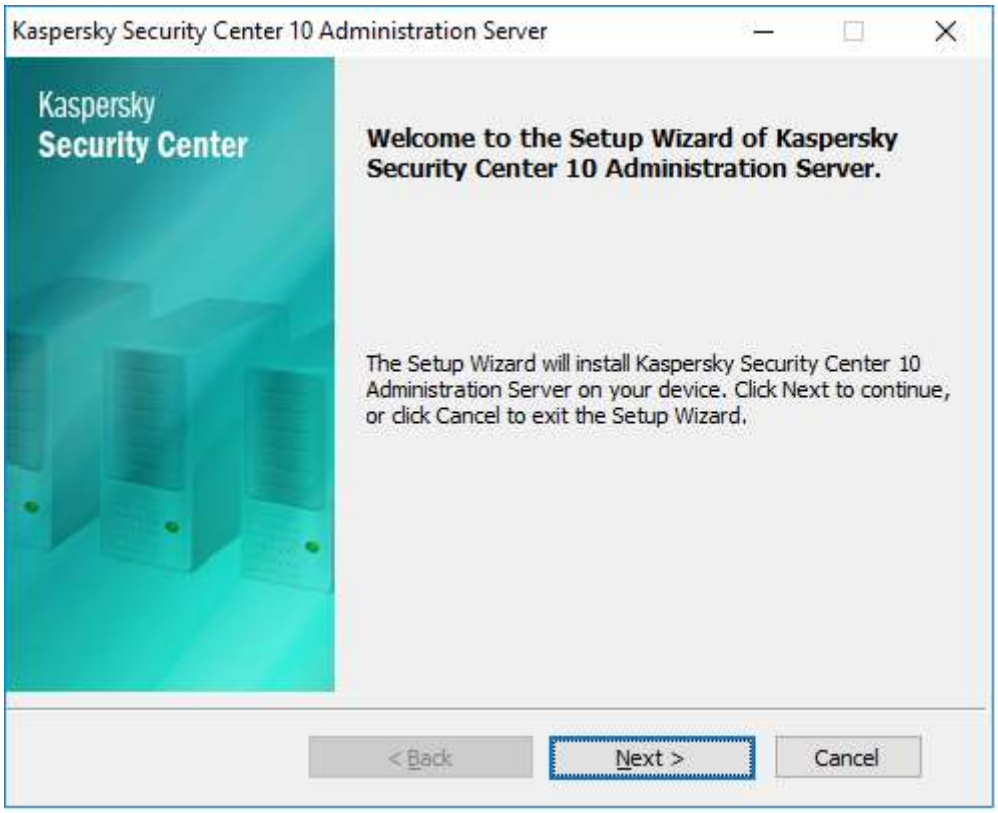
نصب و مدیریت Kaspersky Security Center

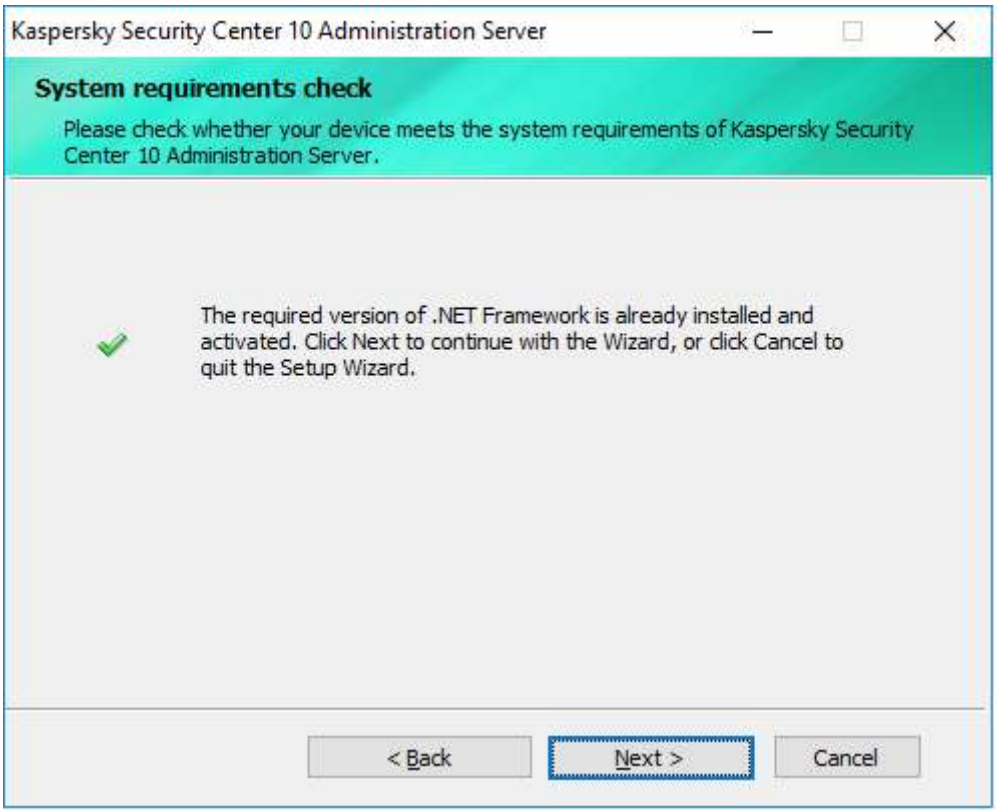
نصب سرور کسپرسکی (Kaspersky Security Center):

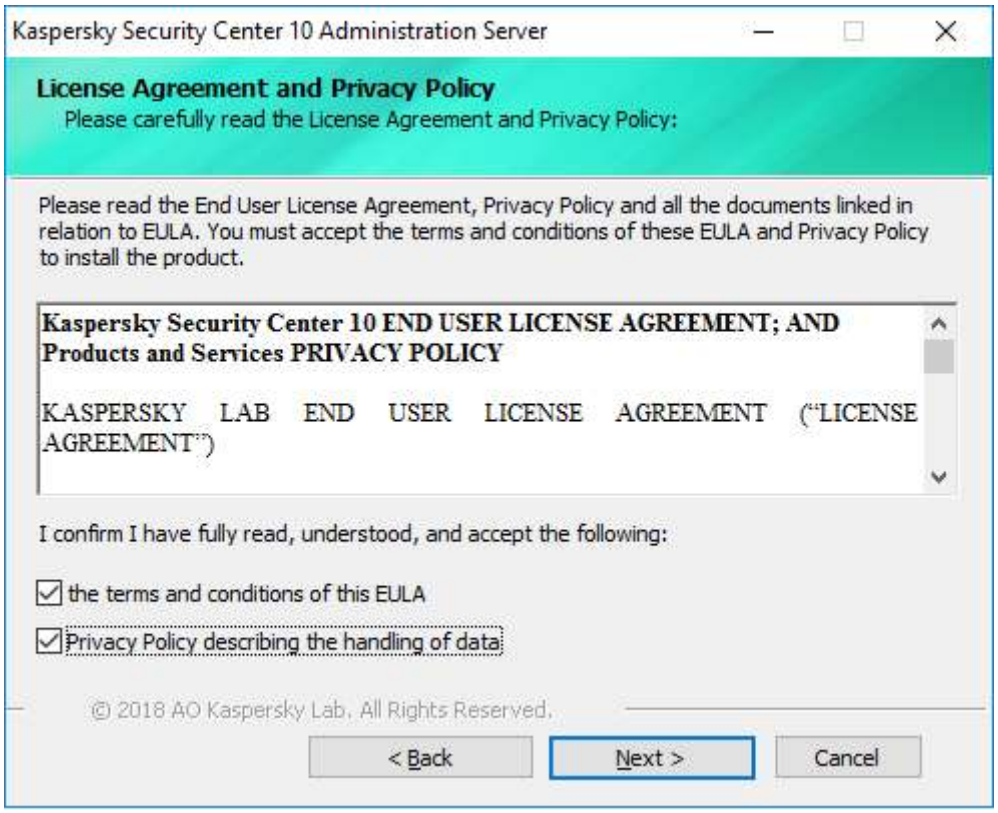
جهت نصب کنسول مرکزی آنتی ویروس، وارد DVD دریافتی شده و مانند تصاویر زیر از درون پوشه Endpoint Security for Business پوشه Kaspersky Security Center ۱۰,۵,۱۷۸۱ را باز کرده و فایل اجرایی موجود در این مسیر را اجرا کنید.

با اجرای این فایل، ویزاردی برای شما باز خواهد شد که با اجرای Install Kaspersky Security Center۱۰ 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.

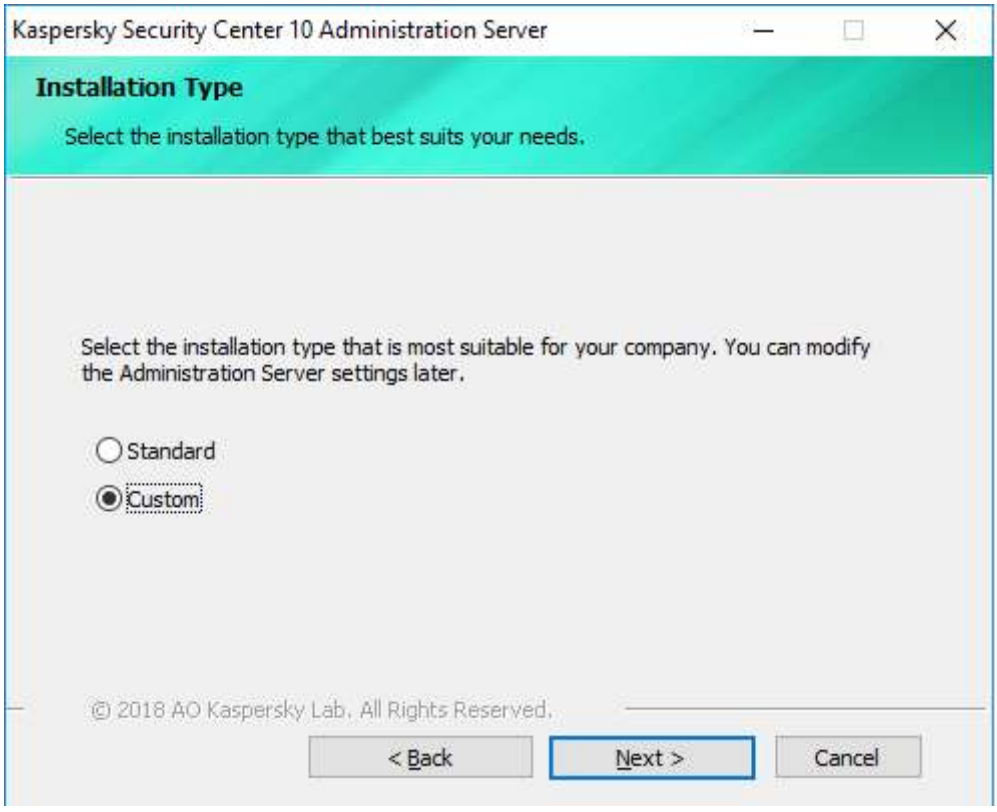
در این مرحله نصب اصلی کنسول آغاز می شود:


Kaspersky Security Center 10 Administration Server
Kaspersky
Security Center
Welcome to the Setup Wizard of Kaspersky Security Center 10 Administration Server.
The Setup Wizard will install Kaspersky Security Center 10 Administration Server on your device. Click Next to continue, or click Cancel to exit the Setup Wizard.
< Back
Next >
Cancel


Kaspersky Security Center 10 Administration Server
System requirements check
Please check whether your device meets the system requirements of Kaspersky Security Center 10 Administration Server.
The required version of .NET Framework is already installed and activated. Click Next to continue with the Wizard, or click Cancel to quit the Setup Wizard.
< Back
Next >
Cancel



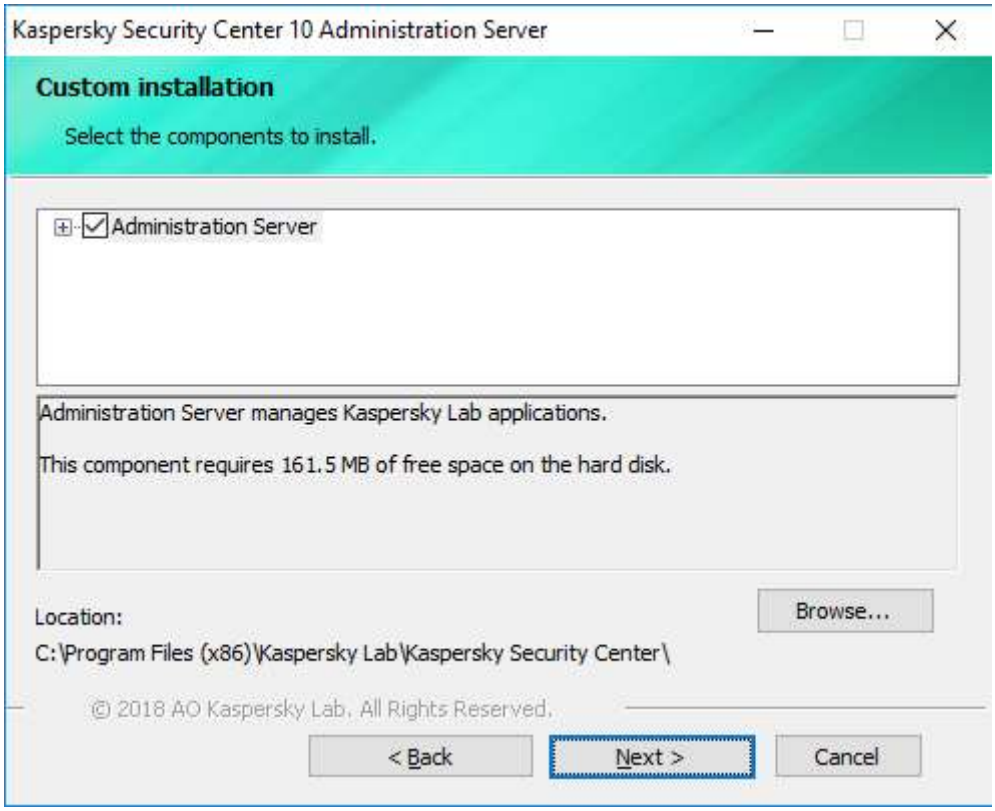
عملیات نصب را به صورت Custom ادامه دهید.



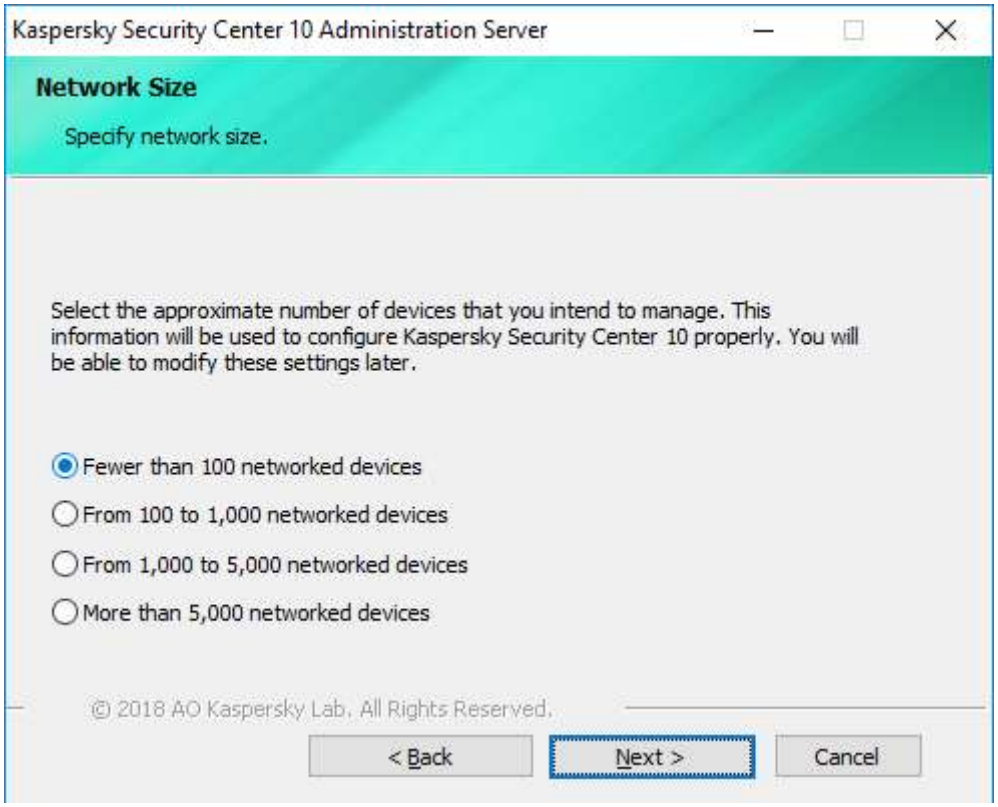
در این قسمت شما Component های مورد نیازبرای نصب Security Center را انتخاب می نمایید. در صورتیکه این سیستم سروراصلی آنتی ویروس شما می باشد، نصب را به همین صورت انجام دهید.در زیر توضیح کوتاهی از Component های موجود خواهید دید.

- 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 درهنگام نصب احتیاج به یک پایگاه داده برای ذخیره اطلاعات دارد.

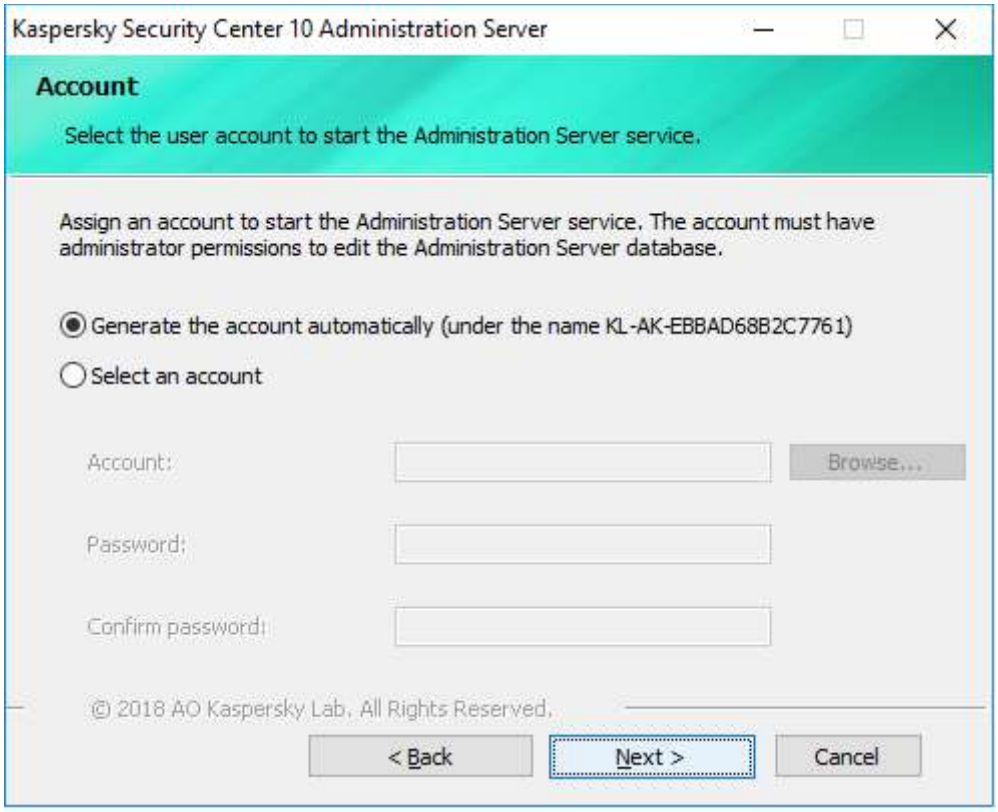
همزمان با نصب این Component نرم افزارNetwork Agent نیز بر روی این سرور نصب می شود که وظیفه برقراری ارتباط بین کلاینت ها و سرور آنتی ویروس را بر عهده دارد، علاوه بر این پس از نصب این نرم افزار بر روی کلاینت ها وظیفه ی انتقال فایل ها و اطلاعات بر عهده آن خواهد بود.



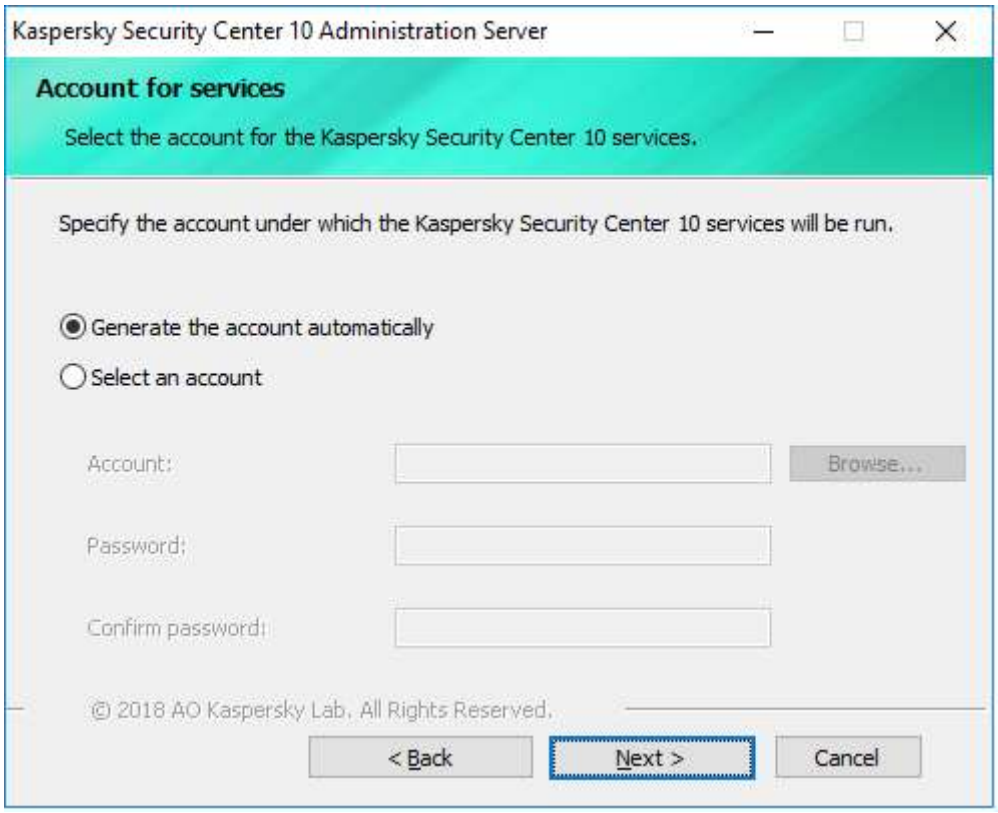
در این مرحله گزینه مناسب را با توجه به وسعت شبکه و با در نظر گرفتن تعداد لایسنس خود انتخاب کنید.



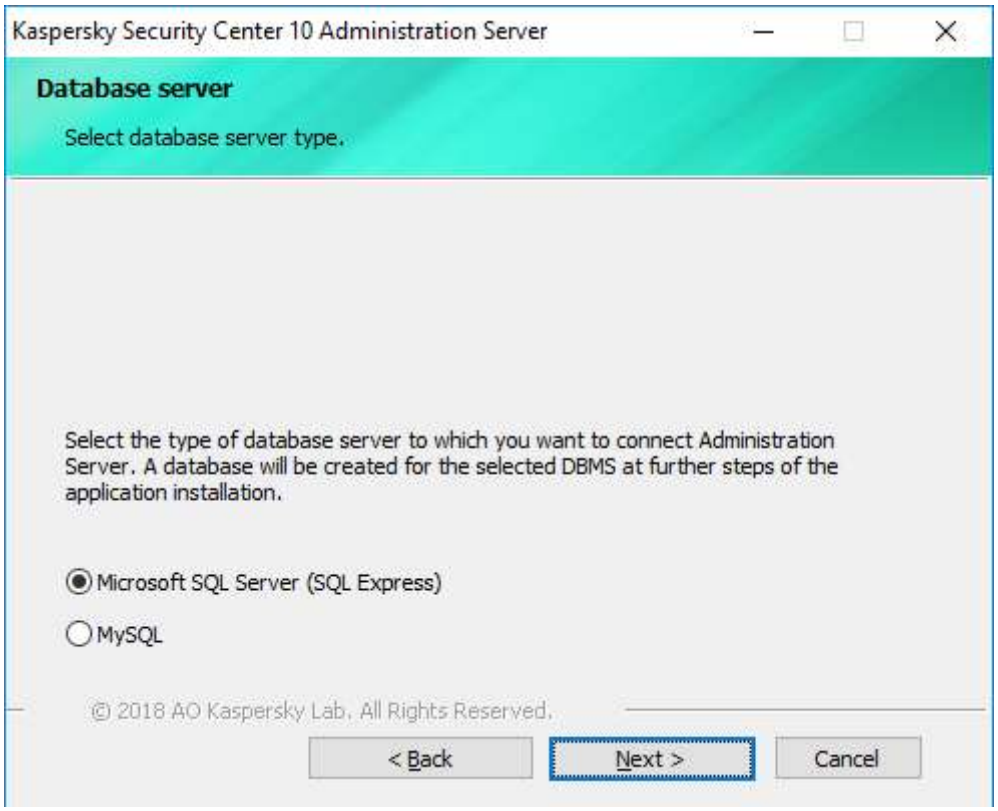
در مرحله بعدی شما باید یک Account برای نصب انتخاب نمایید.در صورت انتخاب گزینه اول، یک اکانت با نام تصادفی ایجاد شده و به طور اتوماتیک عضو گروه های klAdmin و Kloperator در اکتیودایرکتوری میشود. پیشنهاد ما ساخت یک اکانت با نام Kaspersky می باشد این اکانت باید عضو گروه های فوق الذکر شود. اکانت باید داری دسترسی دامین ادمین باشد.



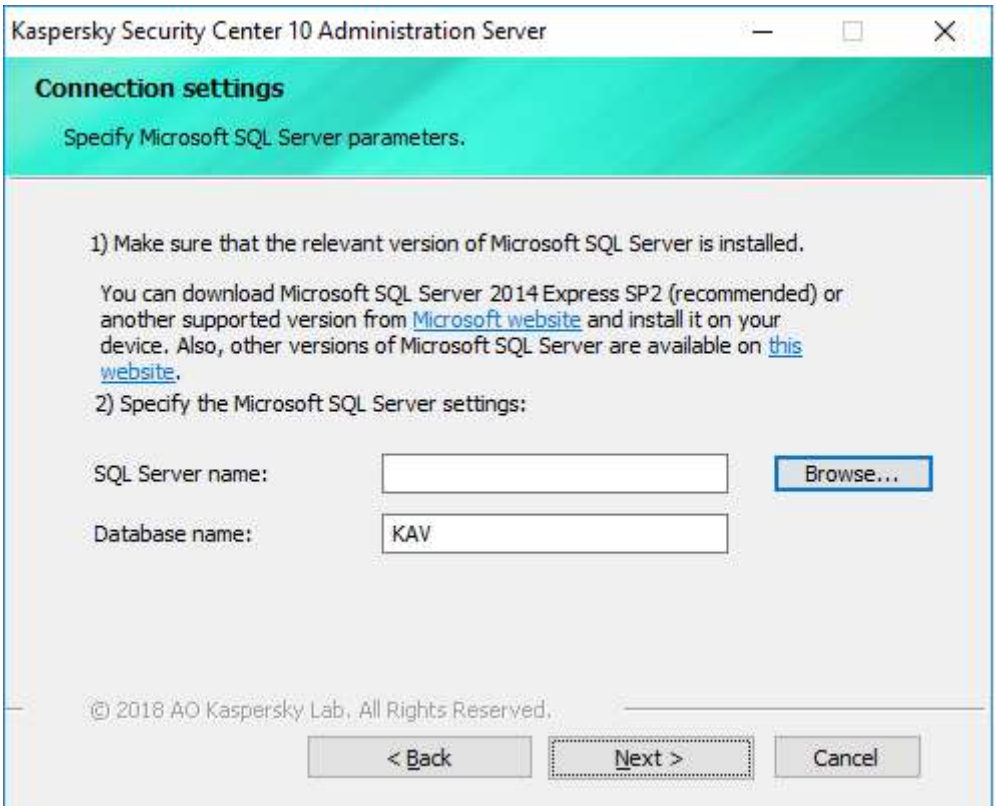
در این مرحله شما باید یک اکانت برای اجرای سرویس ها انتخاب نمایید. اگر گزینه بالا را انتخاب نمایید، اکانتی که در مرحله قبلی انتخاب کرده اید به طور پیش فرض انتخاب می شود.

