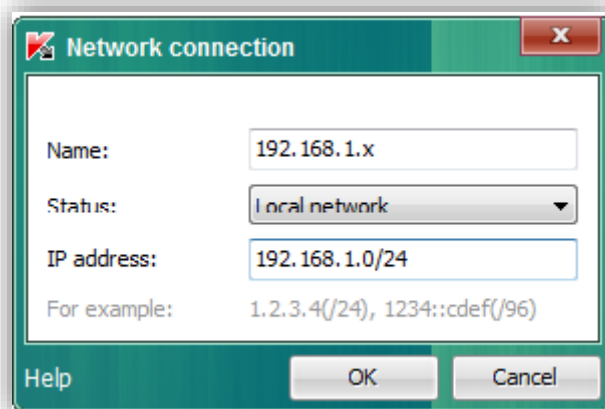


Firewall

این Component تمامی فعالیت های شبکه را بر اساس قوانین مشخص شده در بخش Firewall rules فیلتر می کند. همچنین بادر نظر گرفتن رنج داخلی شبکه، فعالیت های شبکه را مانیتور می کند.

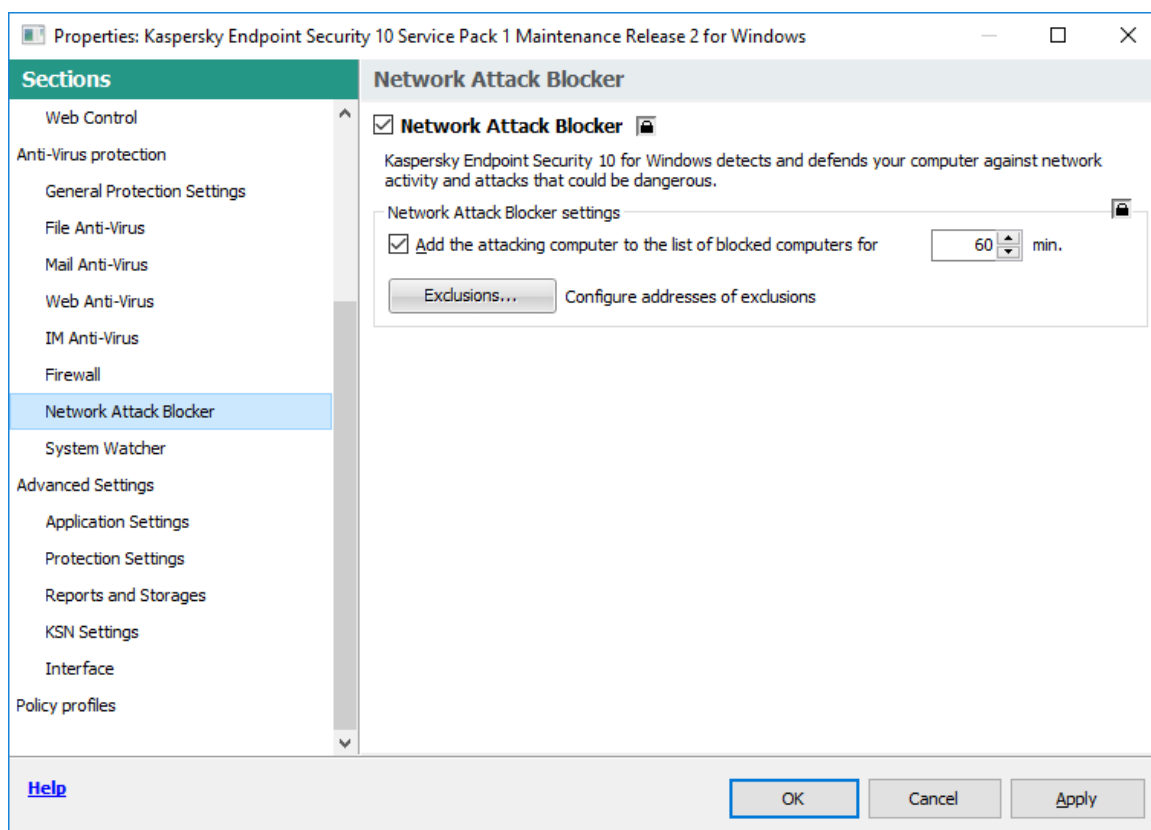


در این قسمت شما باید رنج شبکه خود را بعد از نصب Security Center وارد نمایید برای کار در قسمت Available Setting، Network را زده و با زدن دکمه Add پنجره زیر باز خواهد شد به عنوان مثال اگر رنج شبکه شما 192.168.1.0 تا 192.168.1.255 باشد برای وارد کردن اطلاعات به صورت زیر اعمال نمایید