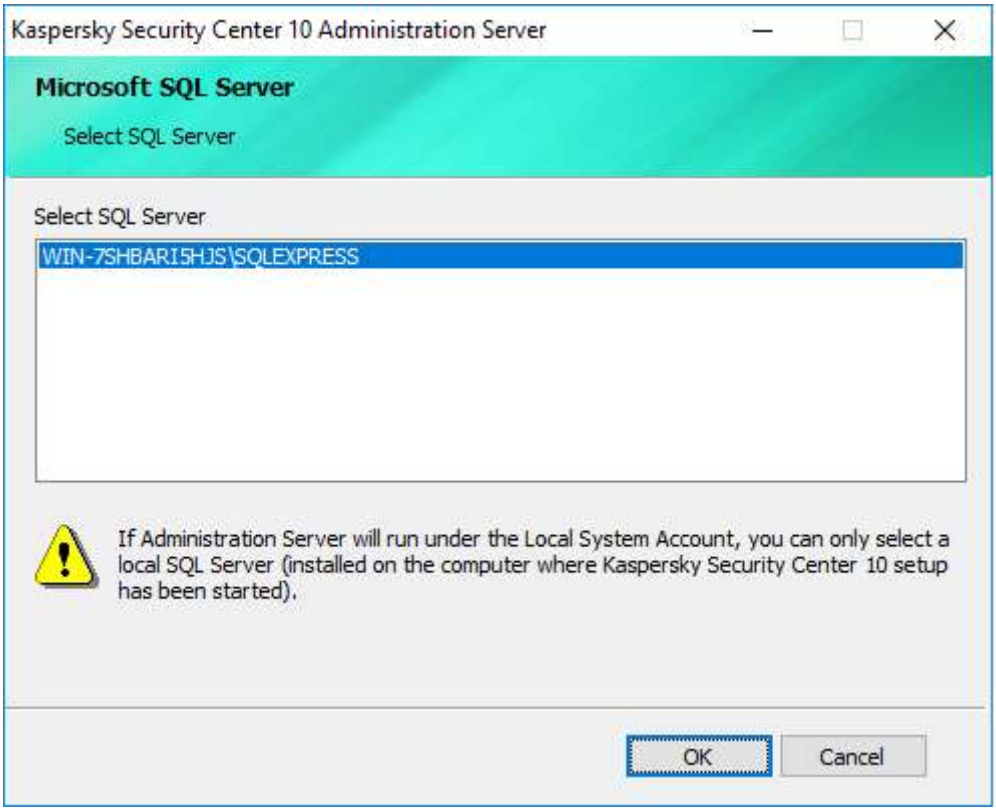


در این مرحله شما باید نوع پایگاه داده را برای استفاده Security Center مشخص کنید.پیشنهاد کسپرسکی استفاده از Microsoft SQL Server می باشد.

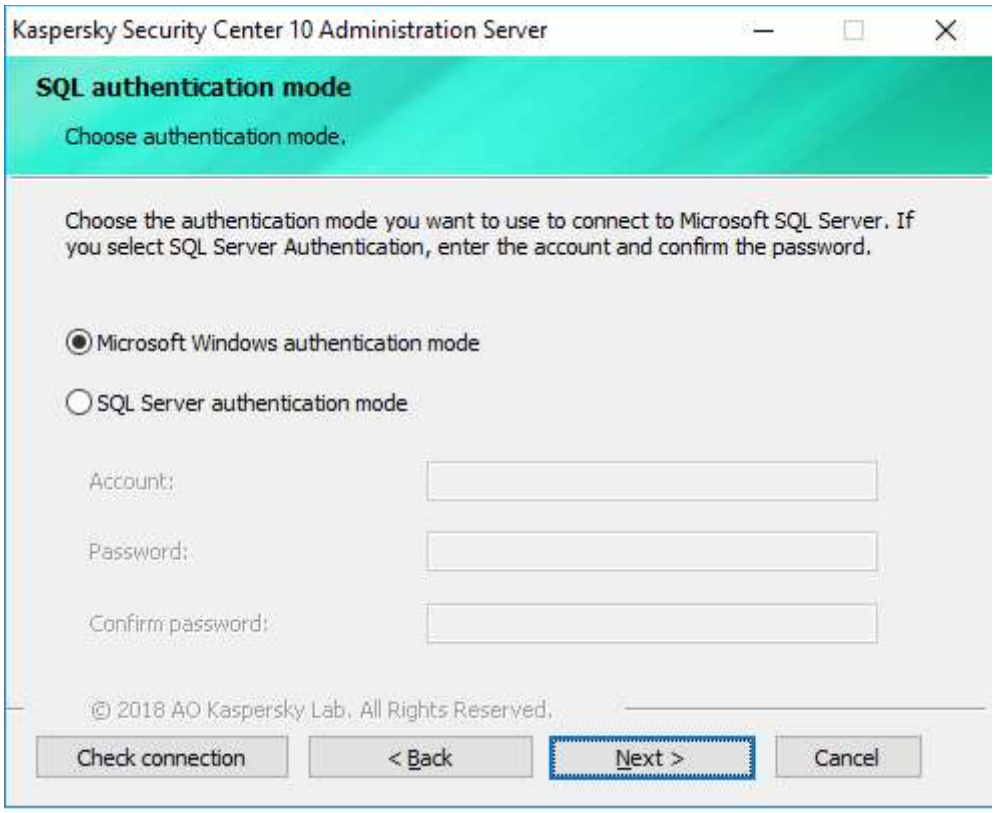


در این مرحله سرور sql که قبلا نصب کرده ایم را انتخاب می کنیم.

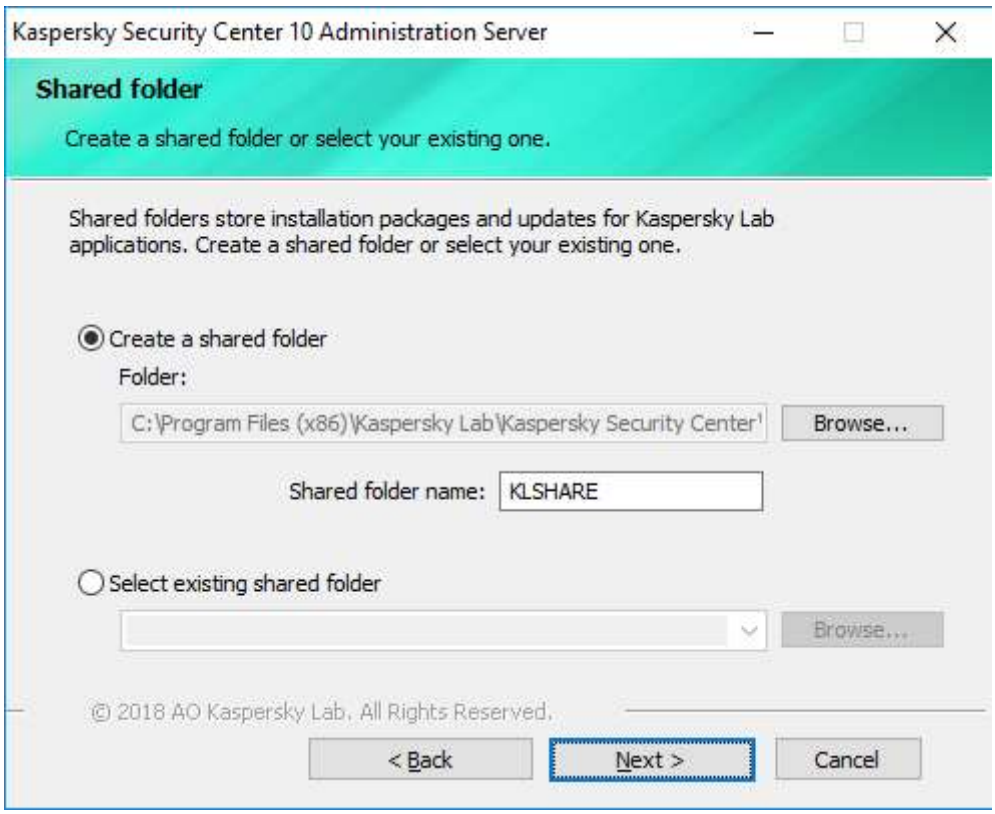




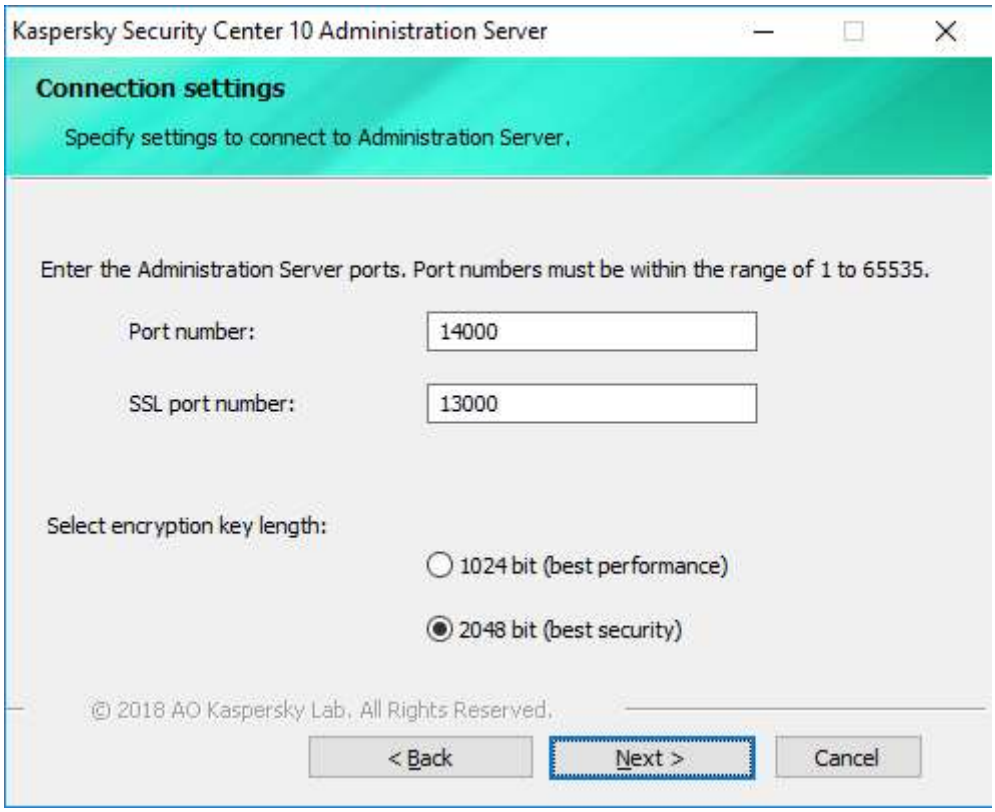
در این قسمت نوع احراز هویت در SQL Server را تعیین کنید. اجازه دهید گزینه ی Windows Authentication Mode در حالت انتخاب باقی بماند.



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 **۱۳۰۰۰** و **۱۴۰۰۰**استفاده می کند. درگاه پیش فرض برای اتصال ۱۳۰۰۰می باشد که یک درگاه امن(SSL) است.در قسمت select encryption key length نوع طول کلید رمزنگاری را مشخص می کنیم. از این مرحله بدون تغییر تنظیمات پیش فرض عبور می کنیم.

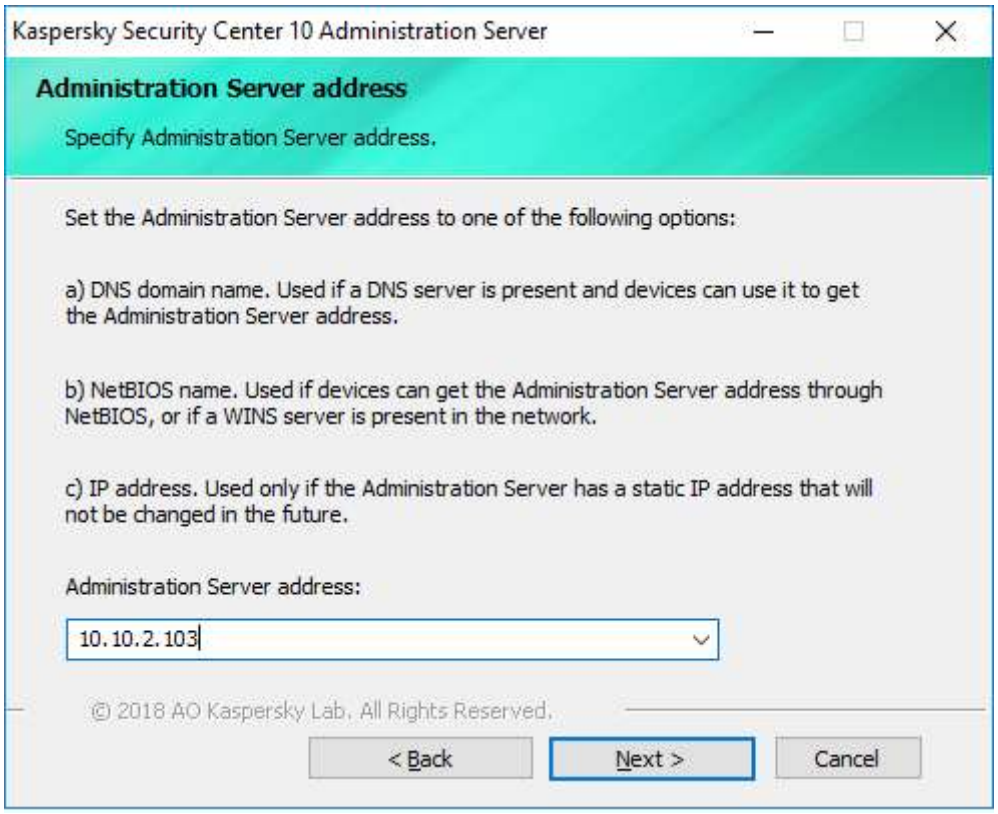


درمرحله بعد، شما باید نحوه ی ارتباط Network Agent نصب شده بر روی کلاینت ها با سرور را مشخص کنید.

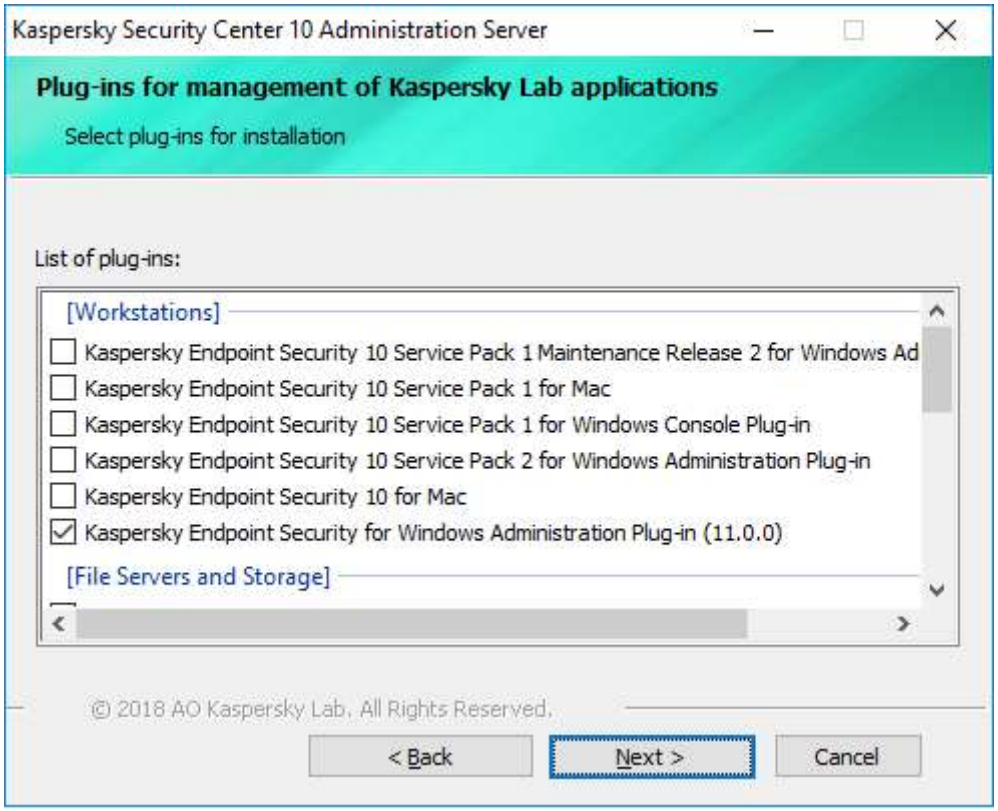
برای ارتباط با سرور، Network Agent می تواند از سه روش زیر استفاده کند:

- **IP Address**: بهترین حالت استفاده از این گزینه می باشد. توجه داشته باشید که در این قسمت حتما از IP سرور استفاده نمایید.
- **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 مجدّداً برقرار کرد.
- **Net Bios Name**: در این قسمت نام خود سرور را انتخاب میکنیم.

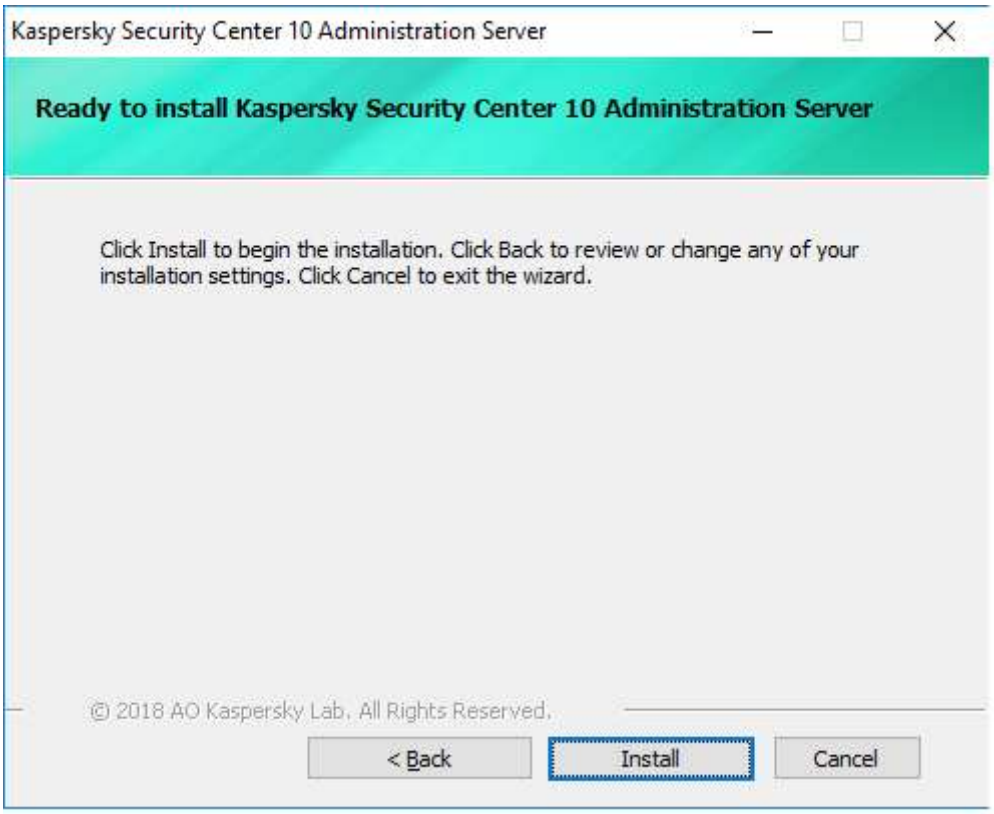
کسپرسکی به صورت پیش فرض از IP Address جهت برقراری ارتباط استفاده می کند.


Kaspersky Security Center 10 Administration Server
Administration Server address
Specify Administration Server address.
Set the Administration Server address to one of the following options:
a) DNS domain name. Used if a DNS server is present and devices can use it to get the Administration Server address.
b) NetBIOS name. Used if devices can get the Administration Server address through NetBIOS, or if a WINS server is present in the network.
c) IP address. Used only if the Administration Server has a static IP address that will not be changed in the future.
Administration Server address:
10.10.2.103
© 2018 AO Kaspersky Lab. All Rights Reserved.
< Back
Next >
Cancel

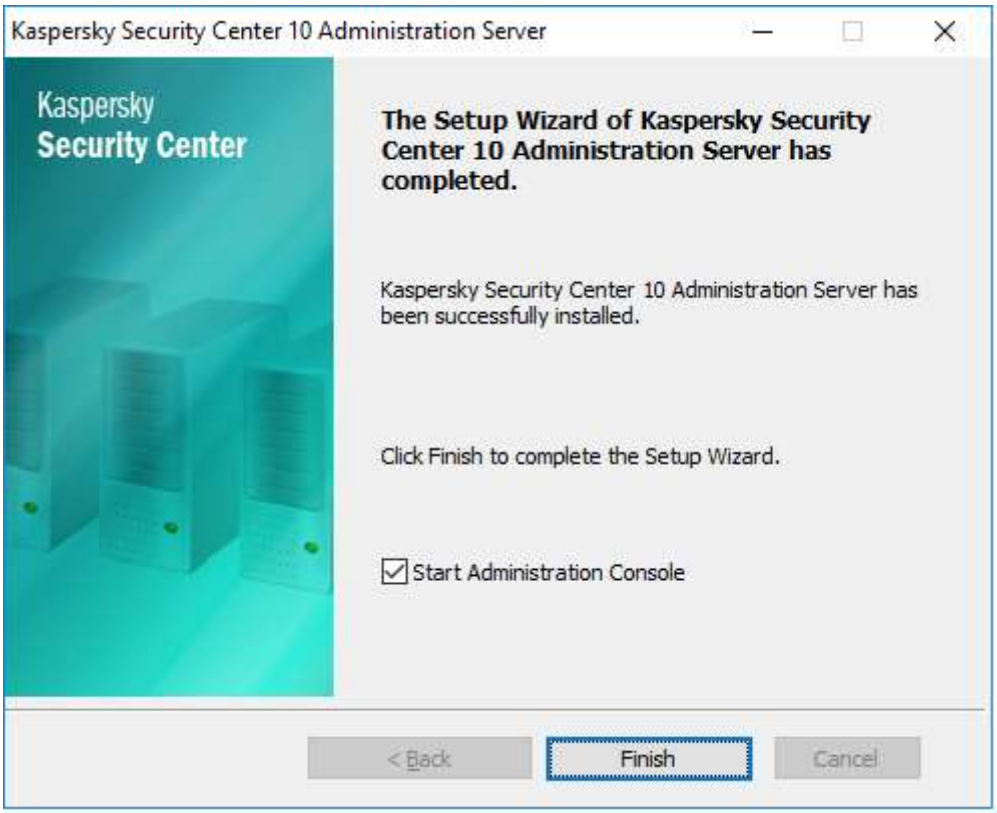
در قسمت بعد شما میتوانید Plugin های آنتی ویروس هایی از کسپرسکی را که می خواهید بر روی سیستم هایتان نصب کنید را انتخاب نمایید تا در زمان نصب کنسول آن ها نیز نصب شوند.



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

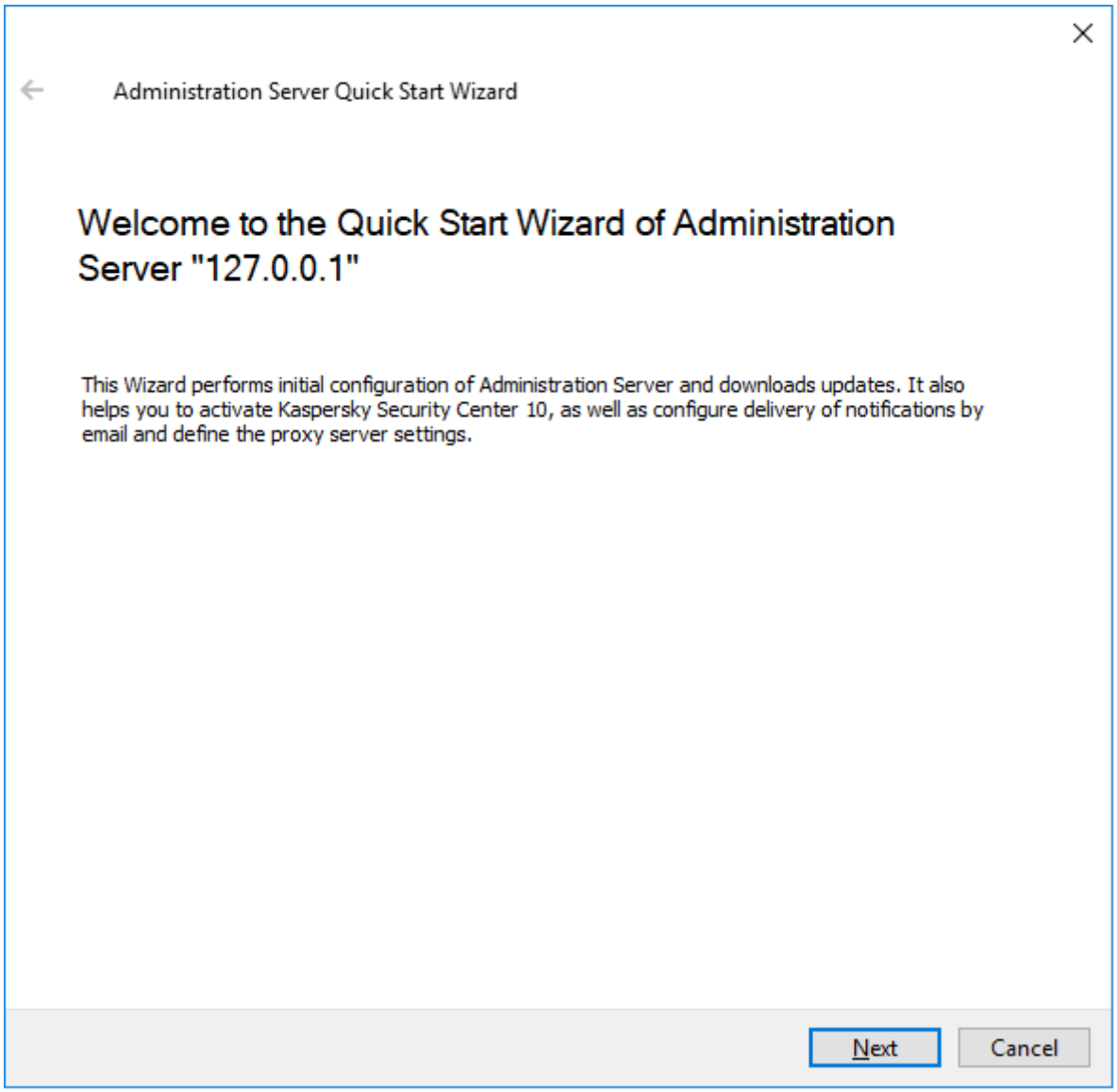


در انتهای نصب بر روی گزینه Finish کلیک کنید.