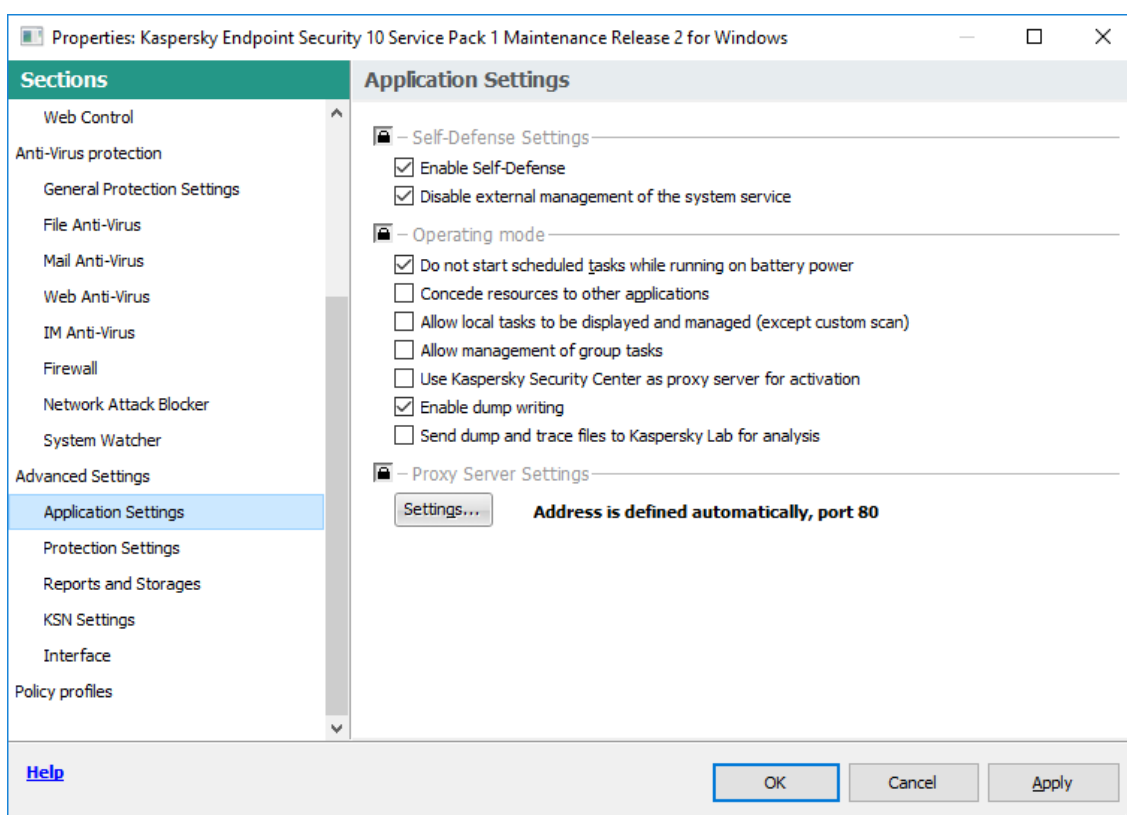
Network Attack Blocker

این component از شبکه شما در برابر حملات داخلی و خارجی که ممکن است برای سیستم های شبکه خطرناک باشد، حفاظت می کند.