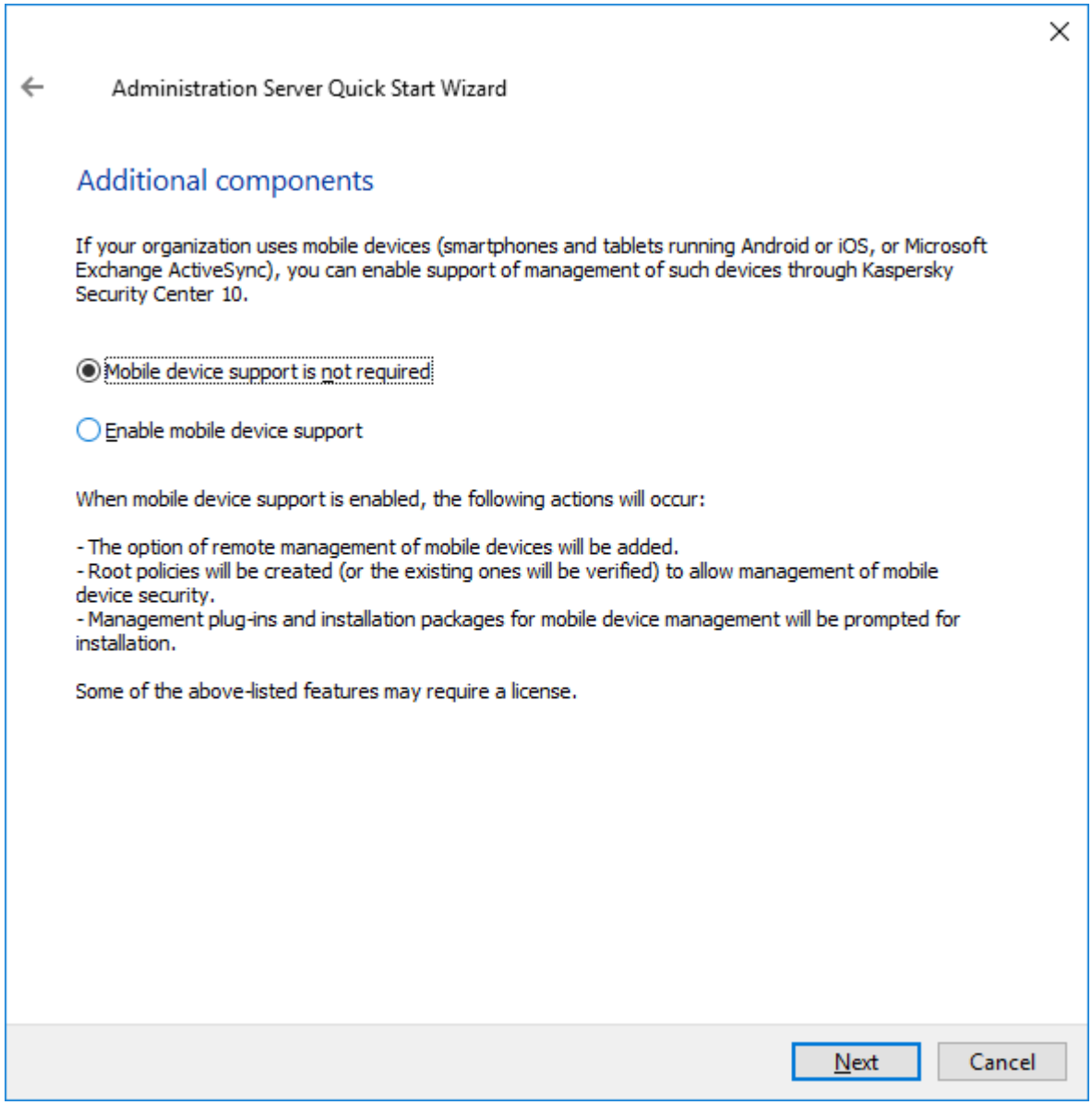


Quick Start Wizard

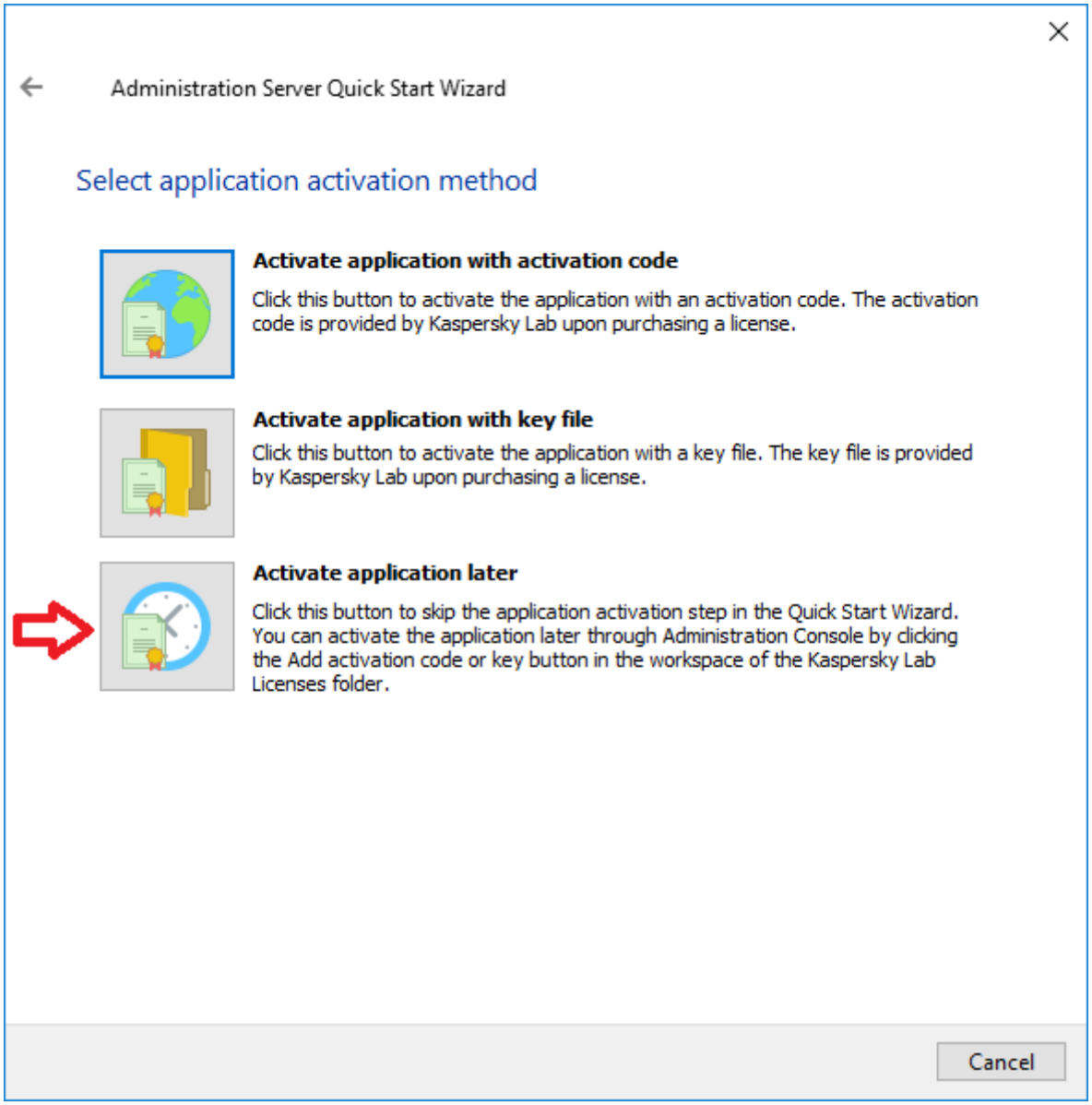
پس از اتمام نصب، پنجره Quick Start Wizard اجرا میشود که Taskها و Policy های اولیه را ایجاد می کند.



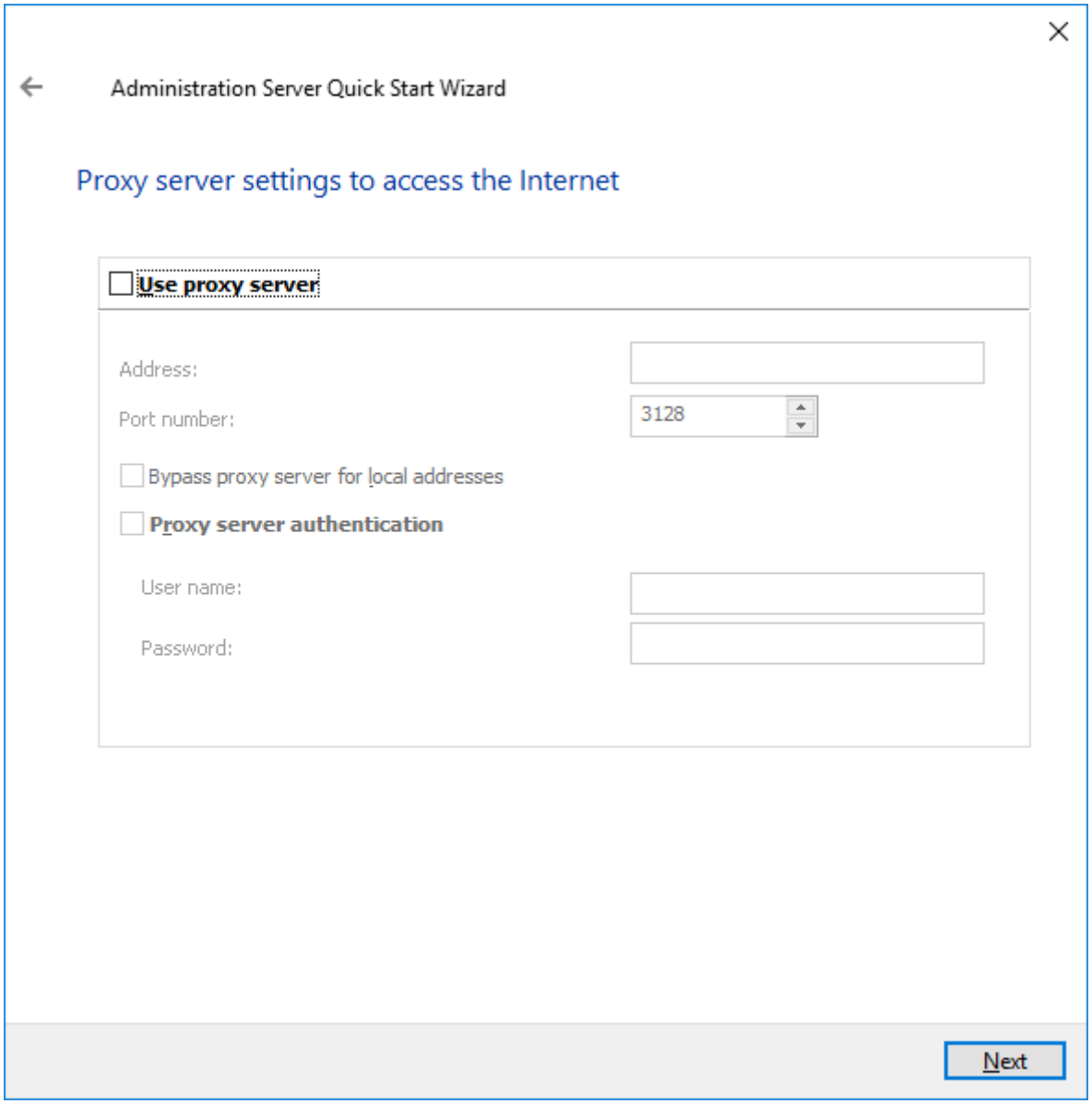
در صورت تمایل برای ایجاد policy موبایل ودستگاه های پرتابل گزینه Enable Mobile device support را فعال کرده و به مرحله بعد بروید.



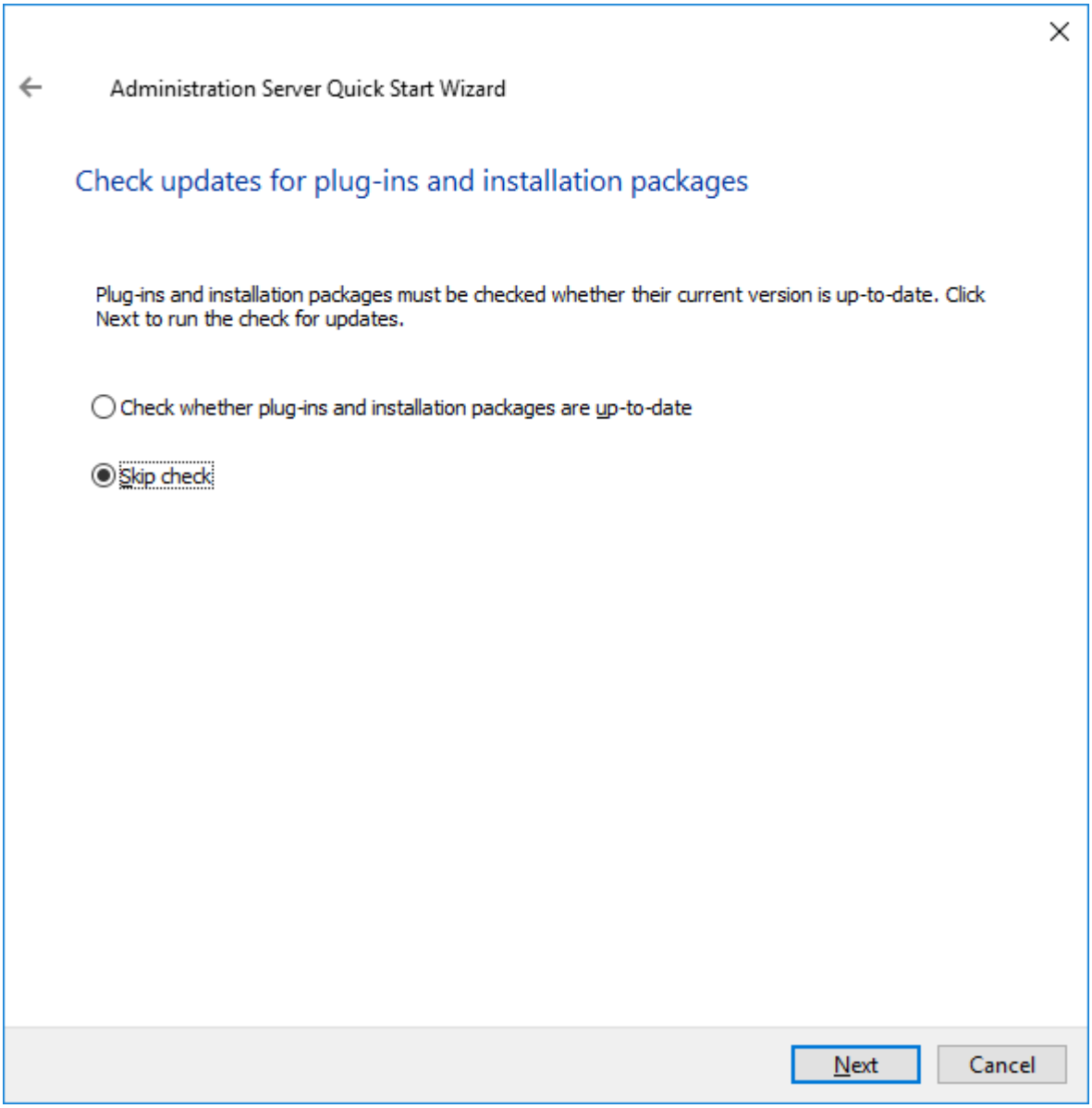
در مرحله بعد لایسنس Security center را از فایل لایسنس اضافه کنید و یا می توانید Activation Application Later را انتخاب و به مرحله بعد بروید.



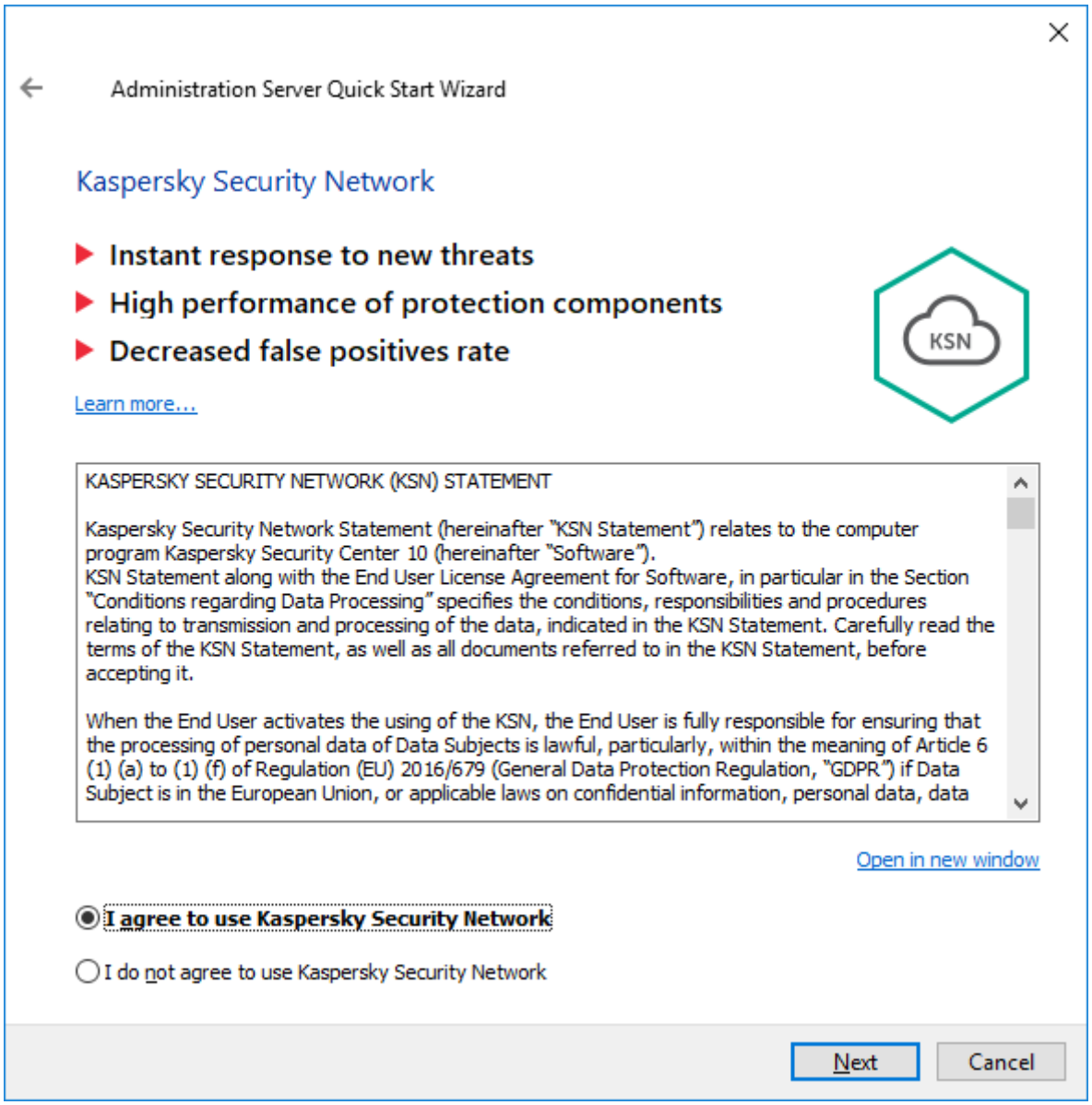
در این مرحله در صورتیکه سرور برای دسترسی به اینترنت از Proxy استفاده می کند، می بایست گزینه Use Proxy Server را فعال کنید و سپس IP Address و پورت آن را وارد نمایید در غیر این صورت به بخش بعدی بروید.



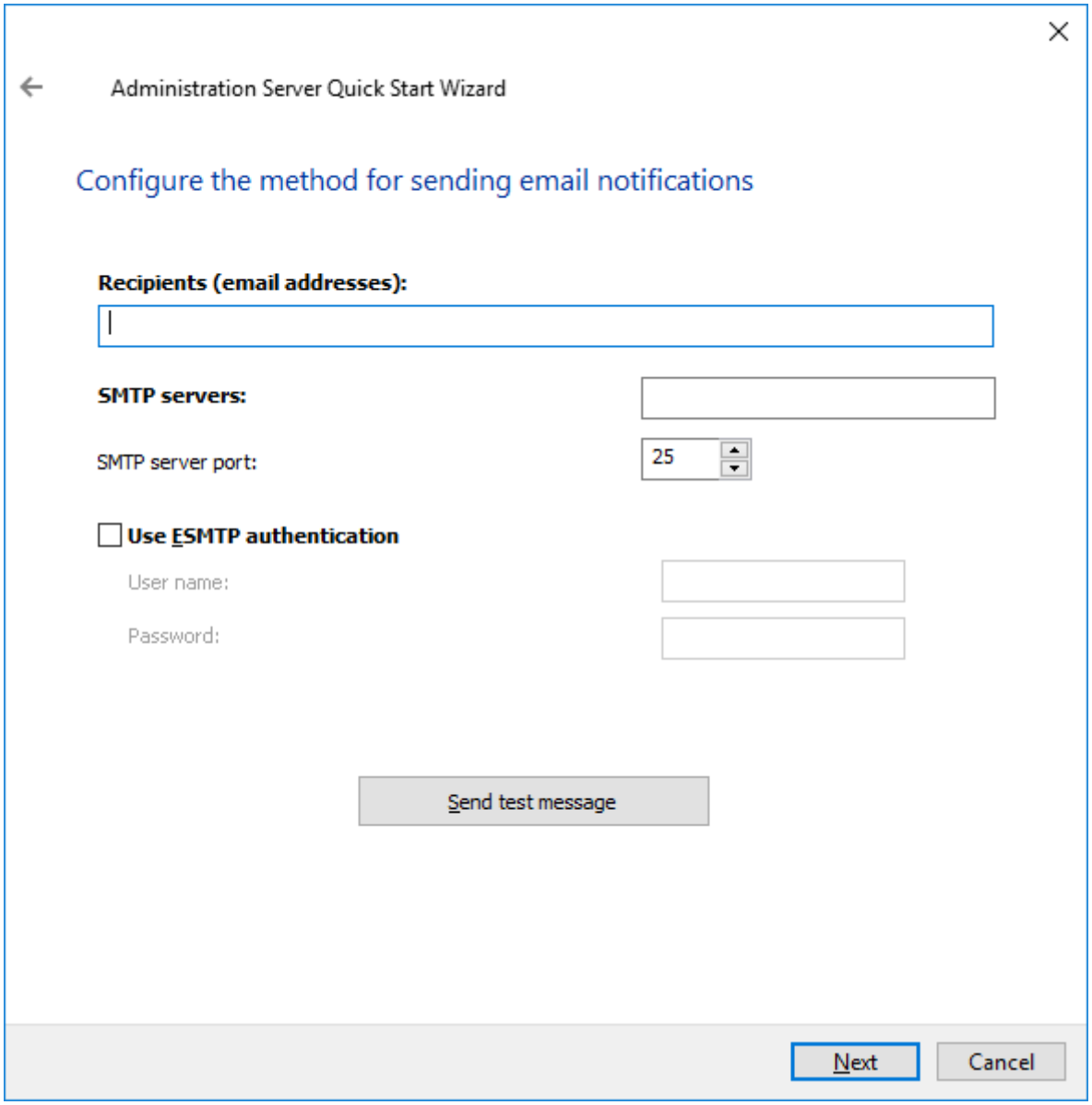
در این مرحله کنسول plug-in های موجود را چک و در صورت وجود plug-in ورژن های قبل، لینک های آپدیت ایجاد میشود. برای سرعت در نصب گزینه skip را انتخاب کنید.



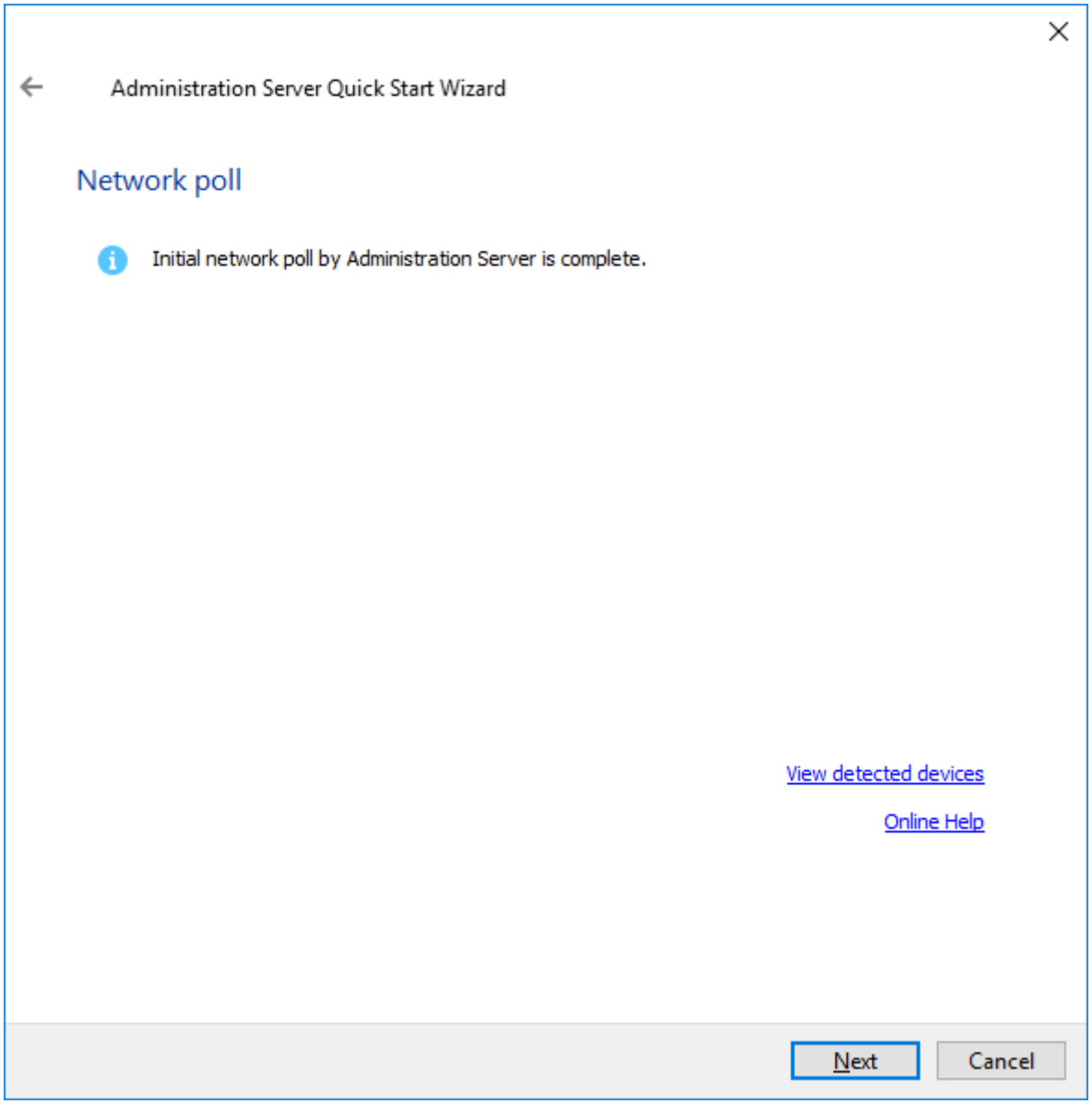
در این مرحله می توانید استفاده از فضای ابری KSN را فعال کنید.Kaspersky Security Network(KSN) فضای ابری شرکت کسپرسکی است که در جهت سرعت بخشیدن به شناسایی ویروس های جدید به کار میرود. پیشنهاد ما فعال بودن این گزینه است.



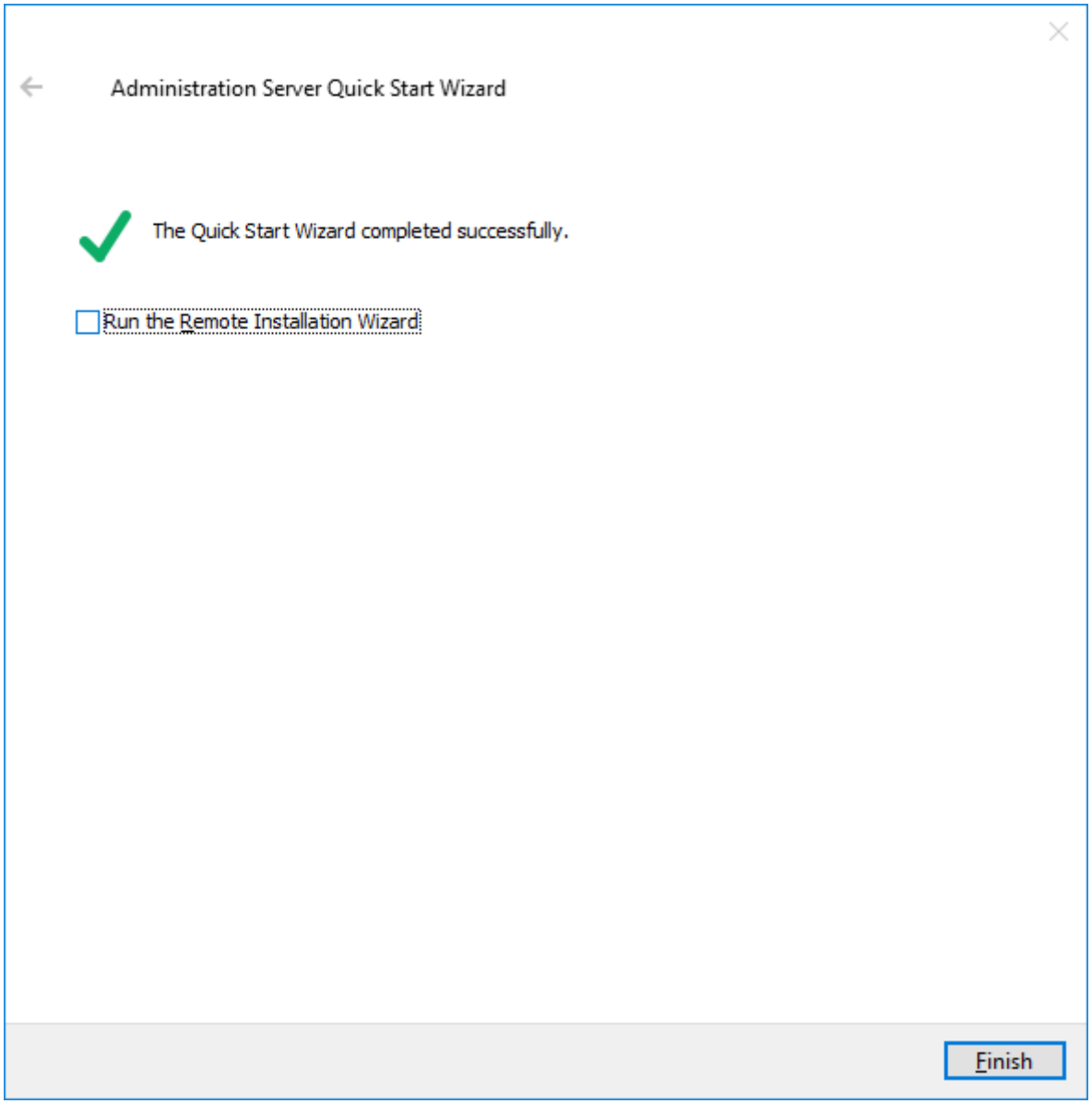
در صورتیکه تمایل داشته باشید Notification های مربوط به کنسول برای شما ایمیل شود، می توانید آدرس ایمیل دریافت کننده، آدرس SMTP Server و پورت مربوط به SMTP Server را در این پنجره وارد کنید تا از این پس پیغام ها برای شما ایمیل شود.



دراین مرحله سرور شروع به جستجو و اکتشاف کامپیوترهای موجود در شبکه می کند. منتظر بمانید تا این مرحله به اتمام برسد.

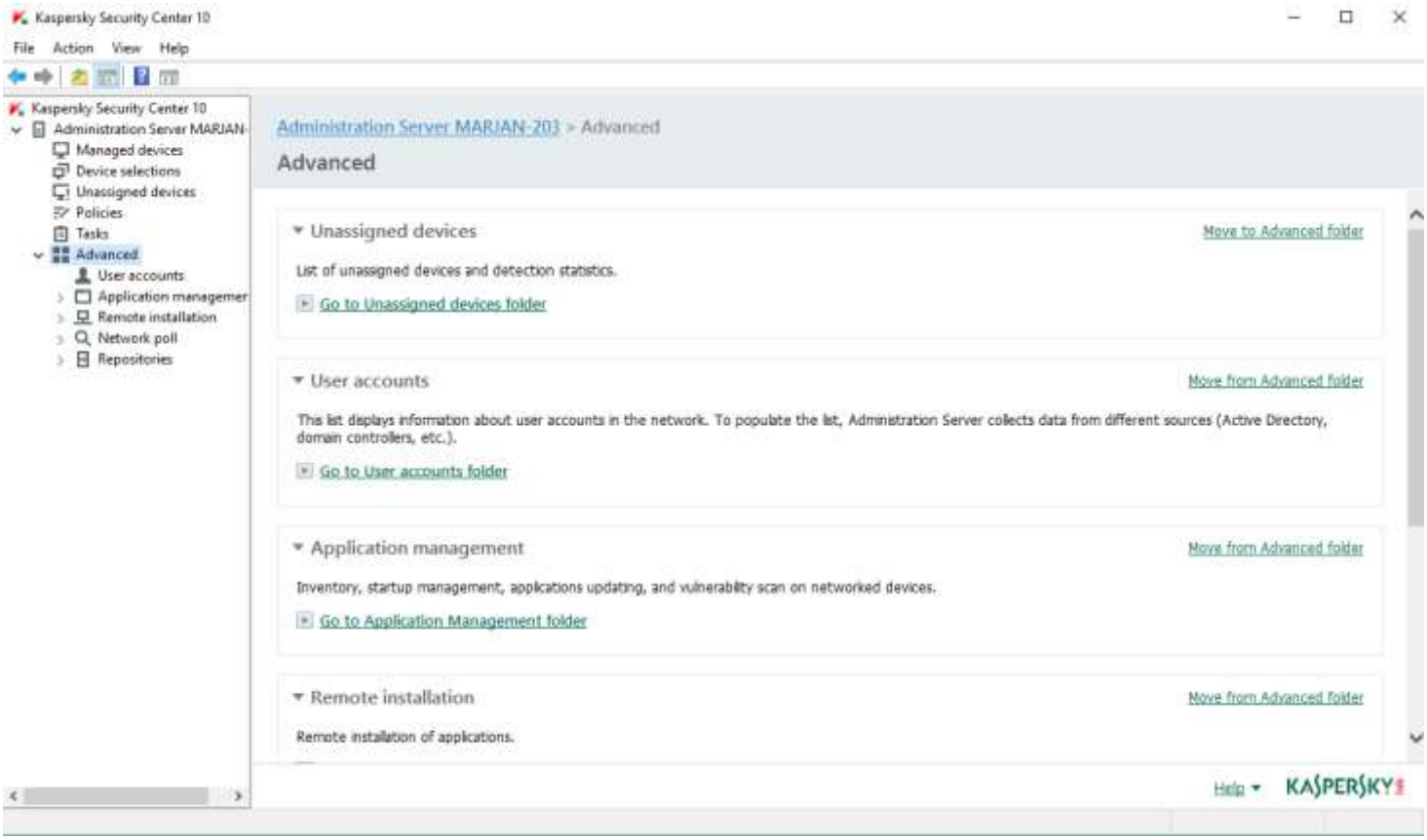


این مرحله، مرحله پایانی این ویزارد می باشد. در صورتیکه بخواهید محصولات Endpoint را روی کلاینت ها نصب کنید، تیک گزینه Run the remote installation wizard را می زنید. در غیر این صورت گزینه Finsh را انتخاب میکنید.



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 کامپوتر 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.

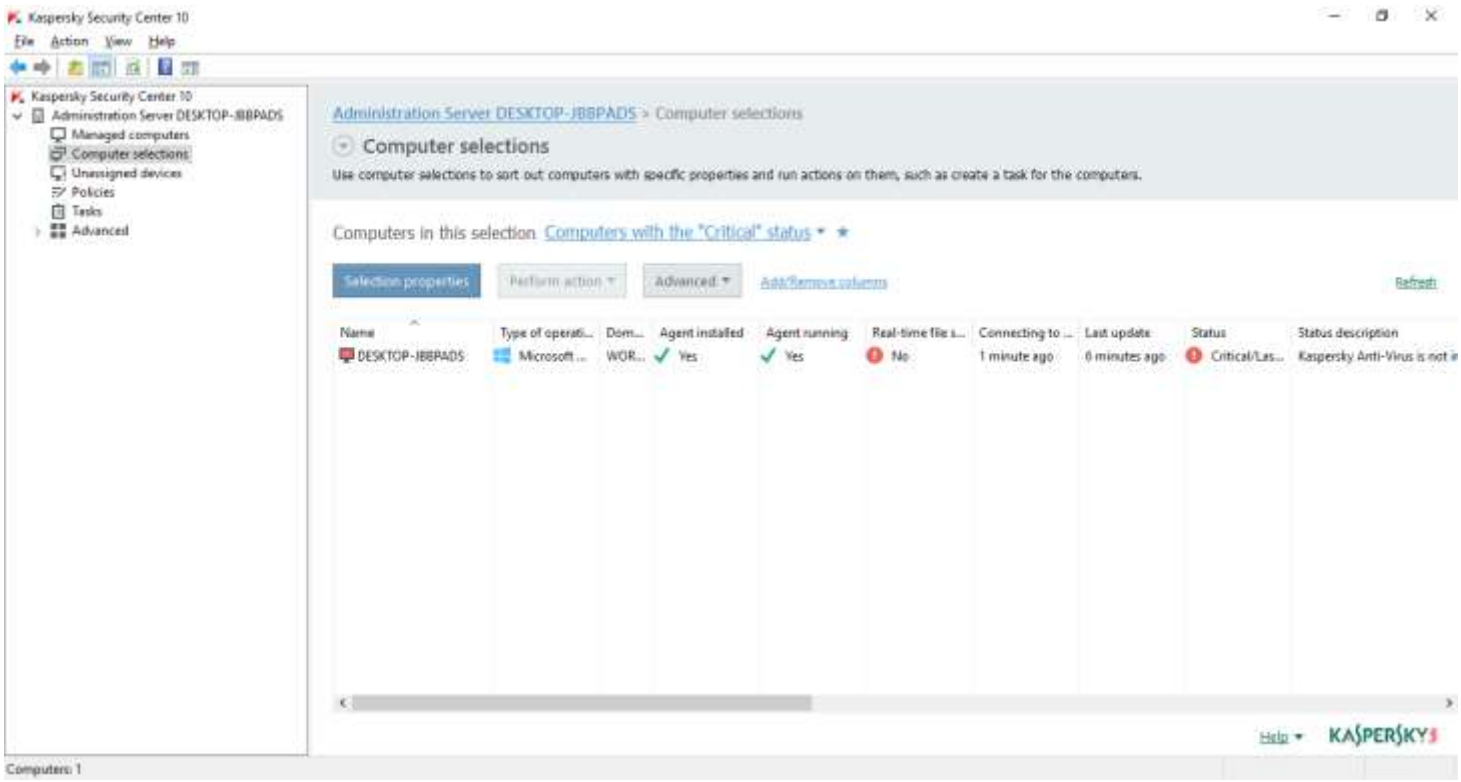
Tasks:

شامل Task های Update و Virus Scan و Find vulnerabilities است و جهت ایجاد Task برای Server ها و Client هااز این تب استفاده می کنیم. در این قسمت Task های مربوط به Security Center نیز قرار می گیرندکه 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.

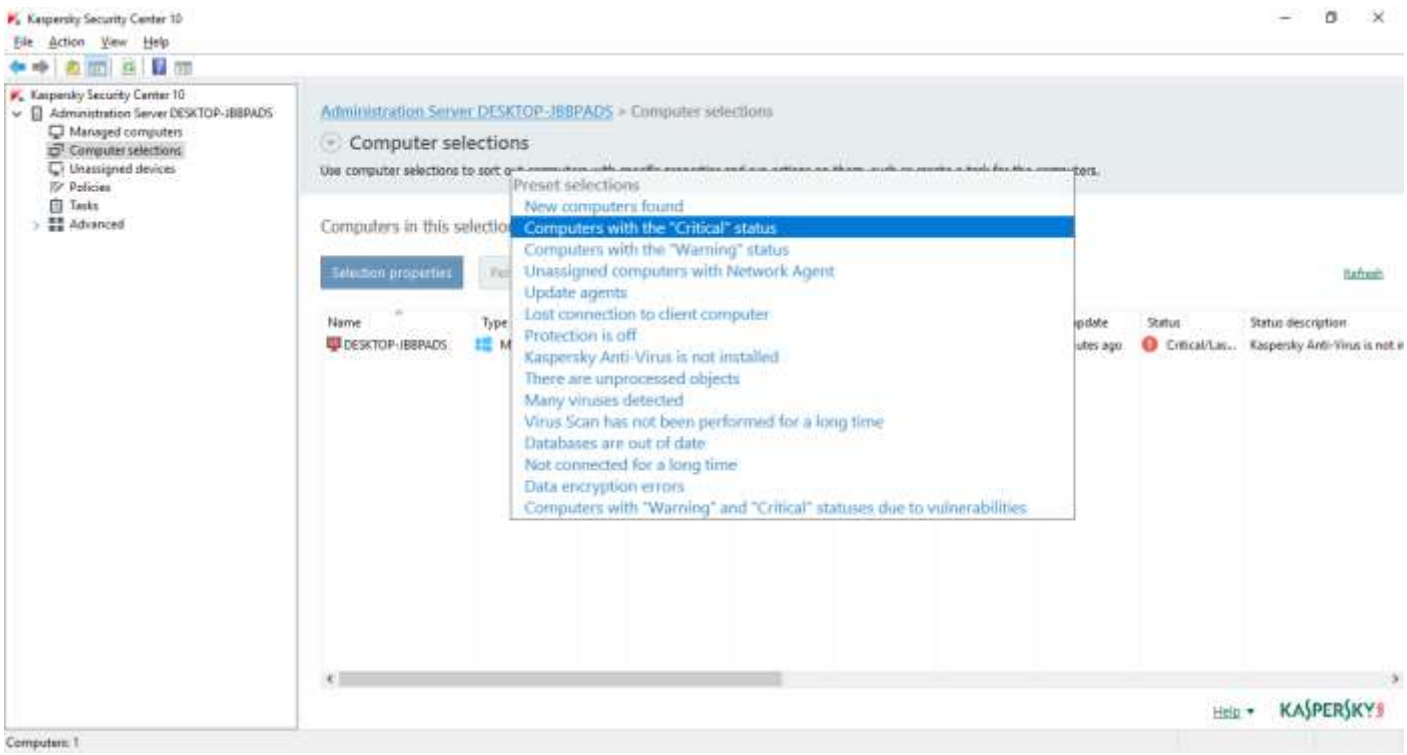
در این قسمت باید در داخل تسک Download updates to the repository در بخش Settings و سپس در بخش Update Source سورس آپدیت سرور کسپرسکی شعب و سرپرستی را بر روی گزینه Master Server قرار دهید.

Computer Selection:

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

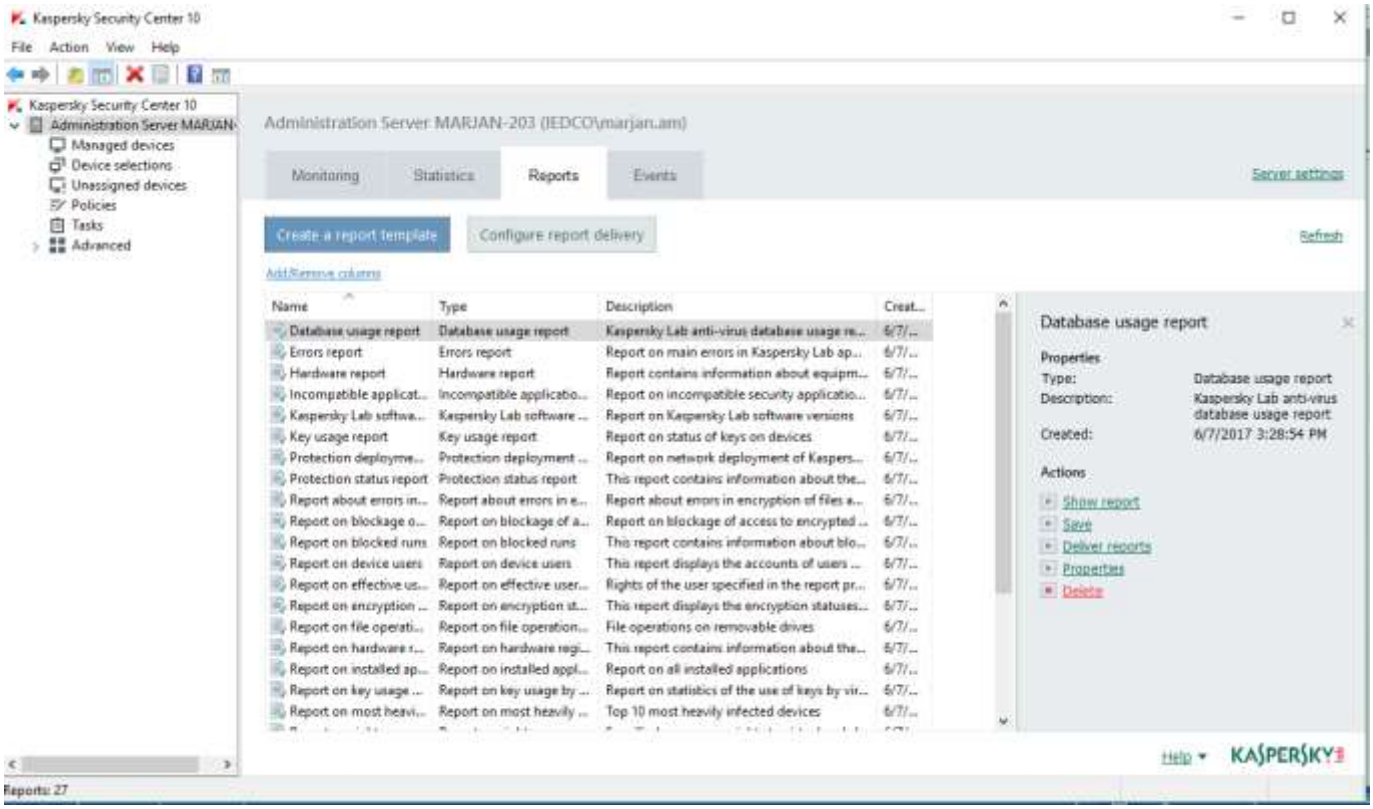


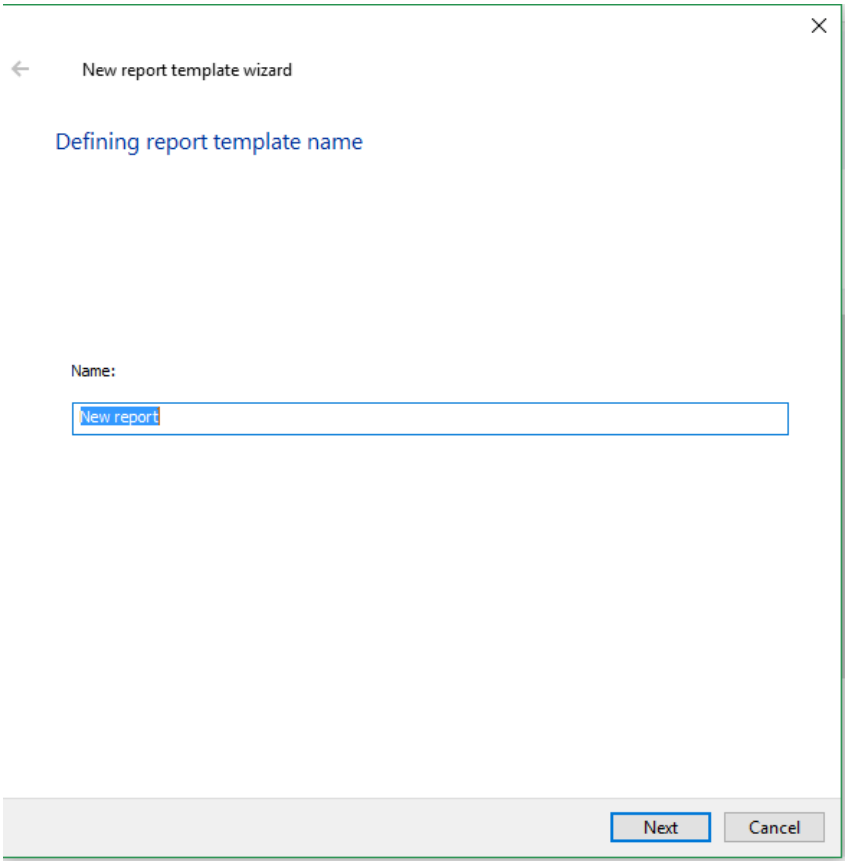
به طور مثال میتوانید سیستم هایی که آپدیت نشده اند را با کلیک بر روی گزینه Database are out of date در سراسر شبکه مشاهده نمایید. به تصویر زیر نگاه نمایید.

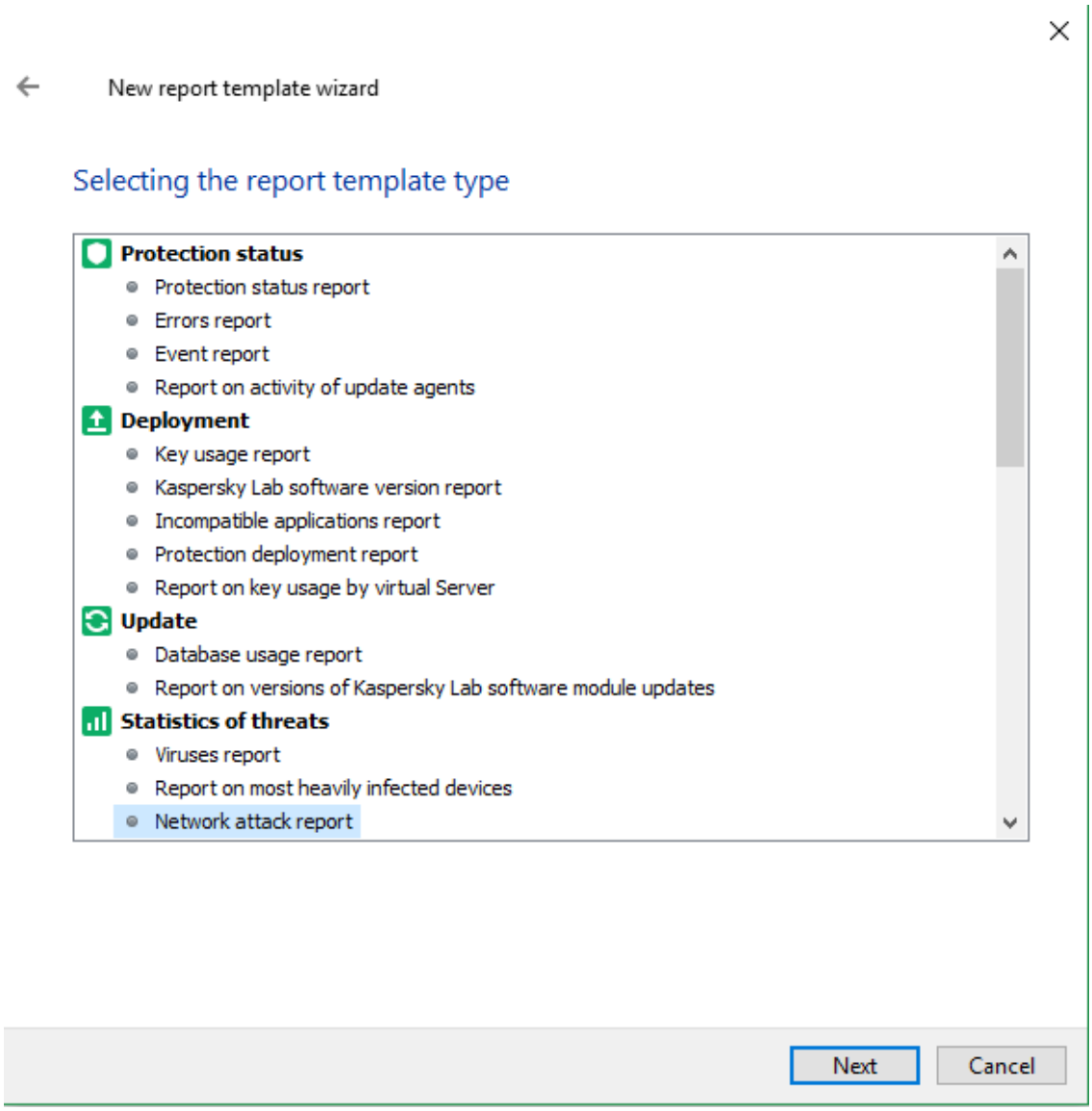


نحوه ایجاد گزارش در کنسول Kaspersky :

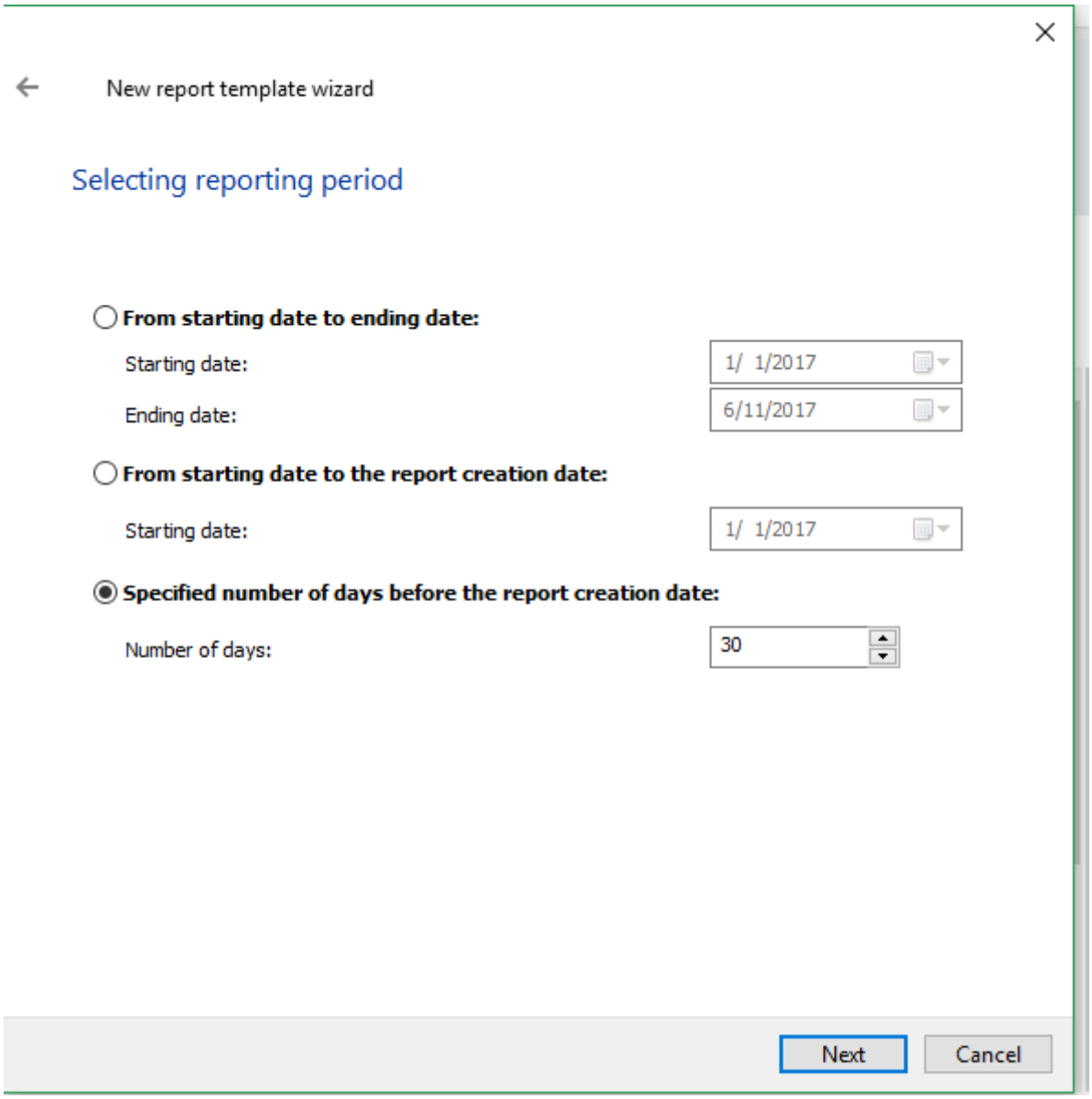
برای اینکار بر روی Administration Server کلیک نمایید ودر تب Report گزینه Create a report template را انتخاب نمایید و بعد از تعیین نام نوع گزارش را انتخاب نمایید.