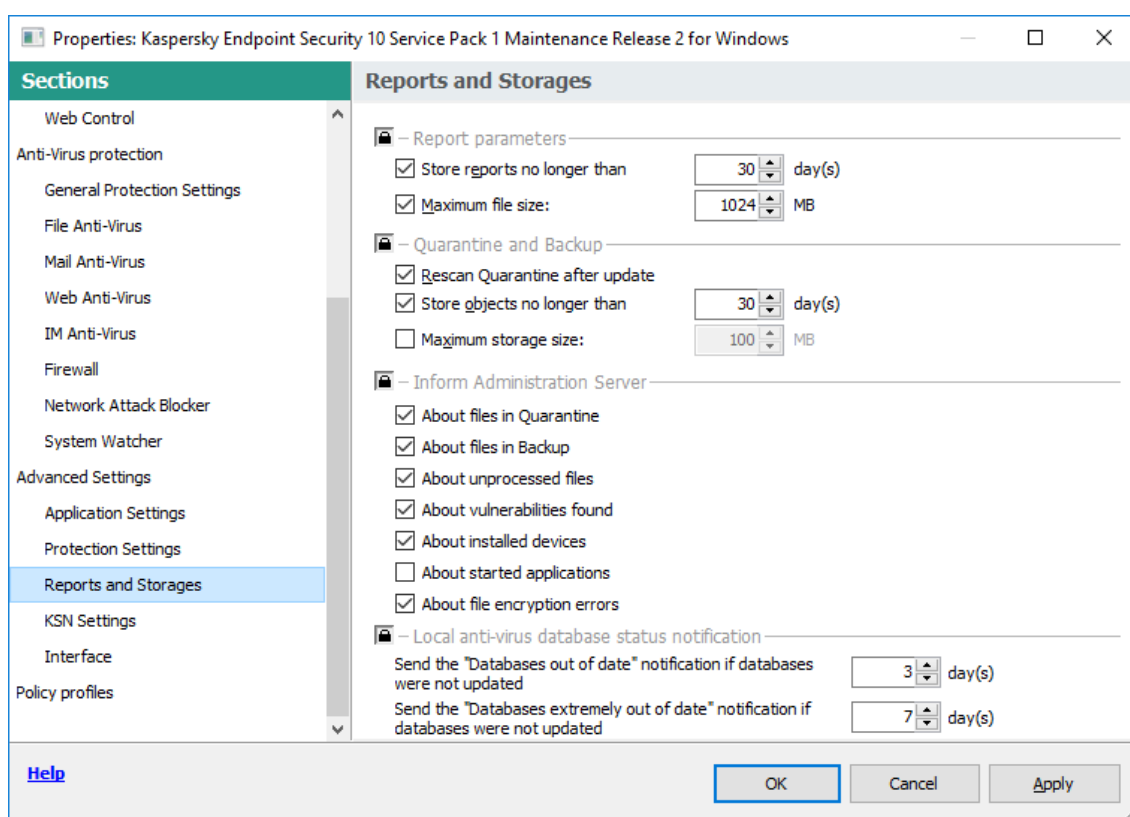
Application Setting

این قسمت مربوط به تنظیمات آنتی ویروس می باشد، به طور مثال با فعال کردن گزینه ی Allow management of group task می توانید به کاربر این امکان را بدهید که به صورت Local، Task های Update و Scan آنتی ویروس خود را مدیریت کند.



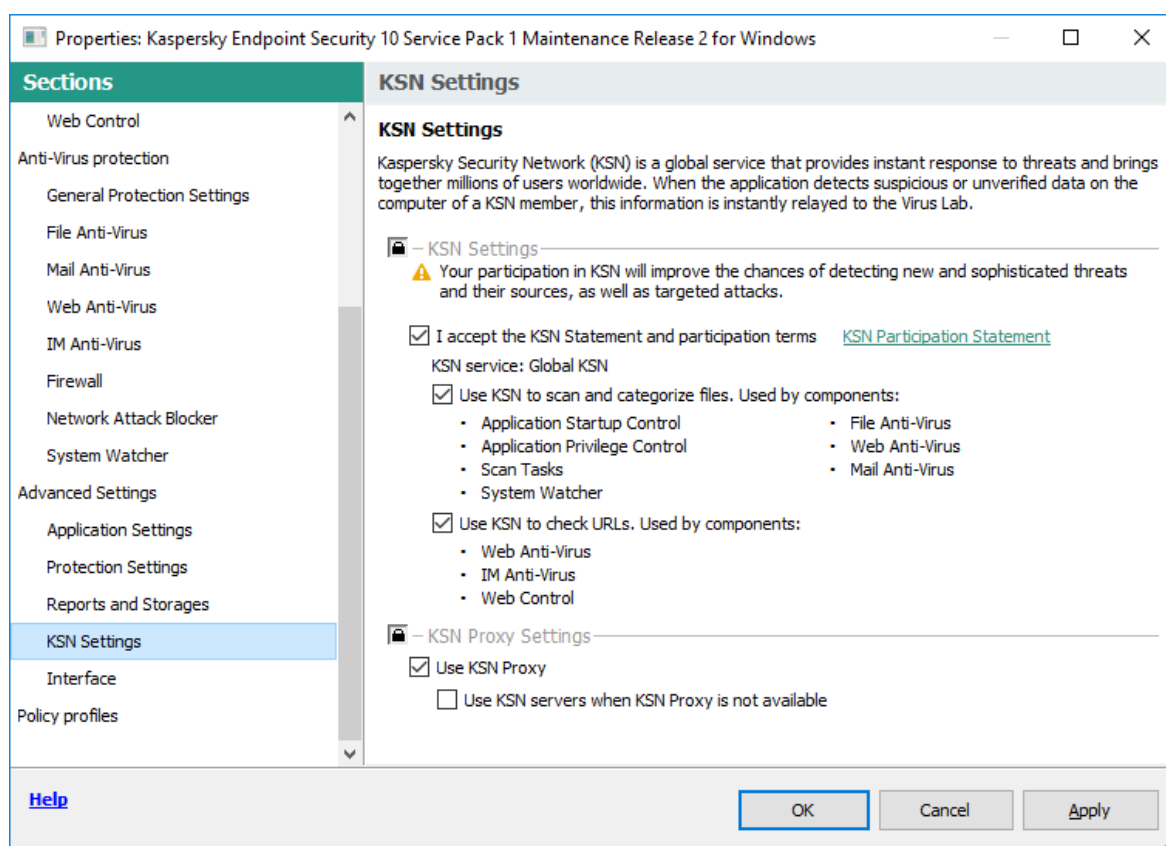
Reports and storages

این قسمت از آنتی ویروس مربوط به تنظیمات گزارش گیری آنتی ویروس ونحوه ی ذخیره سازی آن می باشد.



KSN Setting

یک سرویس جهانی است در جهت فراهم آوردن پاسخی فوری به تهدیداتی که ممکن است شبکه ی شما را مختل کند. در واقع این سرویس میلیون ها کاربر را در سطح جهان دور هم گردآوری می کندو زمانی که آنتی ویروس اطلاعات مشکوک یا تایید نشده ای را بر روی یک کامپیوتر عضو KSN شناسایی می کند این اطلاعات به سرعت برای لابراتوار شناسایی ویروس ها فرستاده می شود.



موفق باشید

پشتیبانی فنی شرکت ایدکو