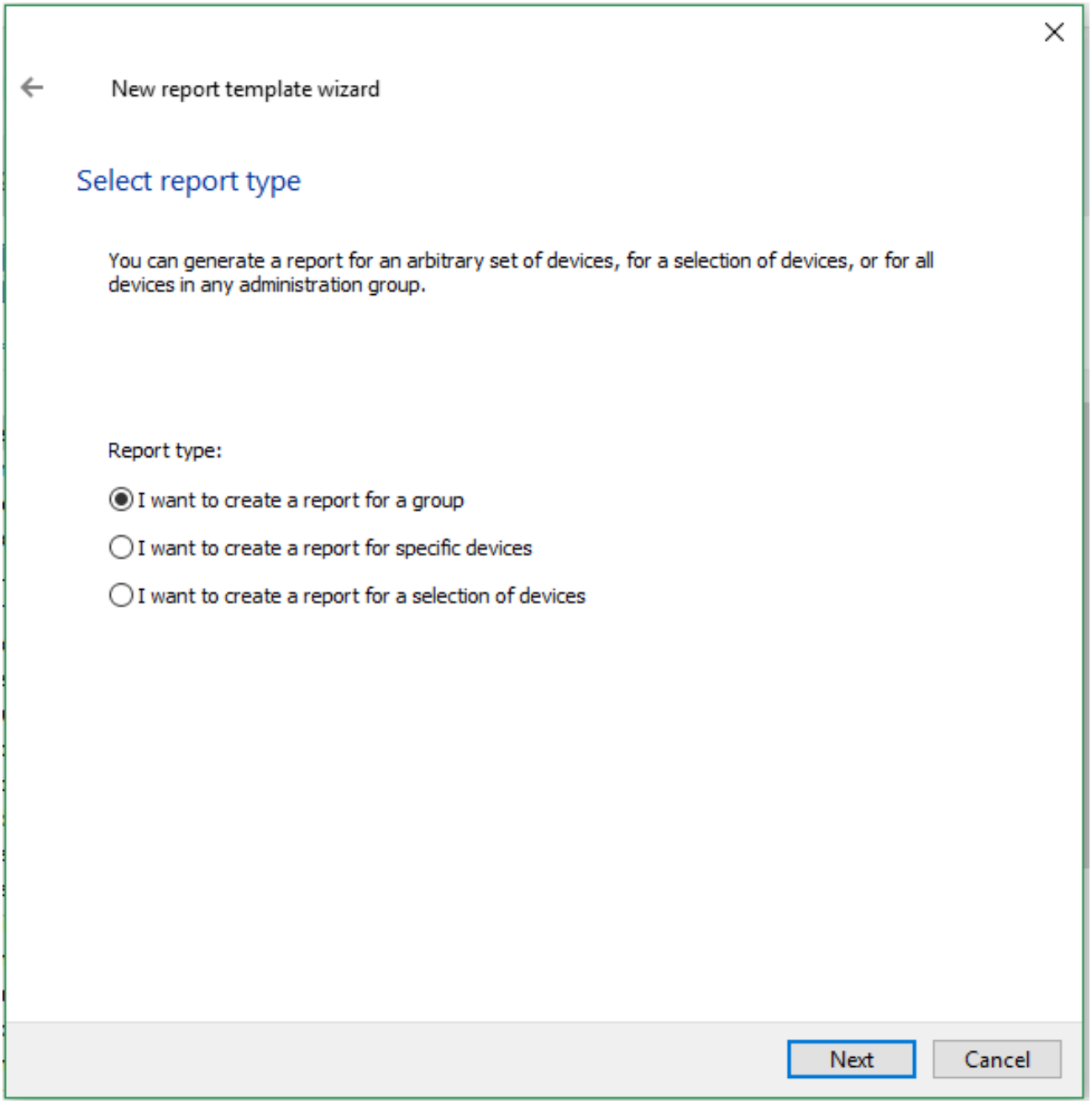

New report template wizard
Defining report template name
Name:
New report
Next
Cancel

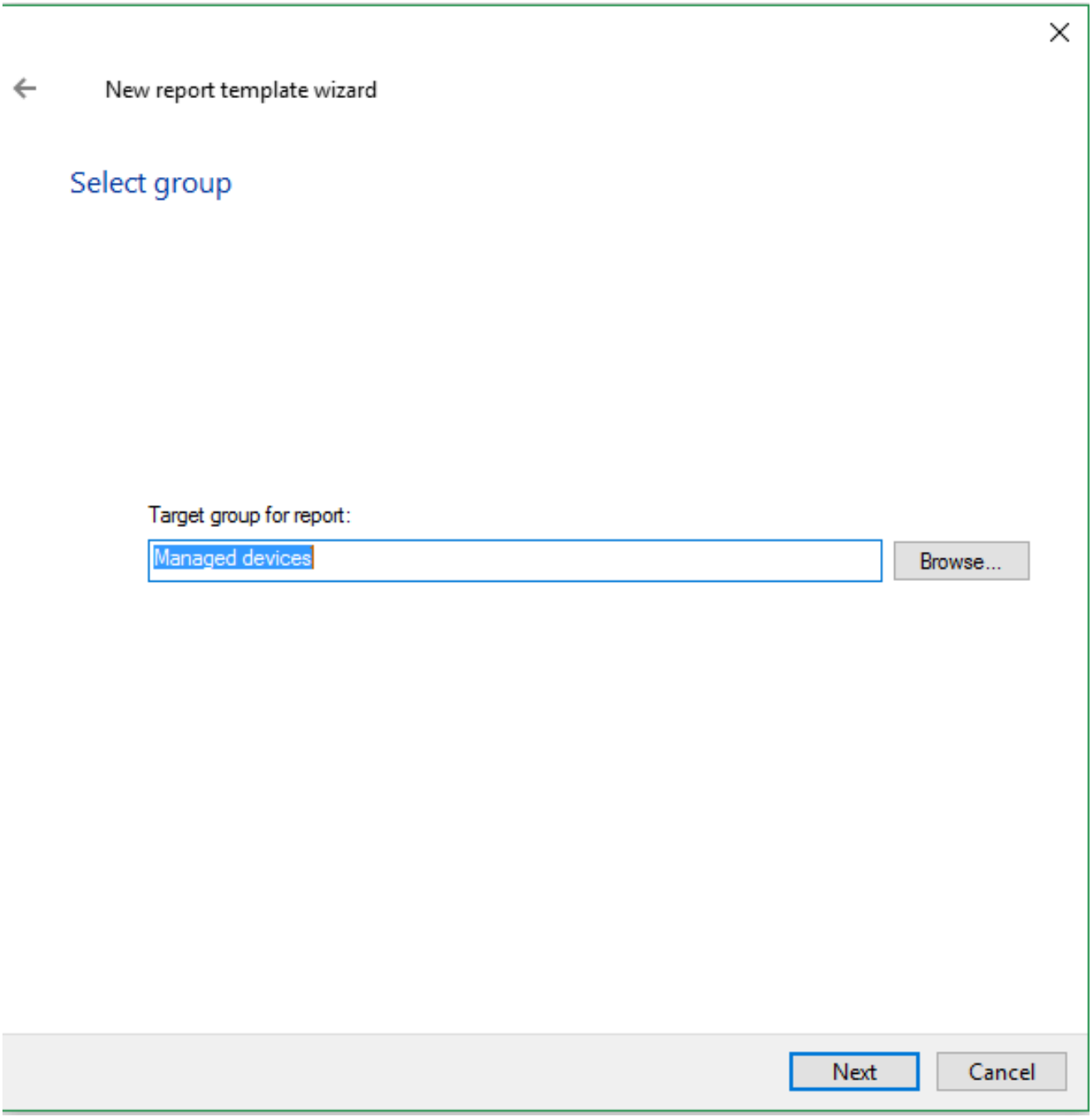

New report template wizard
Selecting the report template type
Protection status
Protection status report
Errors report
Event report
Report on activity of update agents
Deployment
Key usage report
Kaspersky Lab software version report
Incompatible applications report
Protection deployment report
Report 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

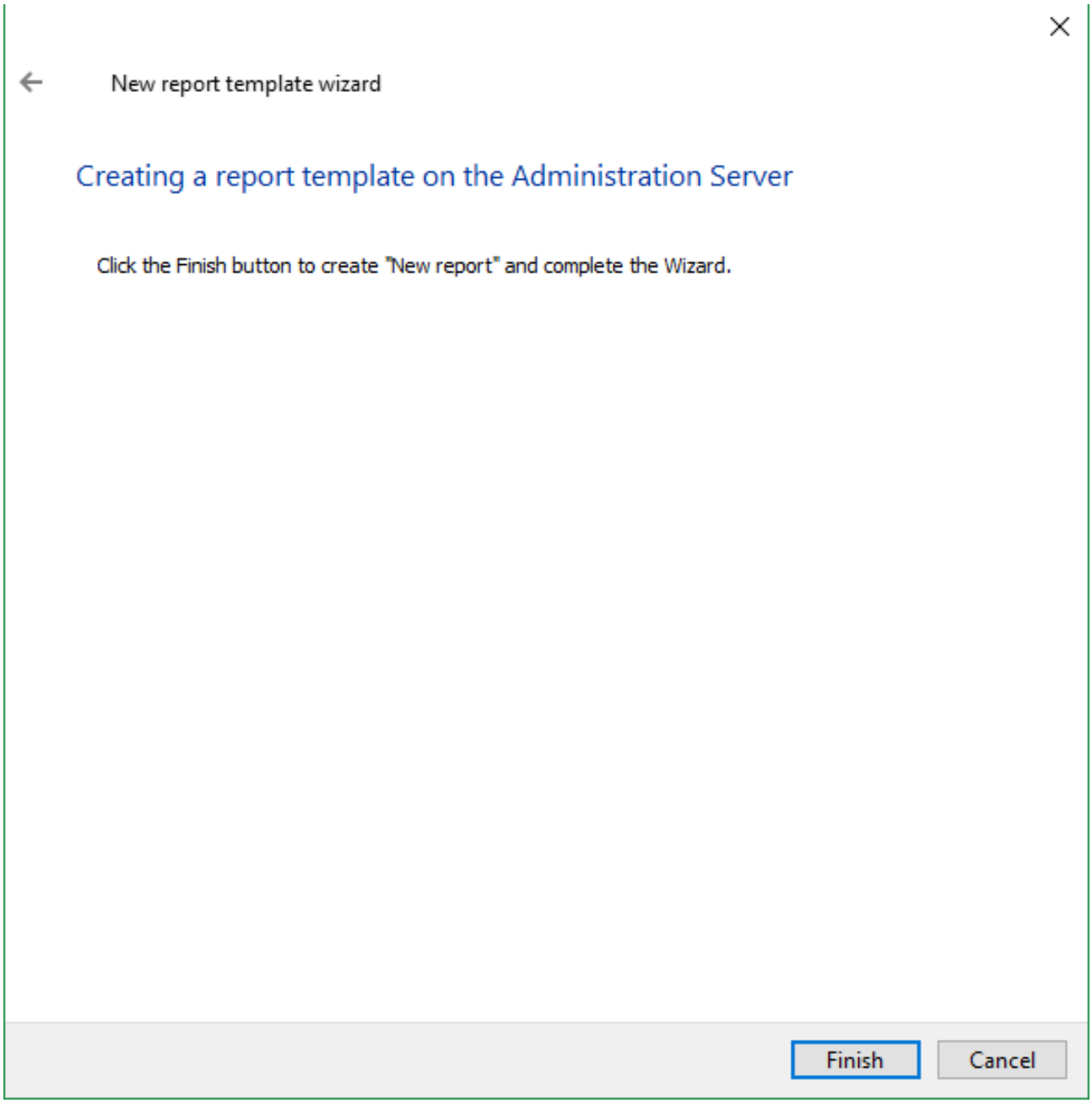
در این مرحله می توانید یک محدوده ی زمانی برای گرفتن گزارش تهیه نمایید، به عنوان مثال ۳۰ روز گذشته.



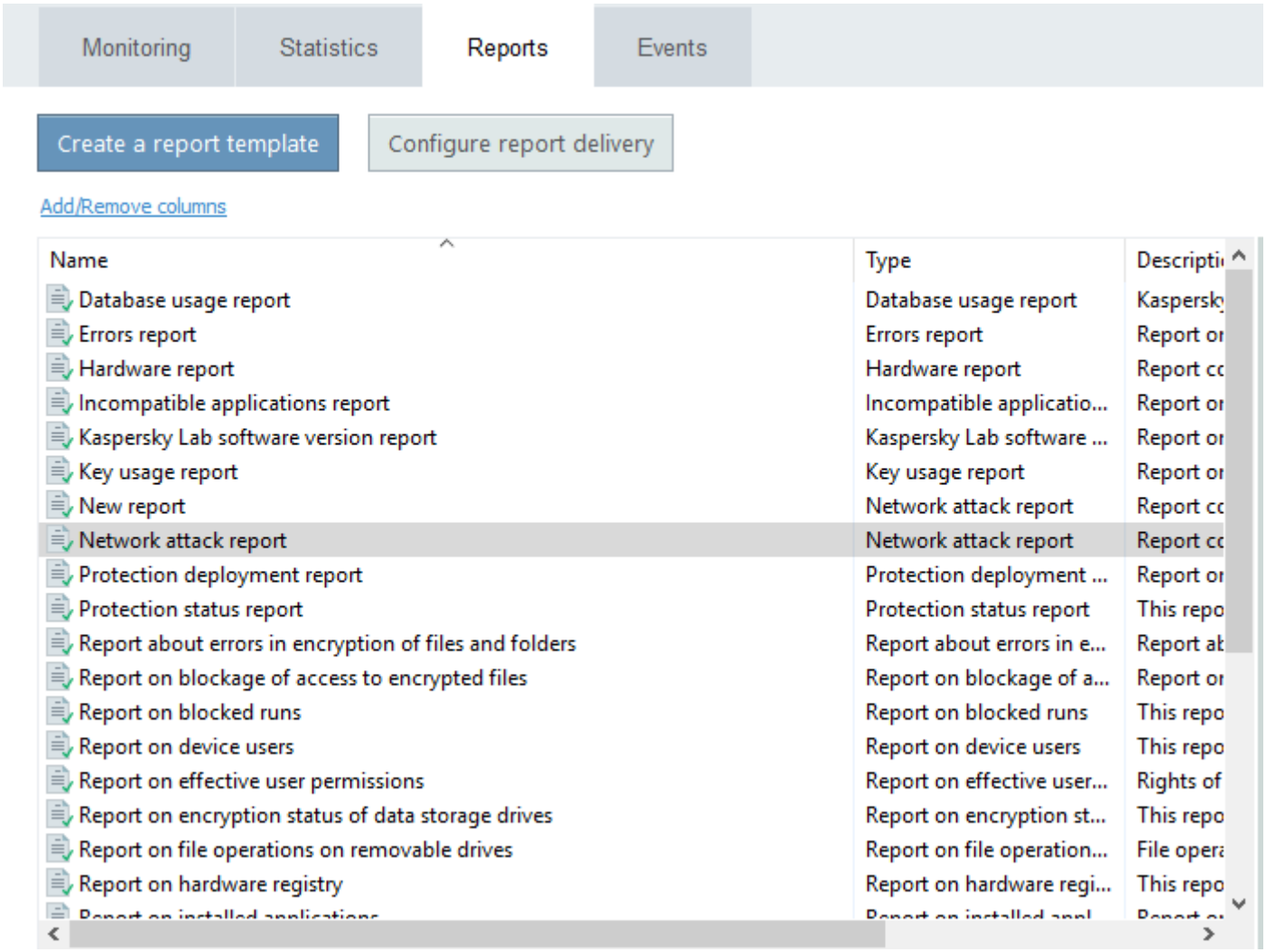
در این پنجره می توانید این گزارش را برای گروه خاصی از سیستم ها ایجاد کنید.




New report template wizard
Select group
Target group for report:
Managed devices
Browse...
Next
Cancel


New report template wizard
Creating a report template on the Administration Server
Click the Finish button to create "New report" and complete the Wizard.
Finish
Cancel

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



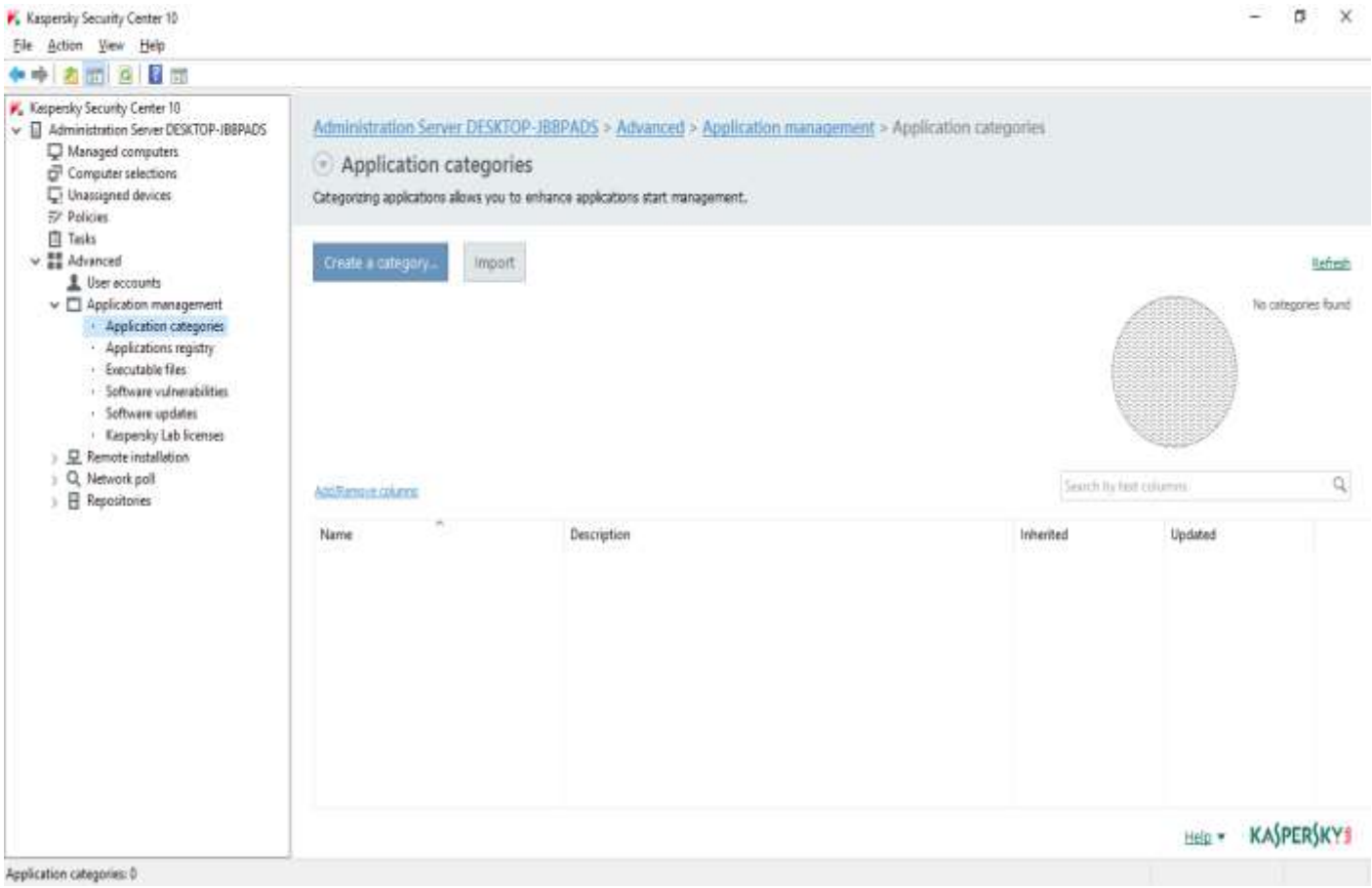
Advanced:

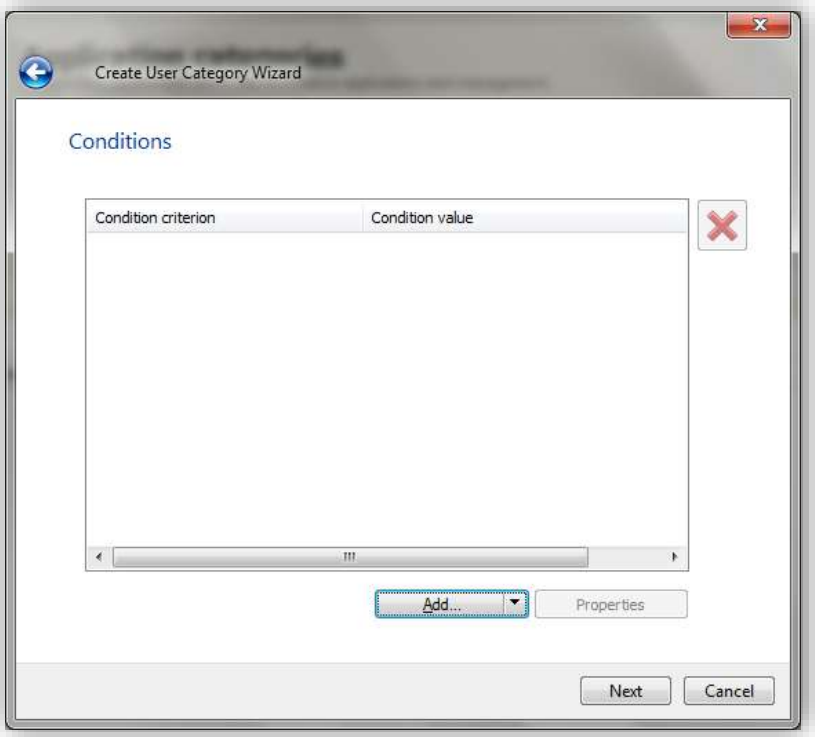
این بخش شامل چندین قسمت است. مانند، ساختن category، مشاهد ه برنامه های نصب شده، فایل های اجرایی داخل شبکه و لایسنس ها و آپدیت سیستم عامل ها است.

Application categories:

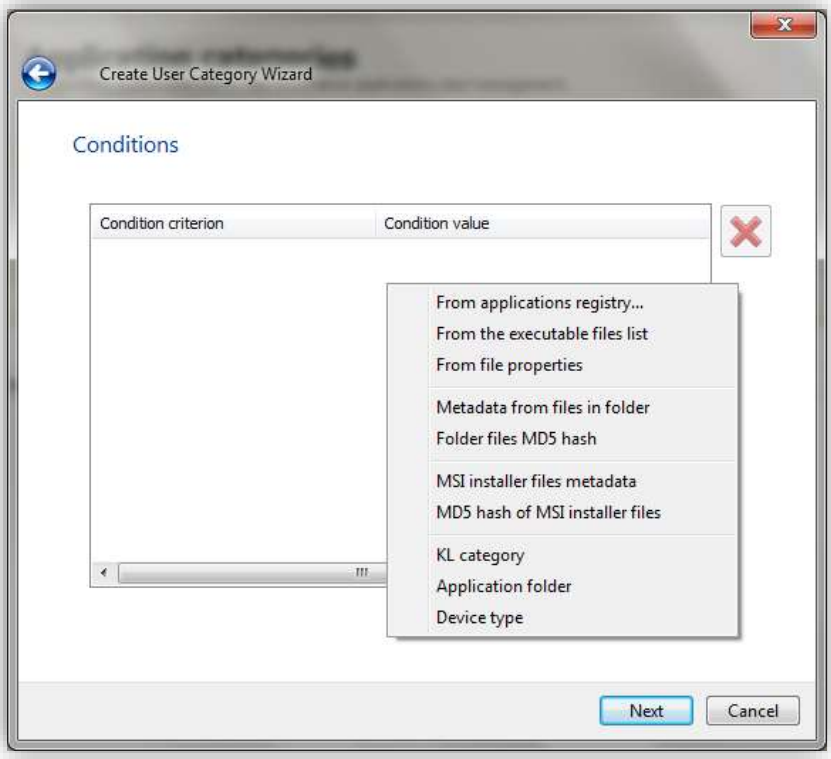
در این بخش شما می توانید دسته بندی های مختلفی بر روی application های نصب شده روی سیستم های داخل شبکه انجام دهید، این قابلیت ها شامل دسترسی یا عدم دسترسی تعدادی از application به کاربران می باشد. در قسمت Policy در بخش Start of application control می توانید از این Category ها استفاده کنید. به صورت پیش 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.

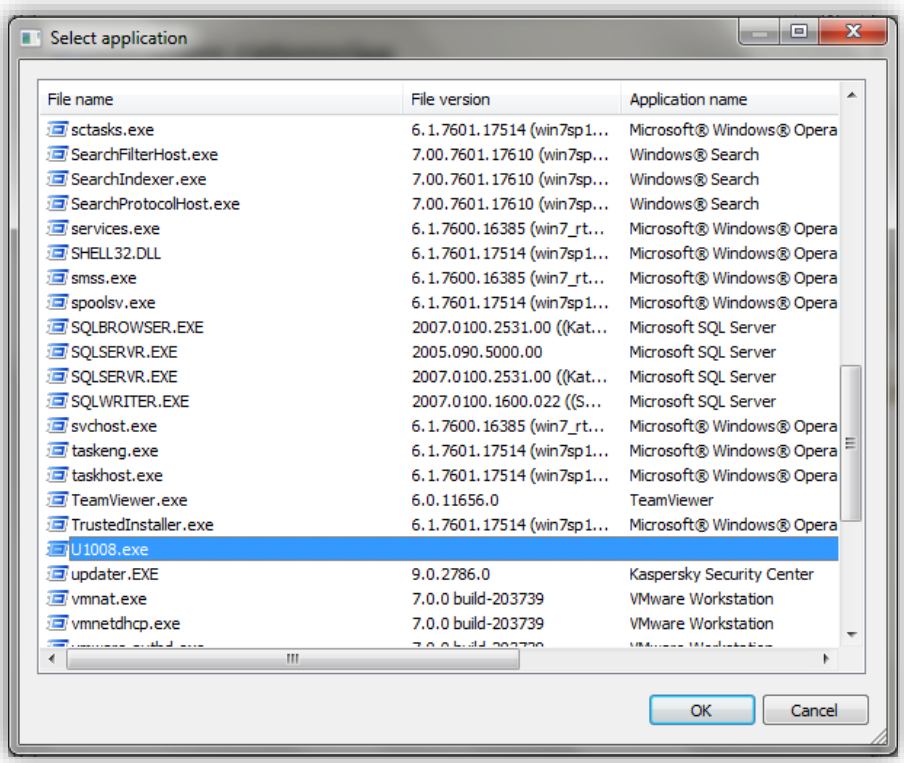


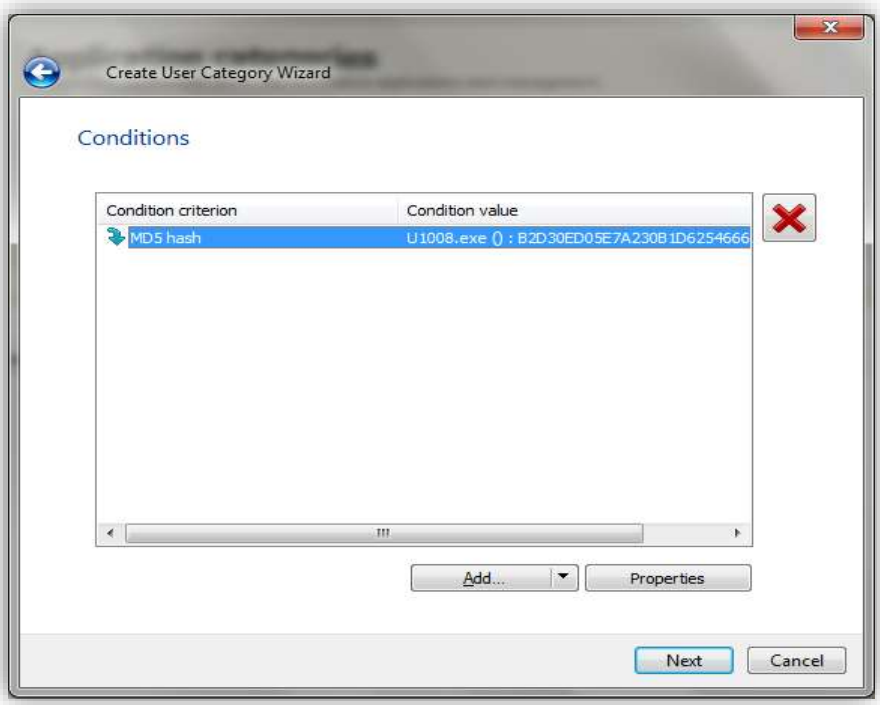


جهت اضافه کردن Application مورد نظر بر روی دکمه Add کلیک نمایید، لیست باز شونده کنار دکمه ی Add این امکان را به شما می دهد تا شیوه ی اضافه کردن application ها در category مورد نظر را انتخاب کنید.در این مثال بر روی لیست باز شونده کلیک می کنیم و روشانتخاب را بر اساس From the executable files list تنظیم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

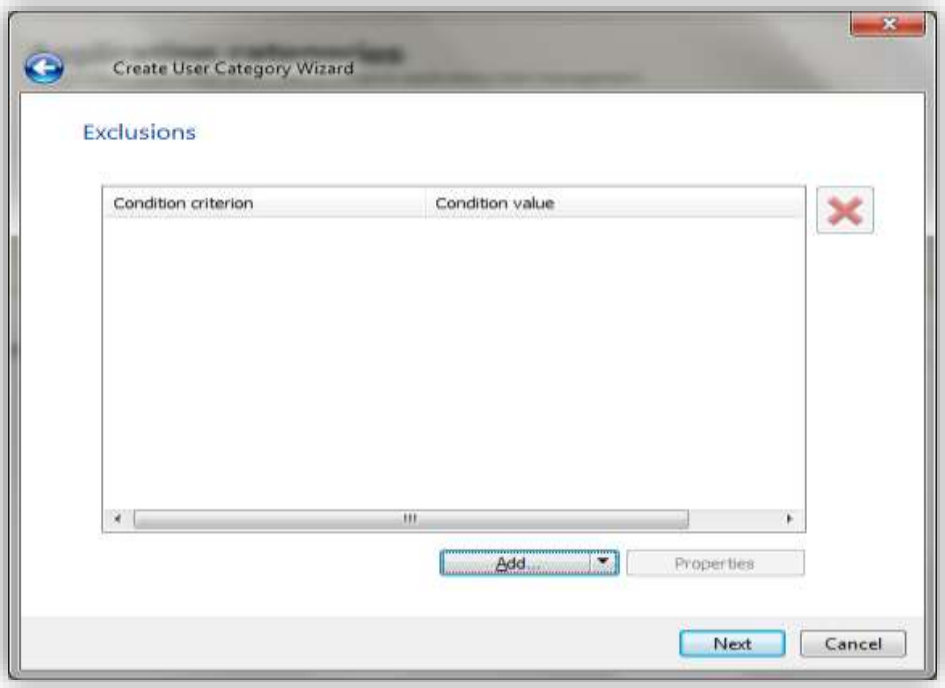


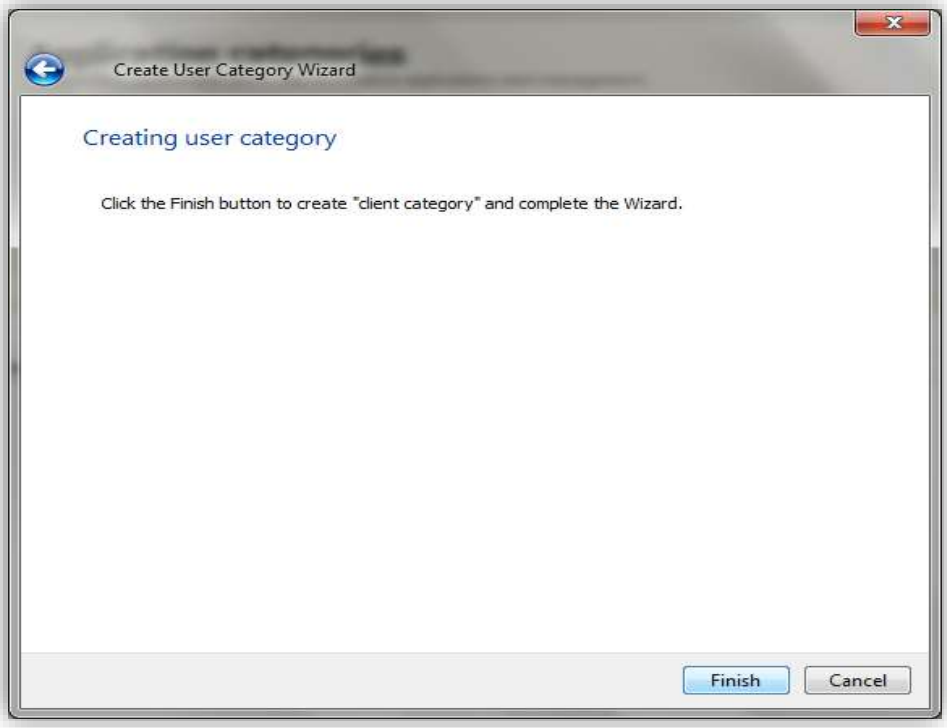
پس از انتخاب این گزینه لیستی از فایل های اجرایی موجود بر روی سیستم های داخل شبکه نمایش می یابد. برای مثال در این پنجره فایل اجرایی فیلتر شکن U۱۰۰۸.exe را انتخاب می کنیم.





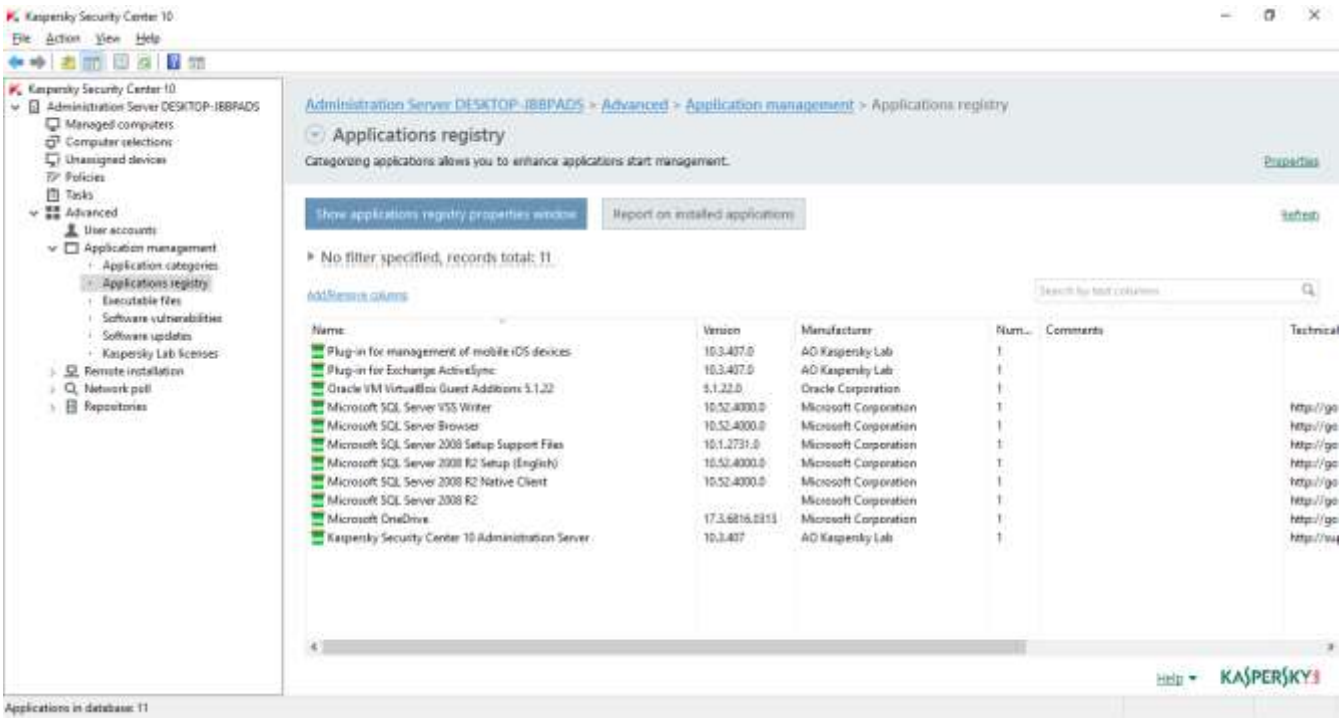
با کلیک بر روی دکمه Add می توانید Application مورد نظر خود را از این لیست مستثنی کنید.





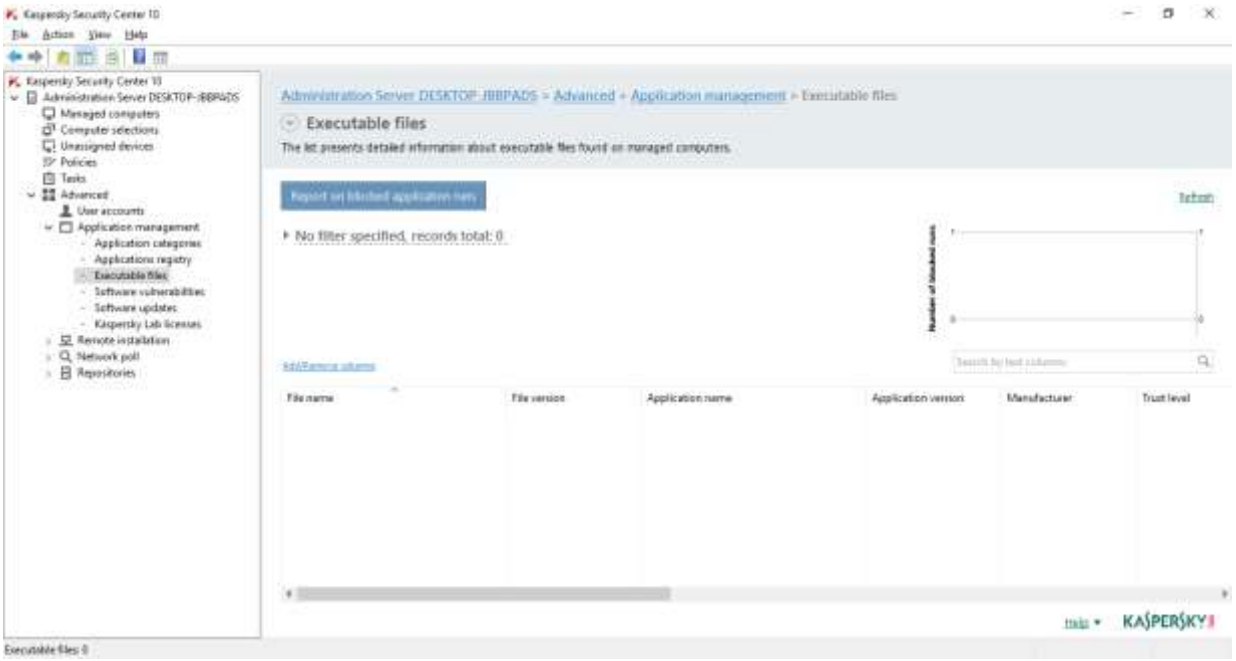
Application registry:

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.



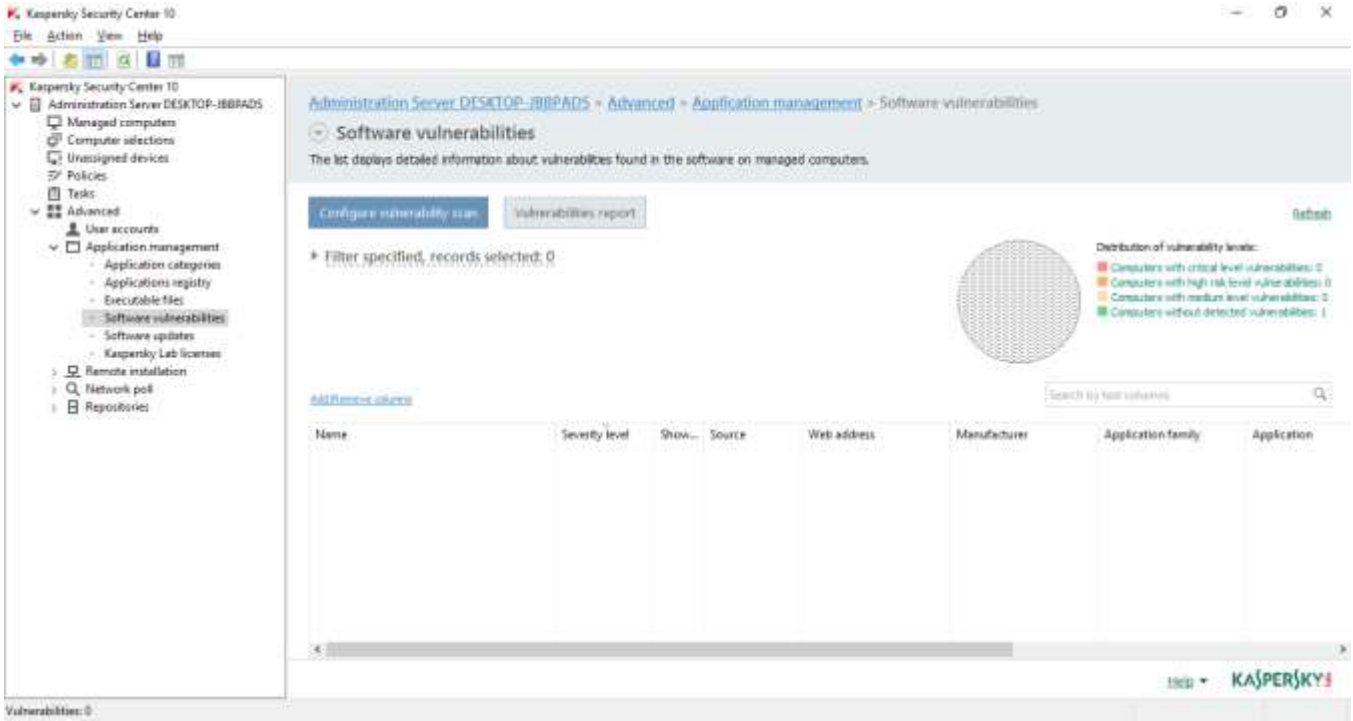
Executable Files:

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



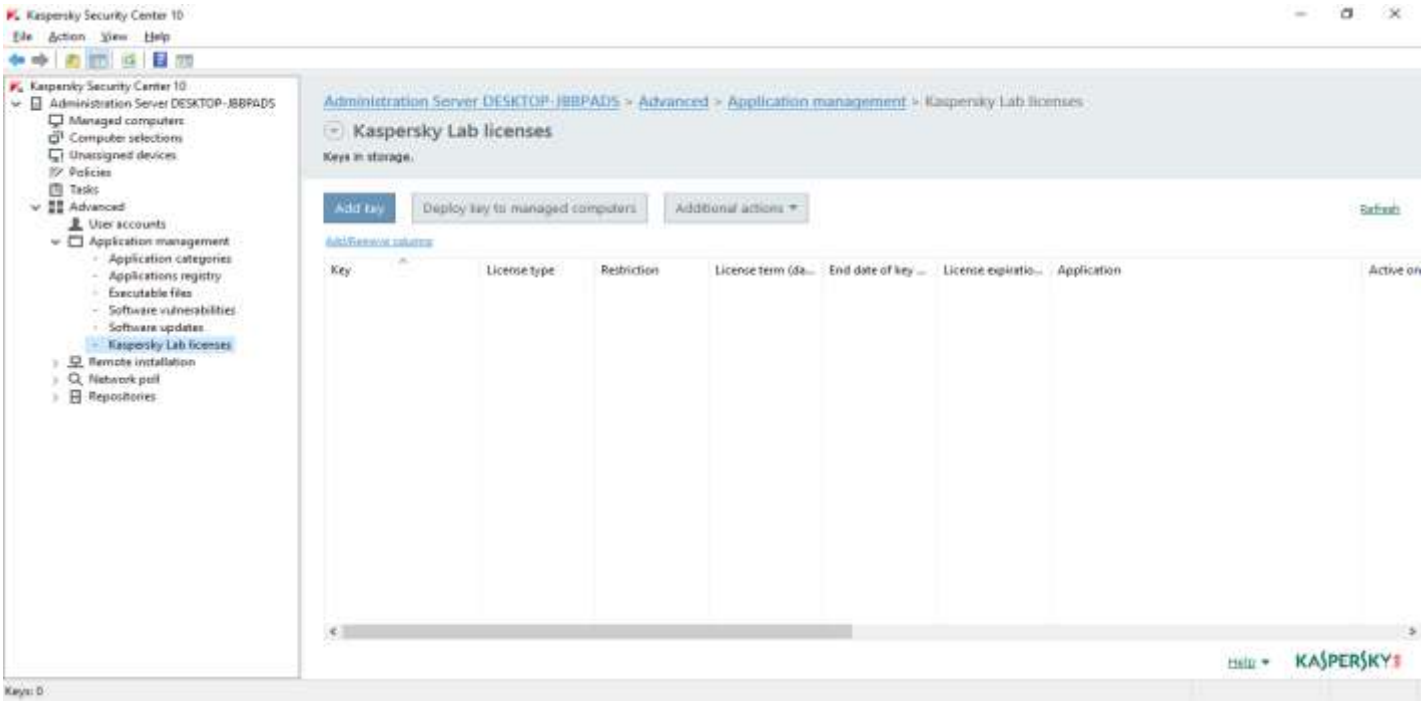
Software vulnerabilities:

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

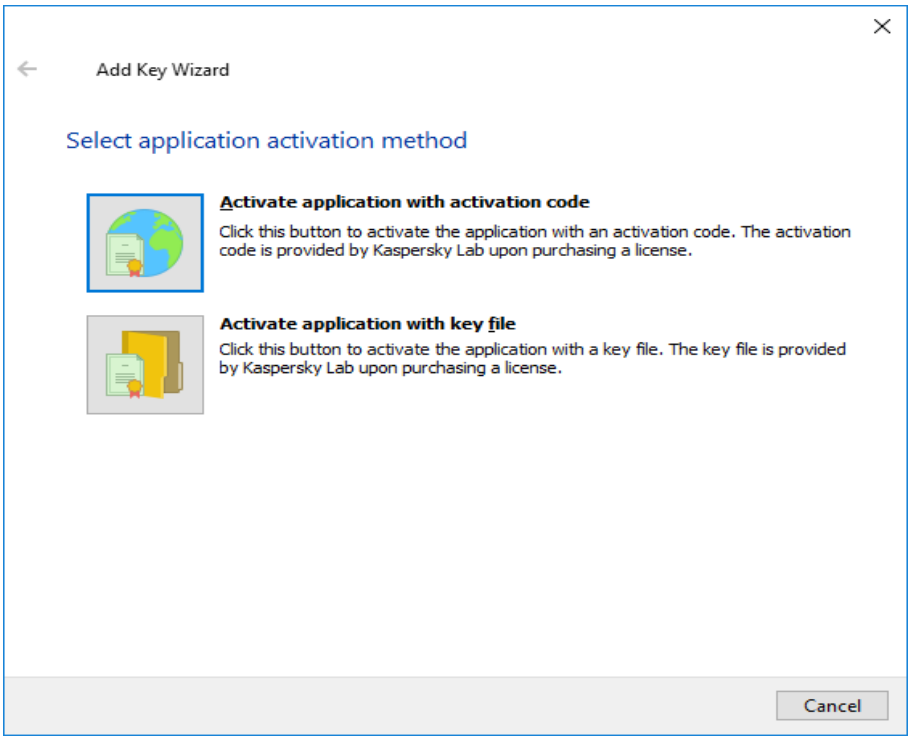


Kaspersky Lab licenses:

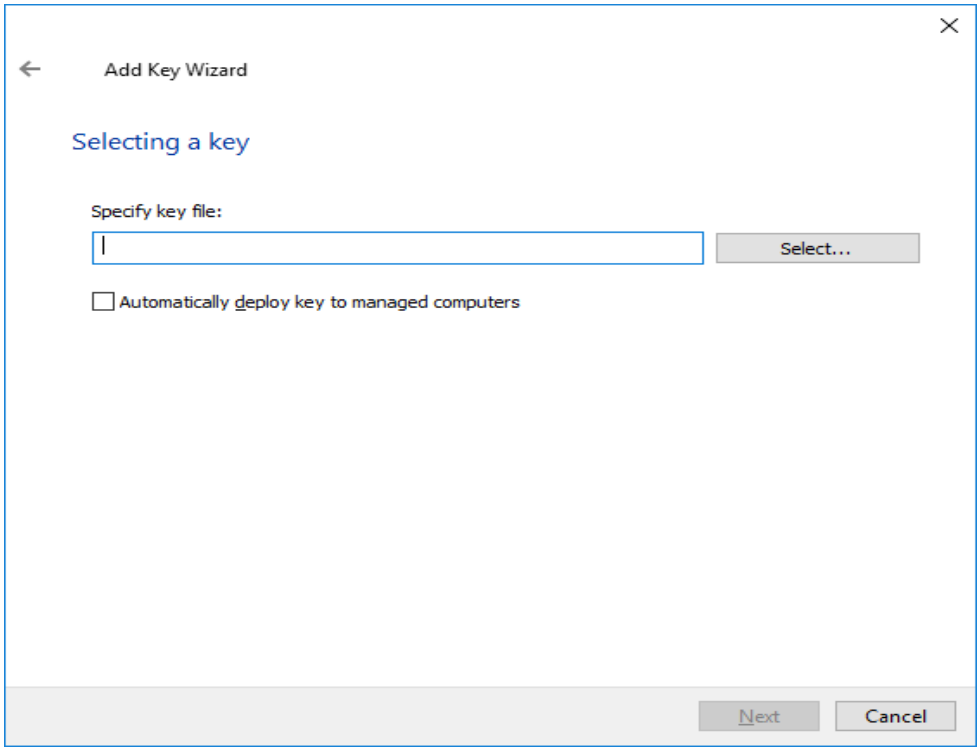
در این قسمت میتوانید لایسنس های کسپرسکی خود را اضافه نمایید تا بعد از نصب آنتی ویروس ها بر روی سیستم های دیگر، لایسنس به صورت اتوماتیک بر روی آن ها قرار گیرد.

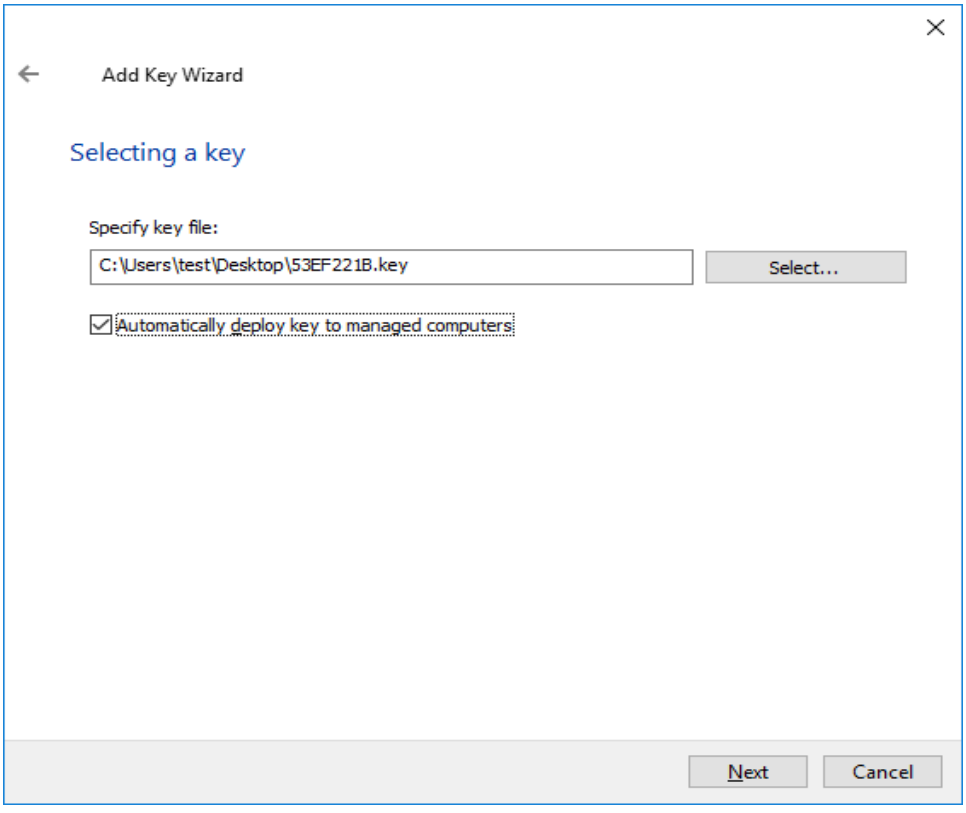


برای اضافه کردن لایسنس ها ابتدا بر روی گزینه Add key کلیک نماییدو پس از باز شدن صفحه زیر، بر روی گزینه Activate application with key file کلیک نمایید.



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.

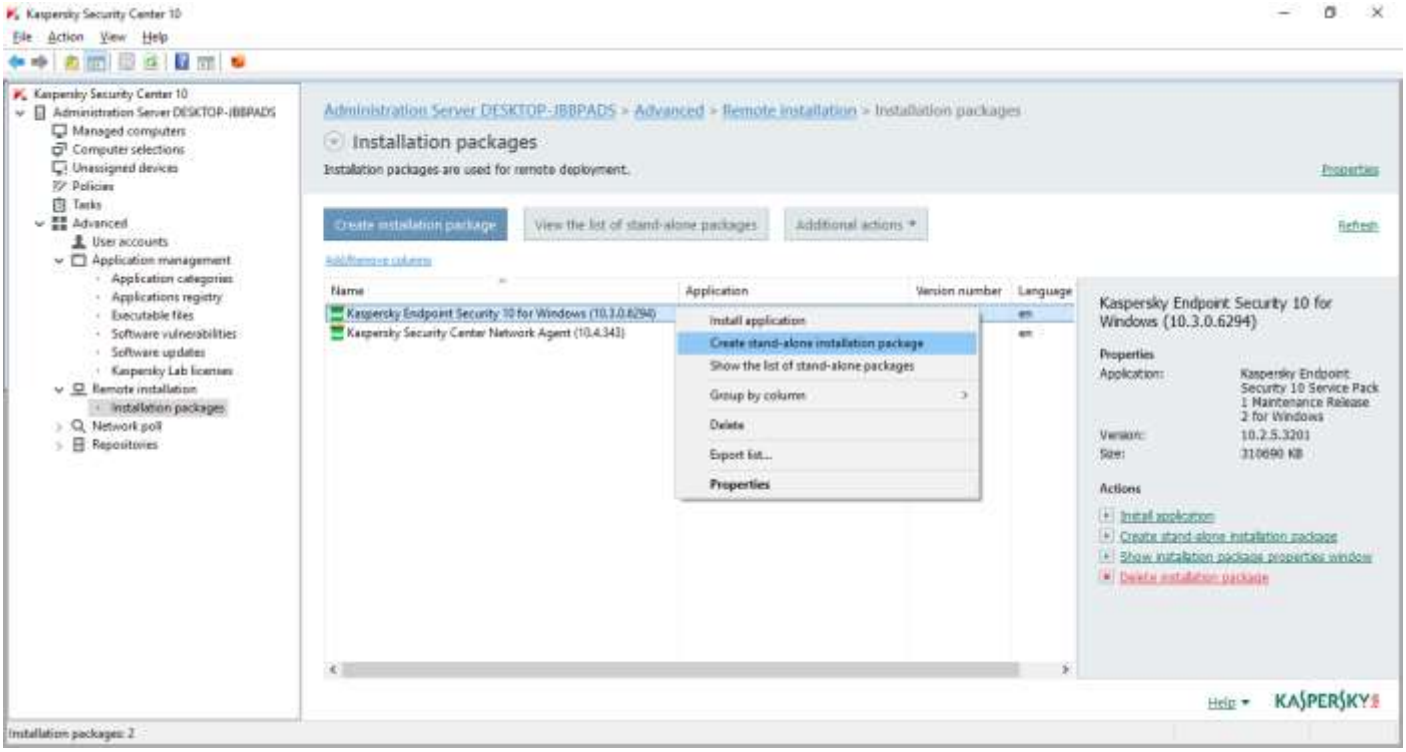




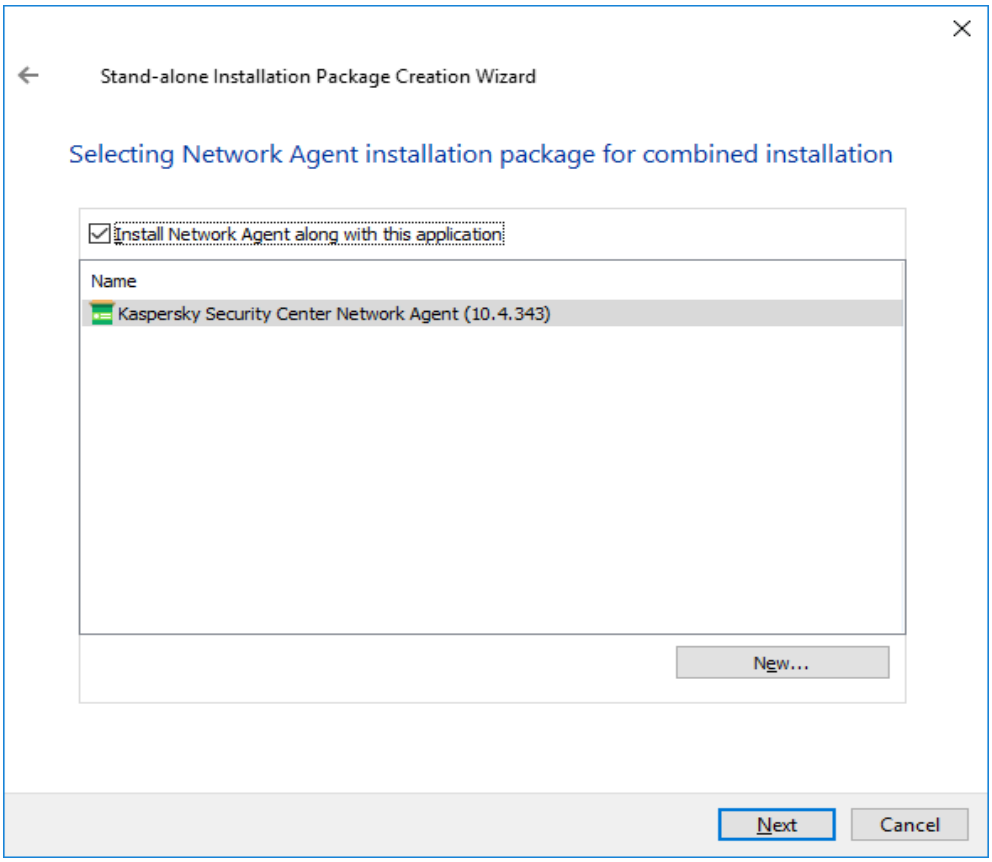
Remote installation:

- **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 افزارهای کسپرسکی با نصب کنسول Security center به صورت پیش فرض ساخته می شود و نیازی به ساختن دوباره آن ها نمی باشد.

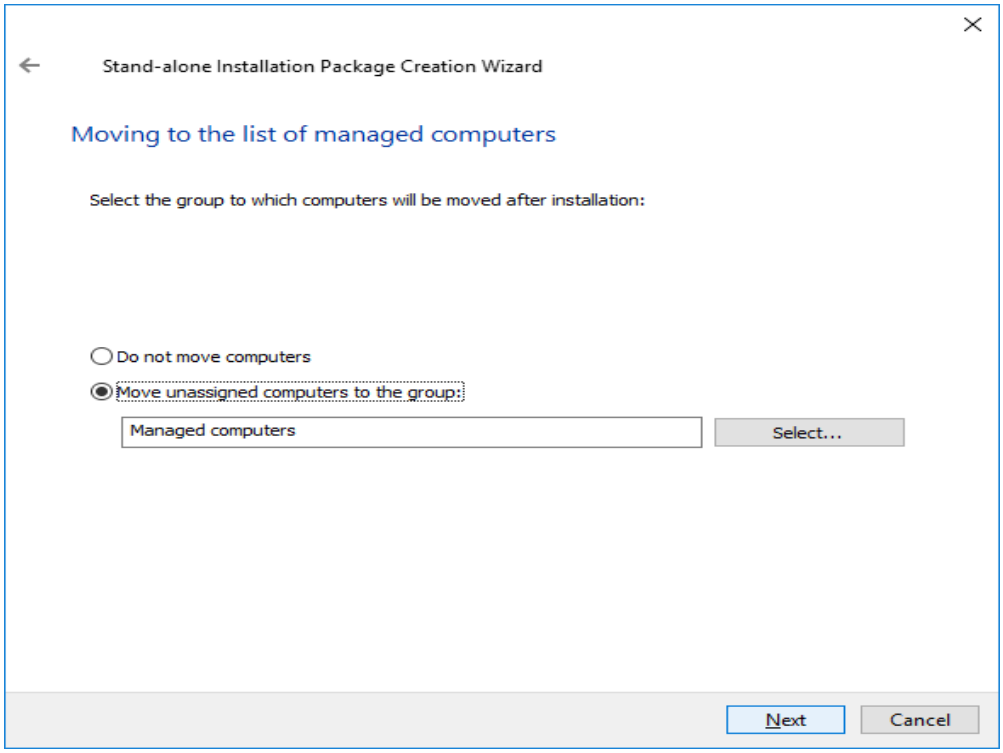
برای نصب بروی کلاینت ها ابتدا باید از پکیج آنتی ویروس موجود در این قسمت یک پکیج نصب به نام Stand-alone بسازید. ابتدا مطابق تصویر زیر بر روی پکیج Kaspersky Endpoint Security راست کلیک کنید و بر روی گزینه Create stand-alone installation package کلیک نمایید.



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

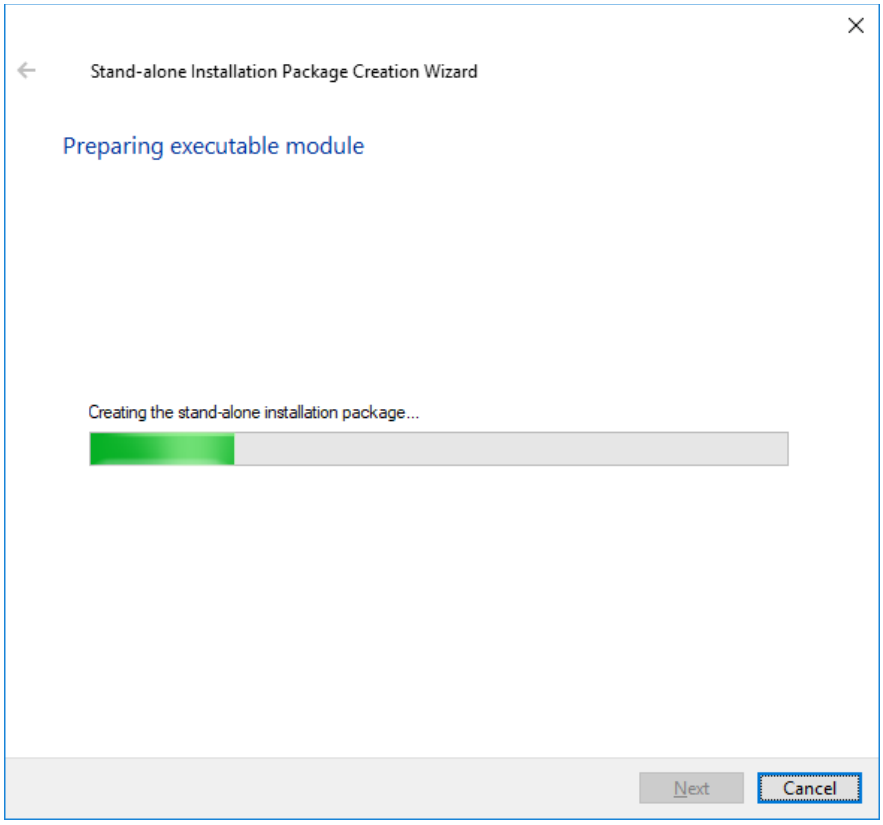


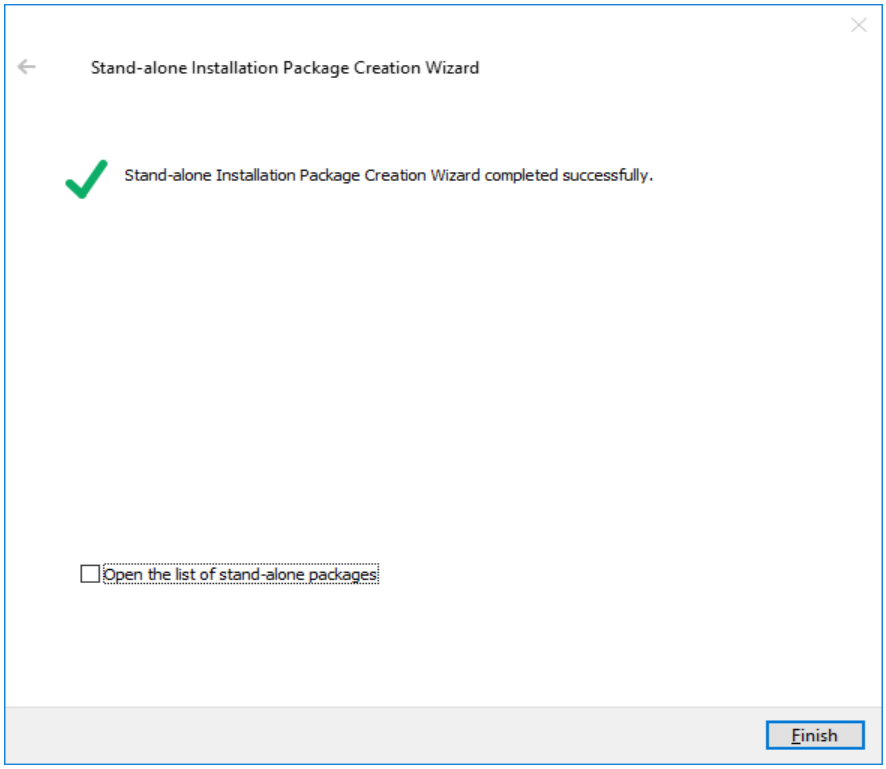
در مرحله بعدی تغییری ندهید و به مرحله بعد بروید.



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

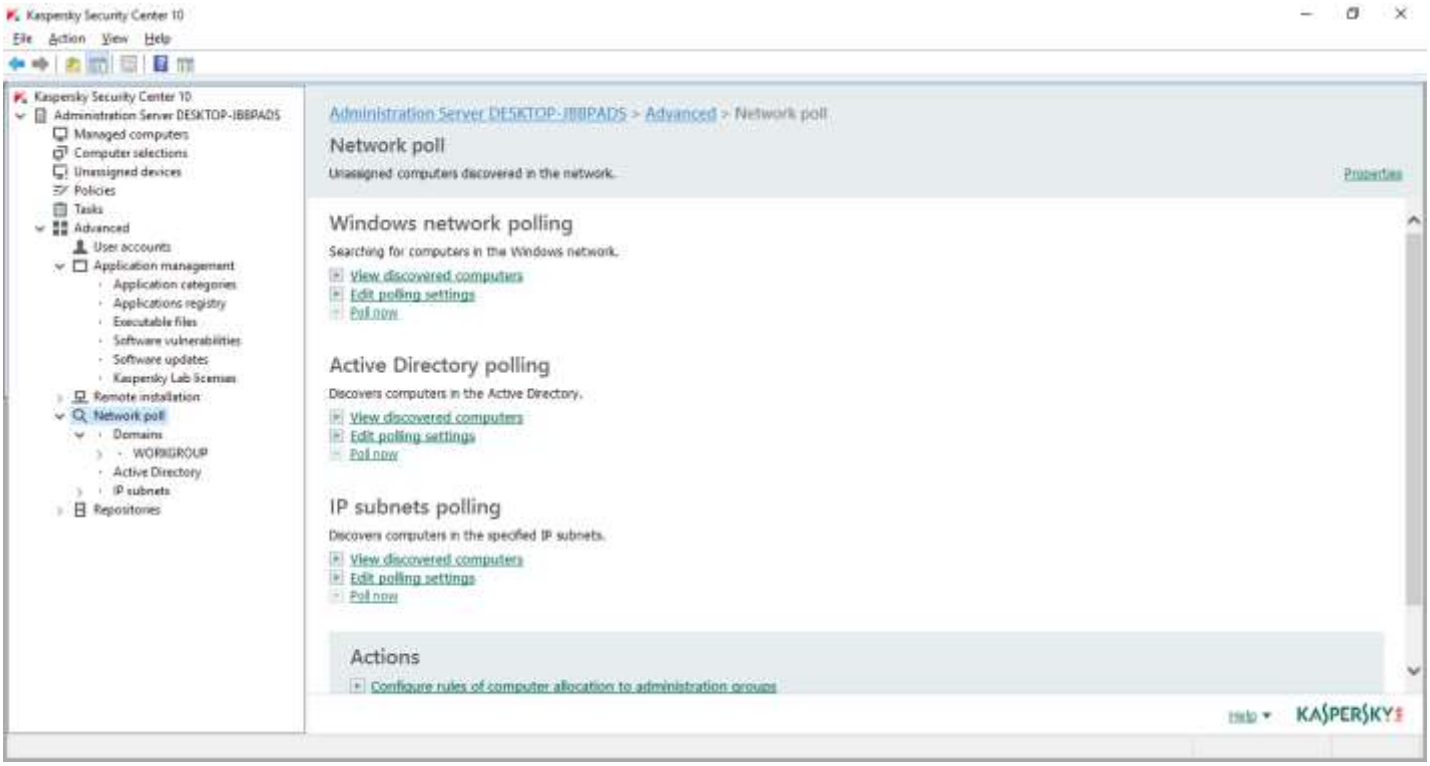
\\Kaspersky server IP\KLshare\pkginst\





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 ماژول های آپدیت و آخرین تاریخ به روز رسانی این اجزا (تاریخ Createشدن و receive شدن فایل های به روز رسانی) می باشد
- **Quarantine**: در صورتیکه آنتی ویروس برنامه ای را مشکوک به ویروس ببیندآن 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

Policyها به طور عموم در جهت تنظیمات کاربردی و حفاظتی بروی سیستم های شما استفاده می‌شود

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.

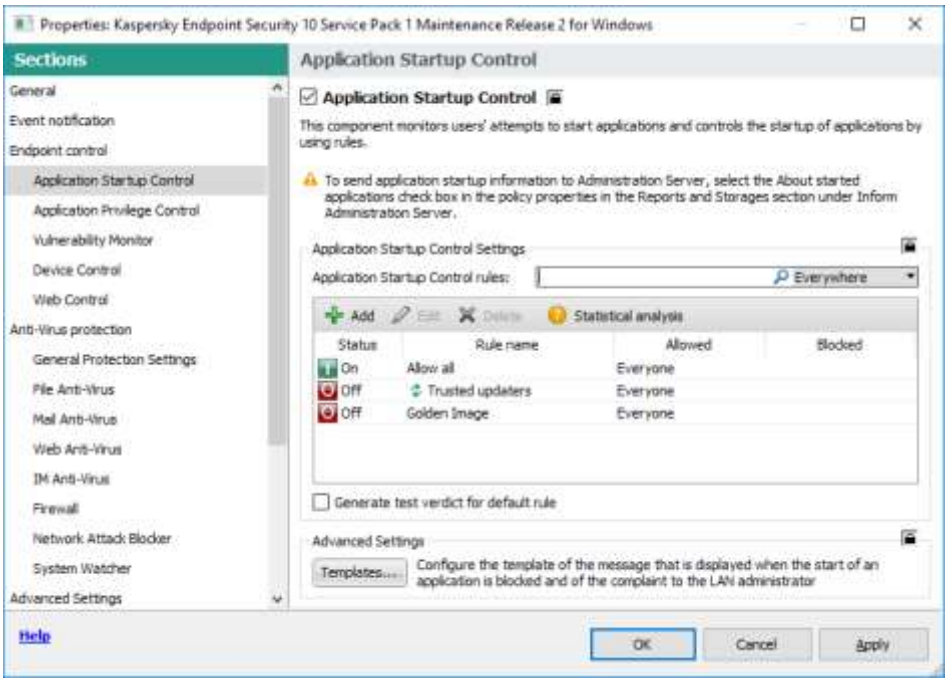
وارد Policies در قسمت Managed computer شوید.

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 یProperties 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 ، آنComponent را بر روی آنتی ویروس سیسستم 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.

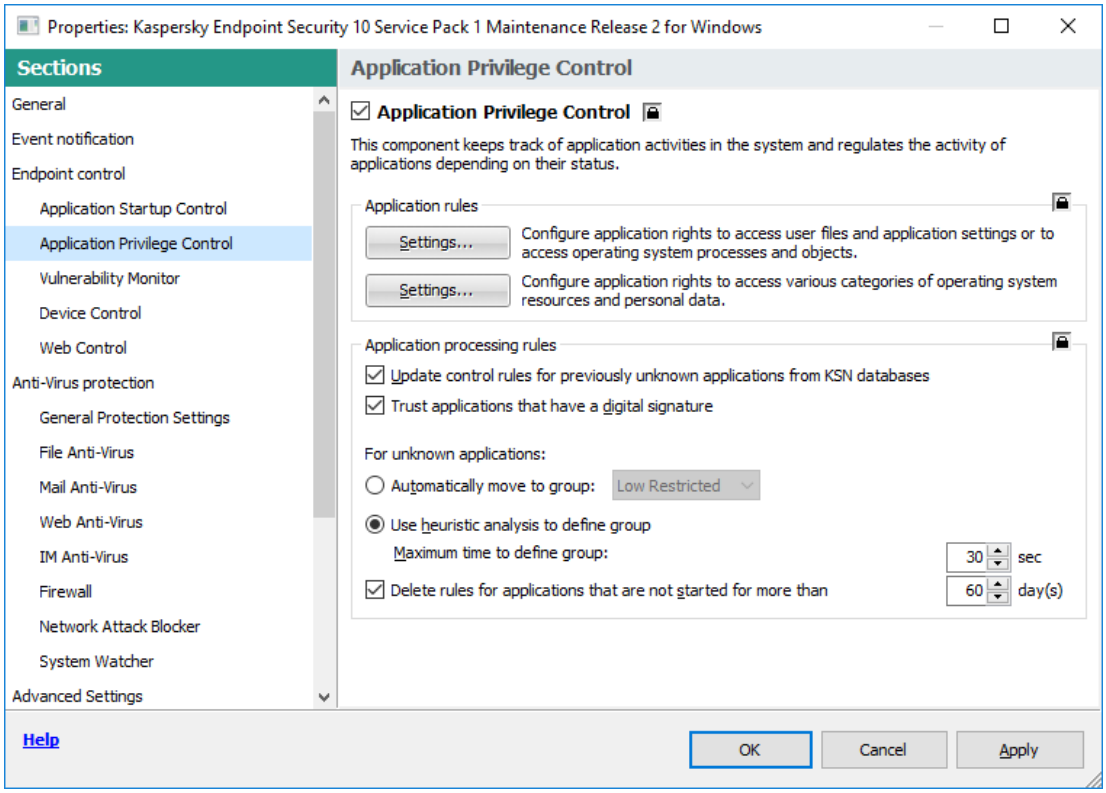
Application startup control

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 ازین قابلیت شما با زدن دکمه Add، Category ساخته شده را رویت می کنید در این قسمت اجازه دسترسی و یا عدم دسترسی را برای کاربران تعیین نمایید .



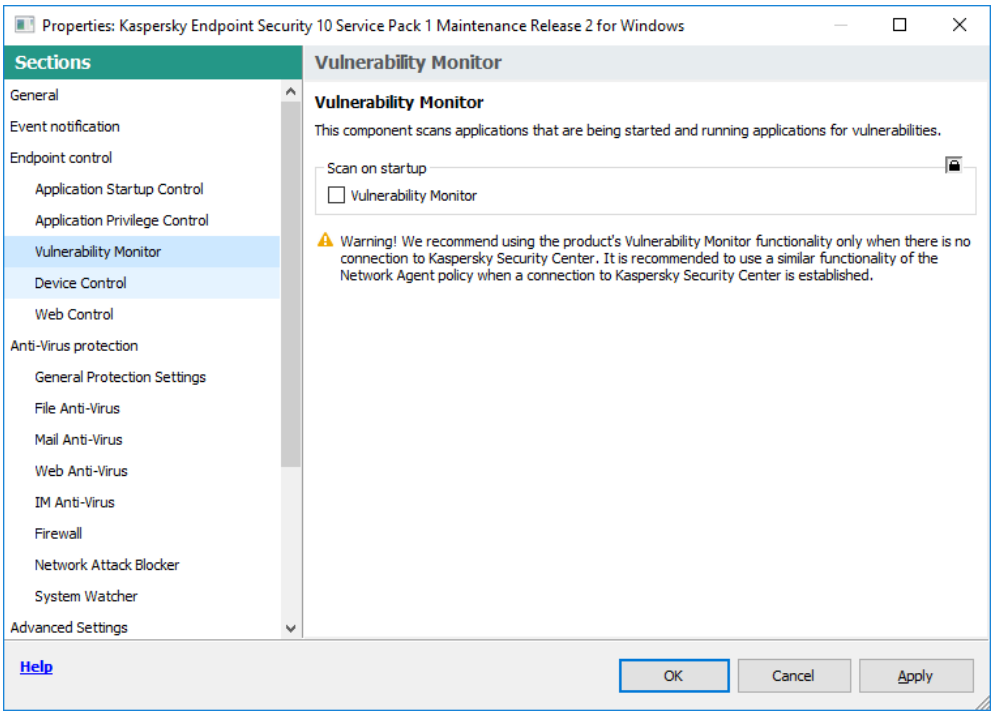
Application Privilege Control

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 ازگروهای Low restricted , High restricted،Untrusted, Trusted 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 نرمافزار های مد نظر خود را در هر سطحی که لازم میدانید اضافه کنید.



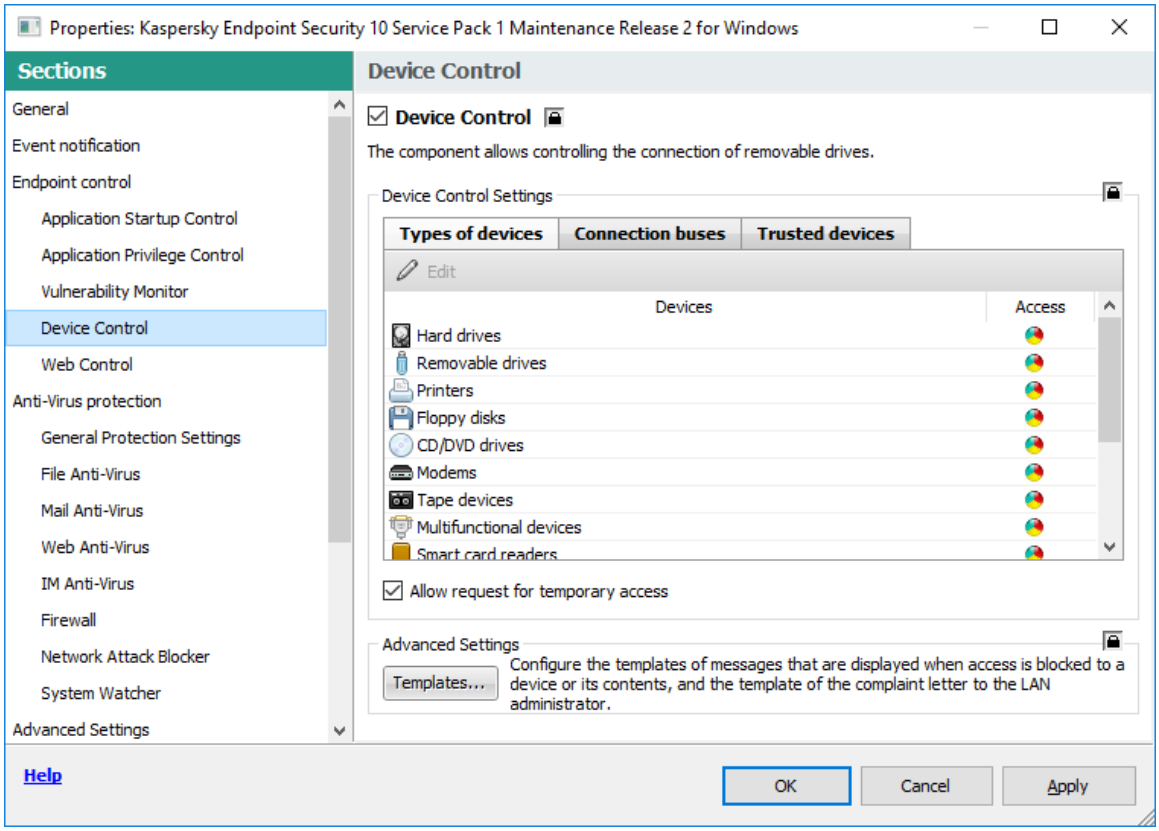
Vulnerability Monitor

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 ودر صورت نیاز می بایست find Vulnerabilities را از داخل Managed computer اجرا کنید.



Device Control

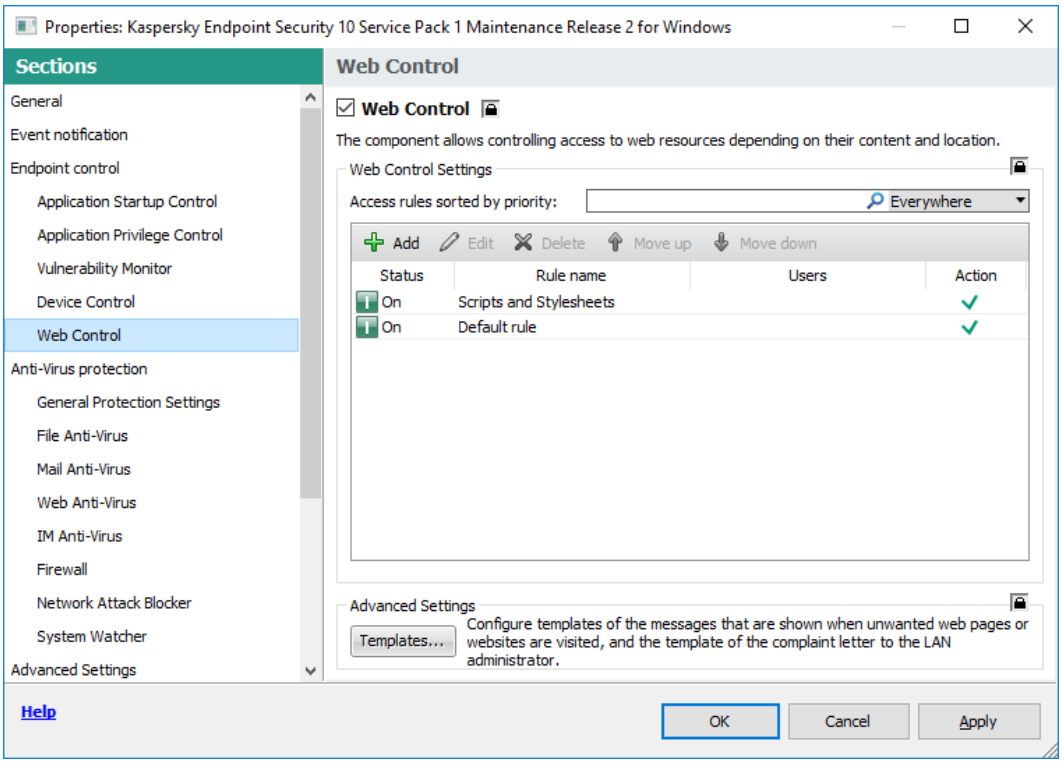
این Component به شما اجازه می دهد تا Removable Device ها را بر روی سیستم های داخل شبکه مدیریت کنید.به طور مثال شما می توانید از این طریق دسترسی به Flash Memory و یا CD\DVD-ROM را روی سیستم های کاربران ببندید.



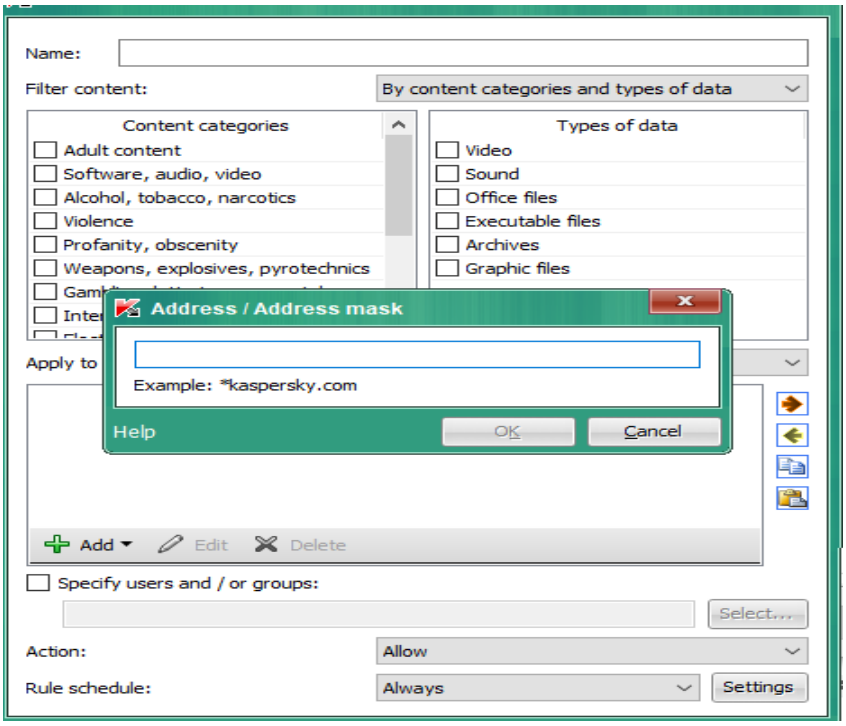
بروی Removable drives کلیک کرده و به صورت پیش فرض در قسمت Access ، Depend On busمی باشد که میتوانید Allow یا blockرا انتخاب نمایید و یا می توانید برای تعیین دسترسی برای تعدادی از کاربران دکمه Edit را بزنید و با اضافه کردن کاربران دسترسی Read ,Write مشخص کنید.

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,....) ویا بر اساس URL ، مدیریت کنید.

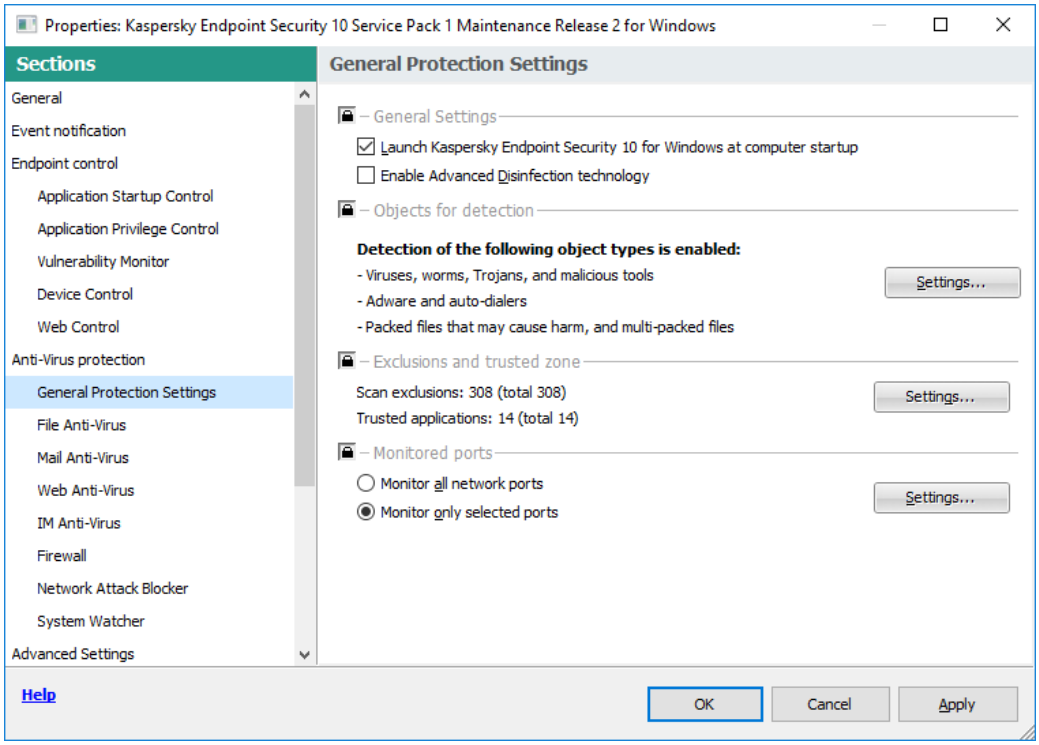


بروی گزینه Addکلیک کرده در قسمت filter Content، همانطور که مشاهده می کنید بر اساس محتوا می توانید سایت های مد نظرتان را فیلتر نمایید . در صورتی که بخواهید آدرس سایت خاصی را فیلتر نمایید در قسمت apply to addressحالت To individual addressرا انتخاب و دکمه Add را می زنید و مانند نمونه سایت را وارد می نمایید.در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



Anti-Virus protection

General Protection Setting



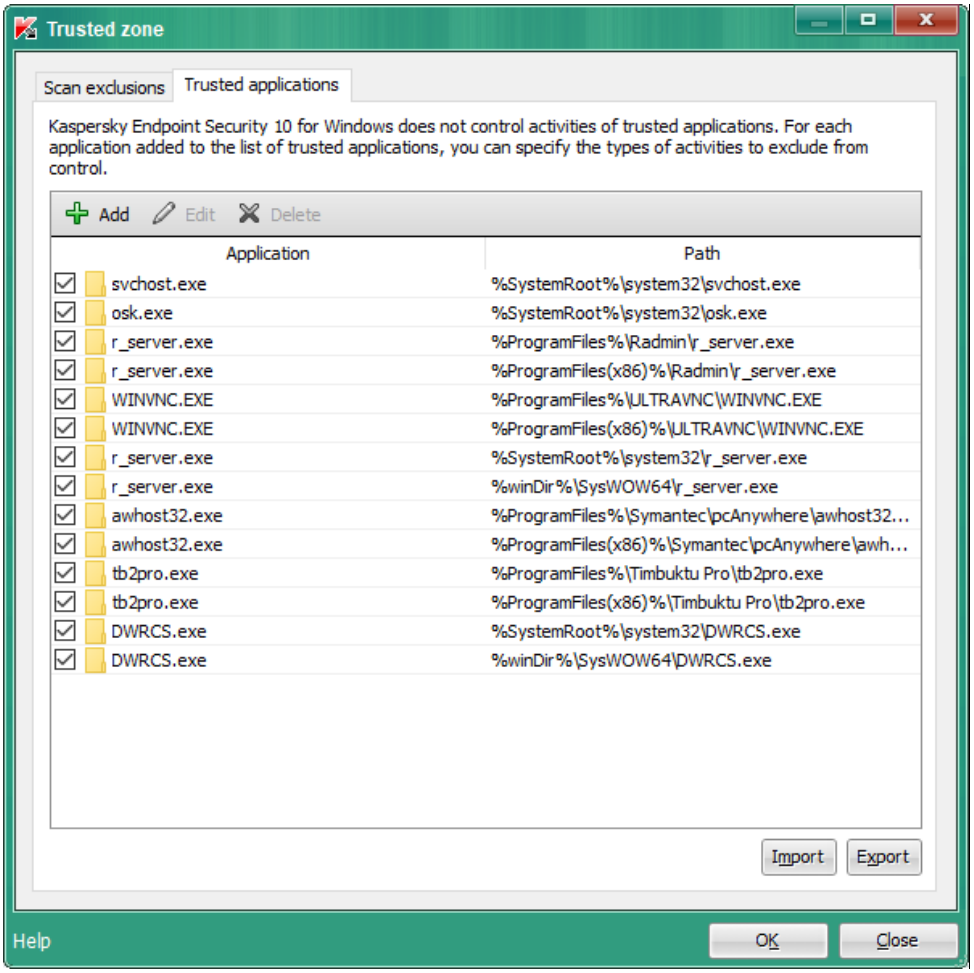
امکان بسیار خوبی که این Component در اختیار شما می گذارد این است که در قسمت Exclusions and trusted zone می توانید یک Application یا یک Folder را Exclude کنید که چه Component هایی از آنتی ویروس بر روی آن فعال نباشد(و یا حتی تمامیComponentهای آنتی ویروس بر روی آن غیر فعال باشد).

از این ویژگی زمانی استفاده می شودکه 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 شودو موجب شود قسمتی ازآن کار نکند.همچنین در مواردی که Crack های یک نرم افزار به عنوان ویروس شناخته می شود، از این ویژگی استفاده می شود.

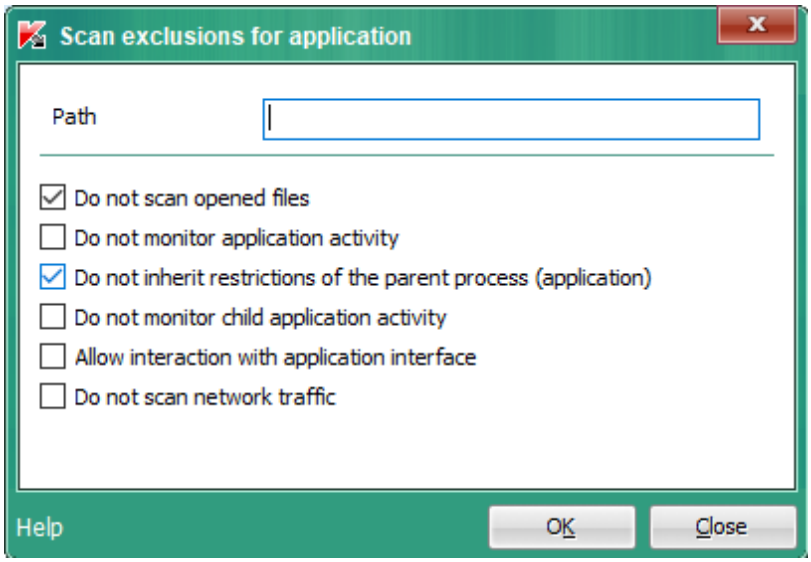
جهت تنظیم این قسمت روی setting کلیک نمایید، سپس وارد تب Trusted application شوید.

دراین 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.

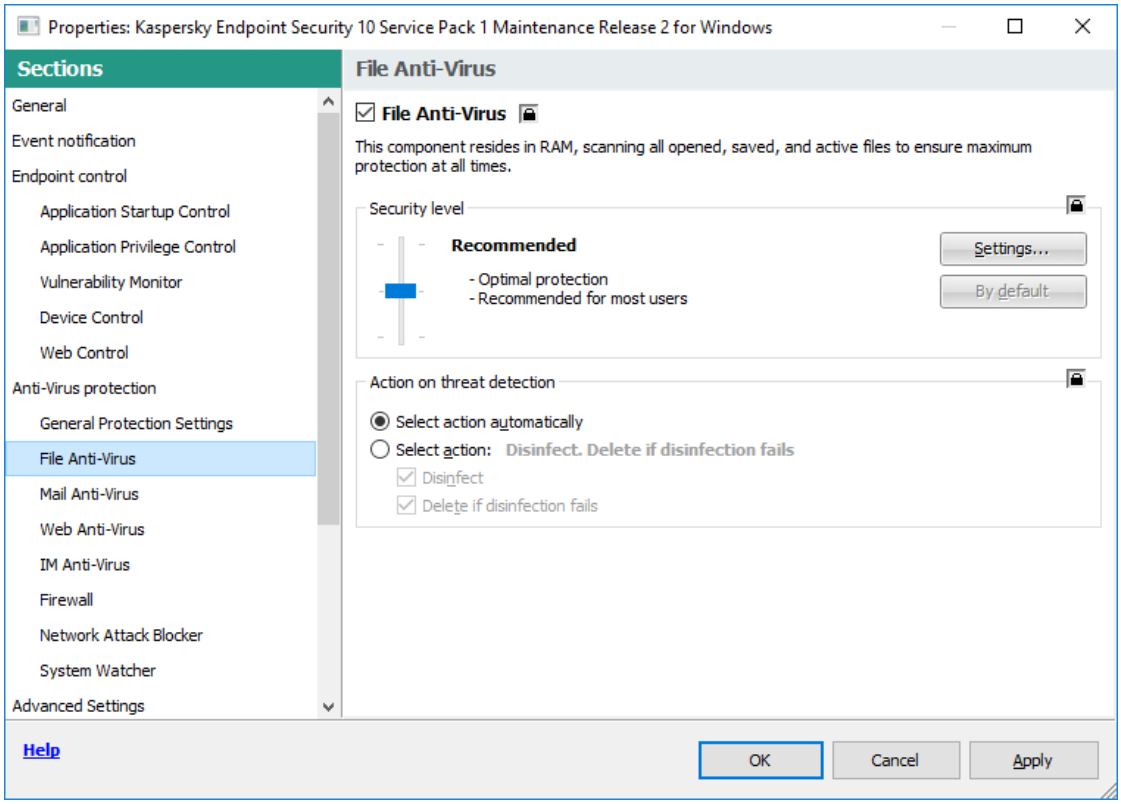


گزینه ی Add را انتخاب کنید و سپس مسیرApplication مورد نظر را در قسمت Applicationوارد کنید و در قسمت Action تعیین کنیدچه عملیاتی بر روی این Application صورت گیرد.



درصورتی که بروی تعداد خاصی client مدنظرتان باشد با زدن تیک Do not scan network trafic بروی Any در قسمت IP addresses کلیک کرده و گزینه spacifyرا زده و IPهای کامپیوتر های مد نظر را وارد نمایید.

File Antivirus

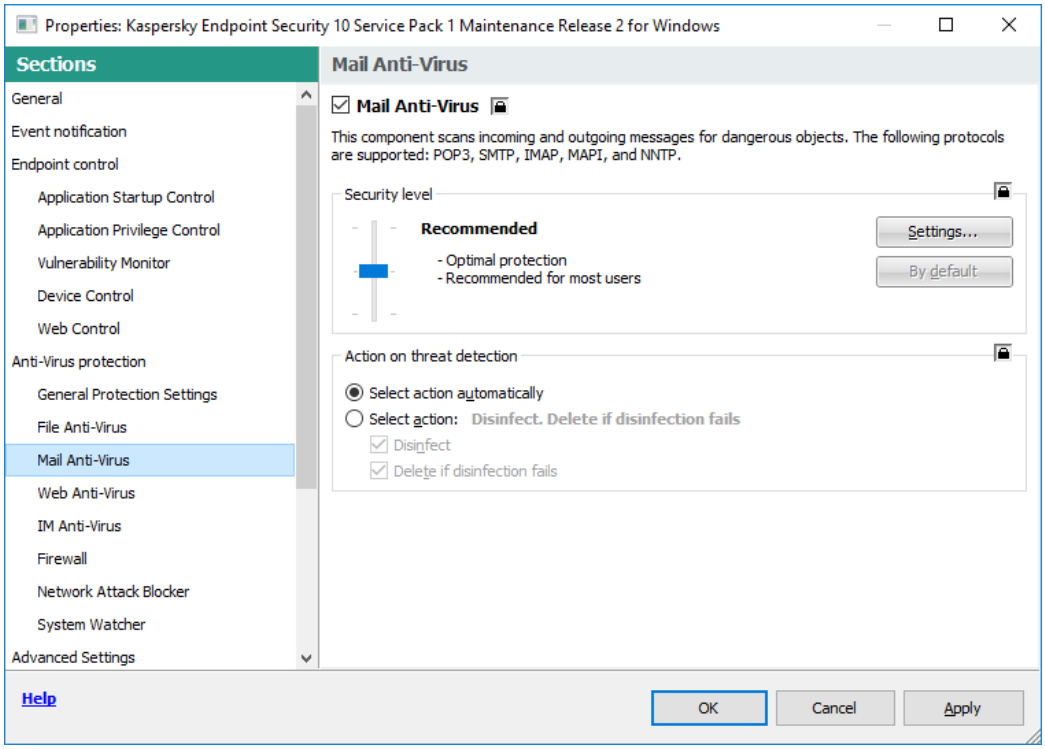


همان طور که مشاهده می کنید قفل ها به صورت پیش فرض بسته است و بنا به نیاز می توانیدآنها را باز کنید، با گذاشتن یا برداشتن تیک گزینه Enable File Anti-virus می توانیداین Component را روی سیستم ها فعال یا غیر فعال کنید.در قسمت Security level سطح امنیتی این Component را تعیین می کنیم و درقسمت Action نحوه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

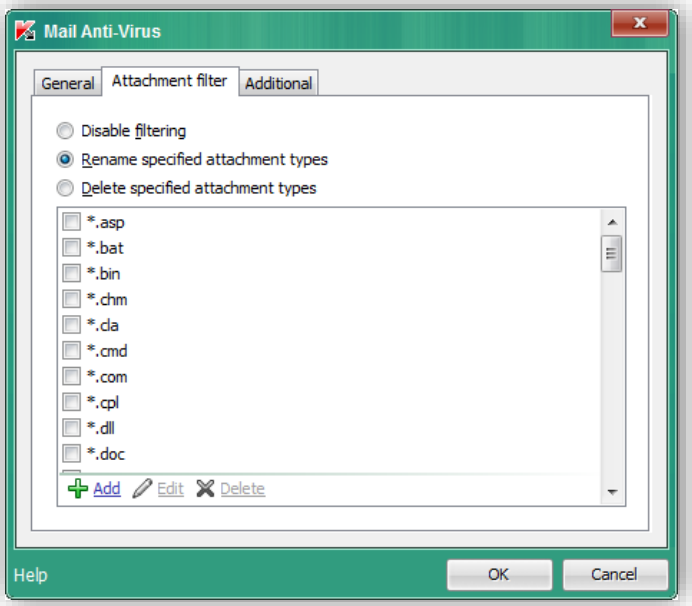
Delete if disinfection fails: در صورتیکه عملیات Disinfect انجام نشود آنتی ویروس کل فایل را پاک خواهد نمود.



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.

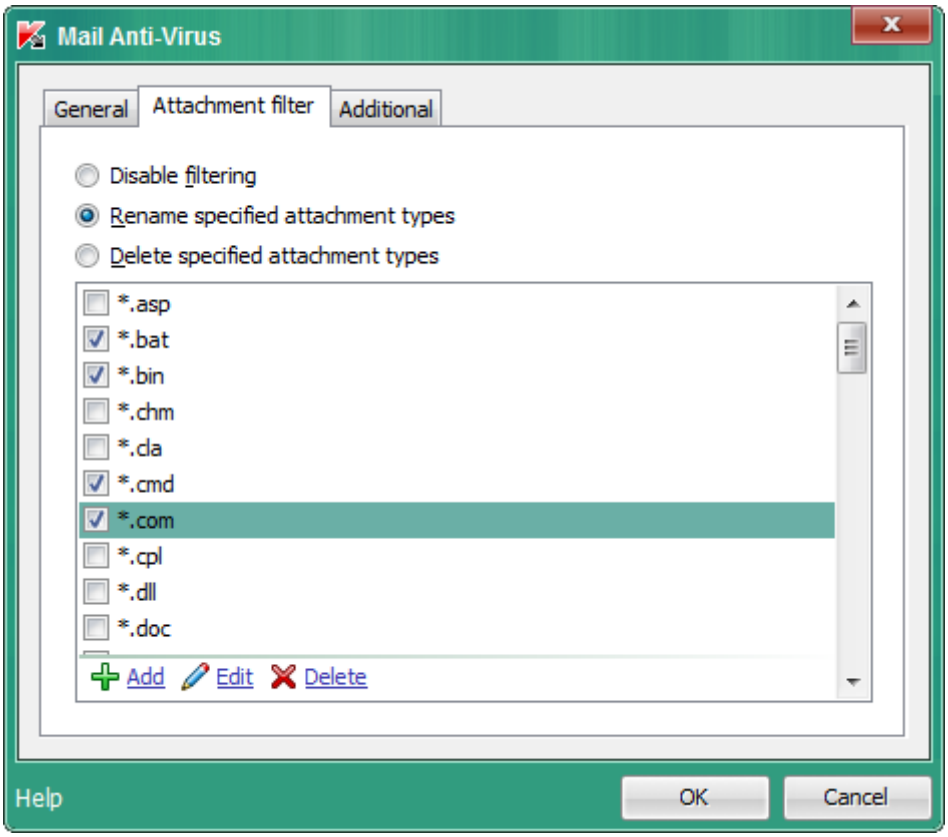
به طور مثال ممکن است یک سری فایل های آلوده به همراه ایمیل ها وارد شبکه ی شما شوند، برای جلوگیری از آلودگی سیستم ها می توانیم در تب Attachment filter یکسری تنظیمات را روی این ایمیل ها اعمال نمایید.برای اینکار روی گزینه ی setting کلیک نمایید و در پنجره ای که باز می شود وارد لبه attachment filter شوید.



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

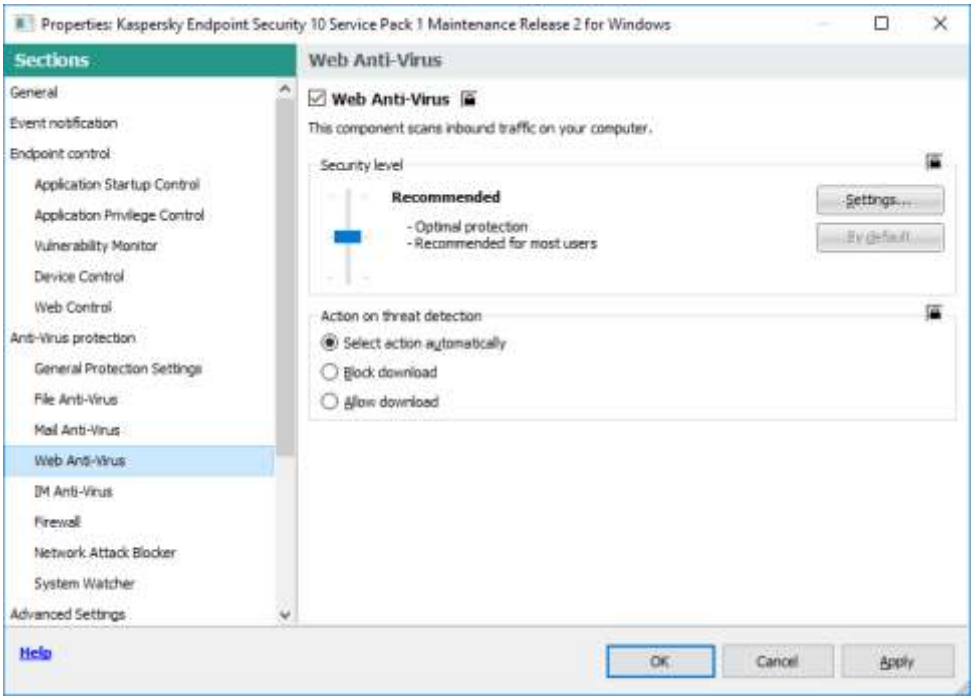
همچنین با انتخاب گزینه ی Rename specified attachment type ، در صورت دریافت ایمیلی همراه Attachment ی با پسوند های انتخاب شده در لیست ، این پسوند تغییر نام خواهد داد (در واقع فایل ویروسی همراه ایمیل، دارای Script ی است که پس از Rename شدن قادر به اجرا نمی باشد.)

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.

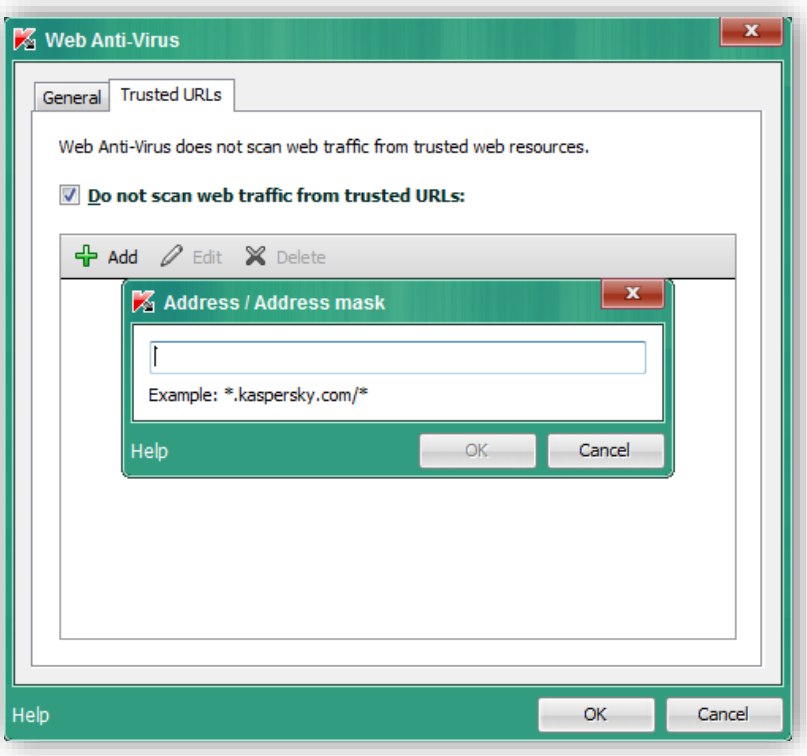


Web Anti-virus

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.

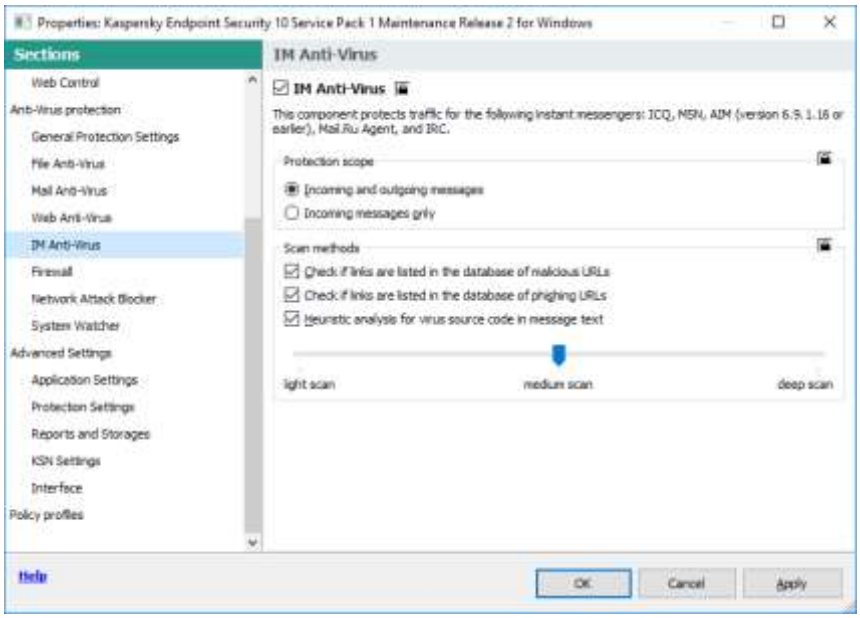


برای اینکار وارد قسمت settings شوید ووارد تب Trusted URLs شوید و مطابق نمونه URL مورد نظر خود را وارد کنید.



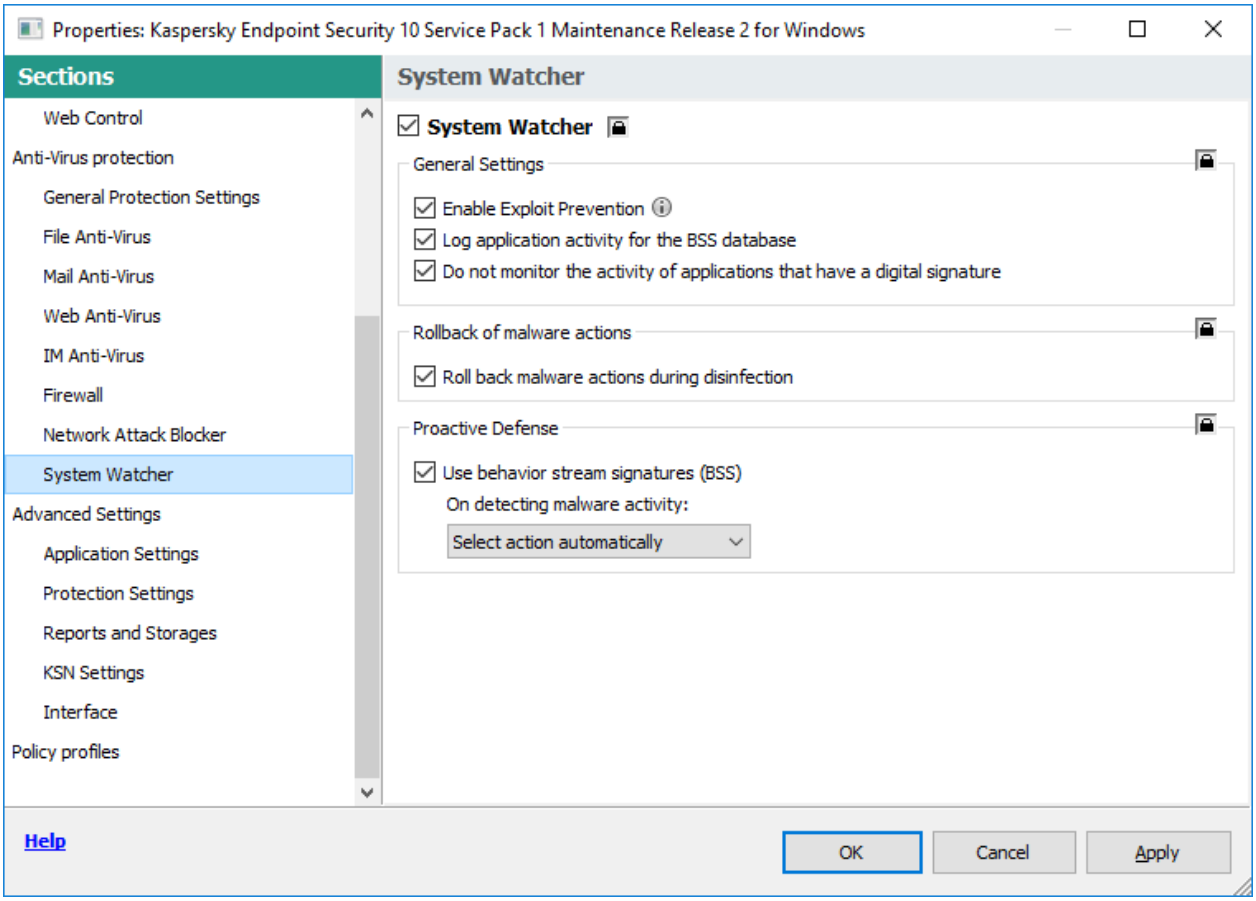
IM Anti-Virus

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



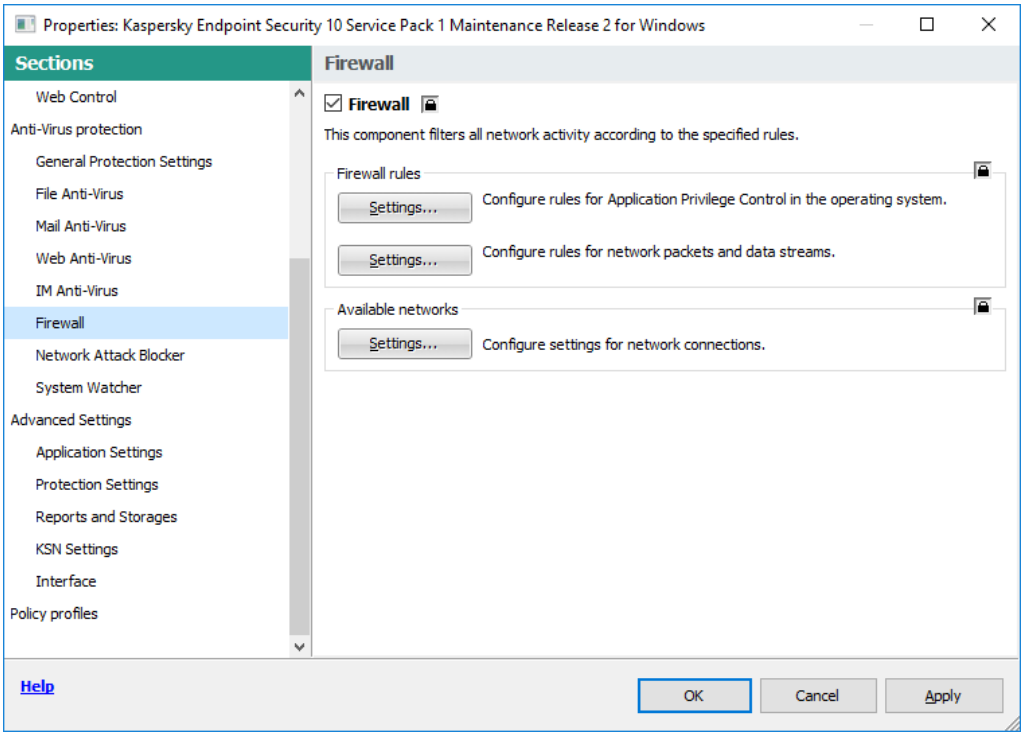
System Watcher

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 جزیی تری برای سایر Component های آنتی ویروس جهت حفاظتی عمیق تر، فراهم می آورد.

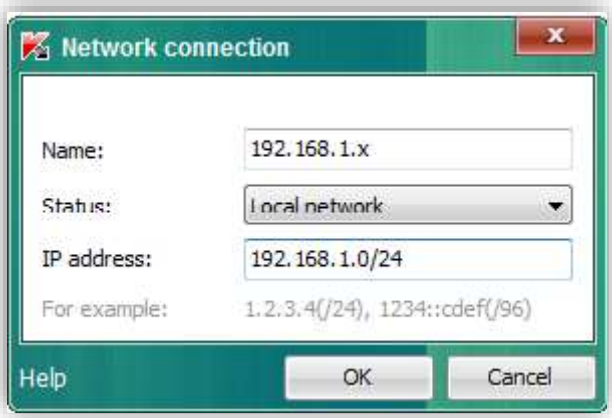


Firewall

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.

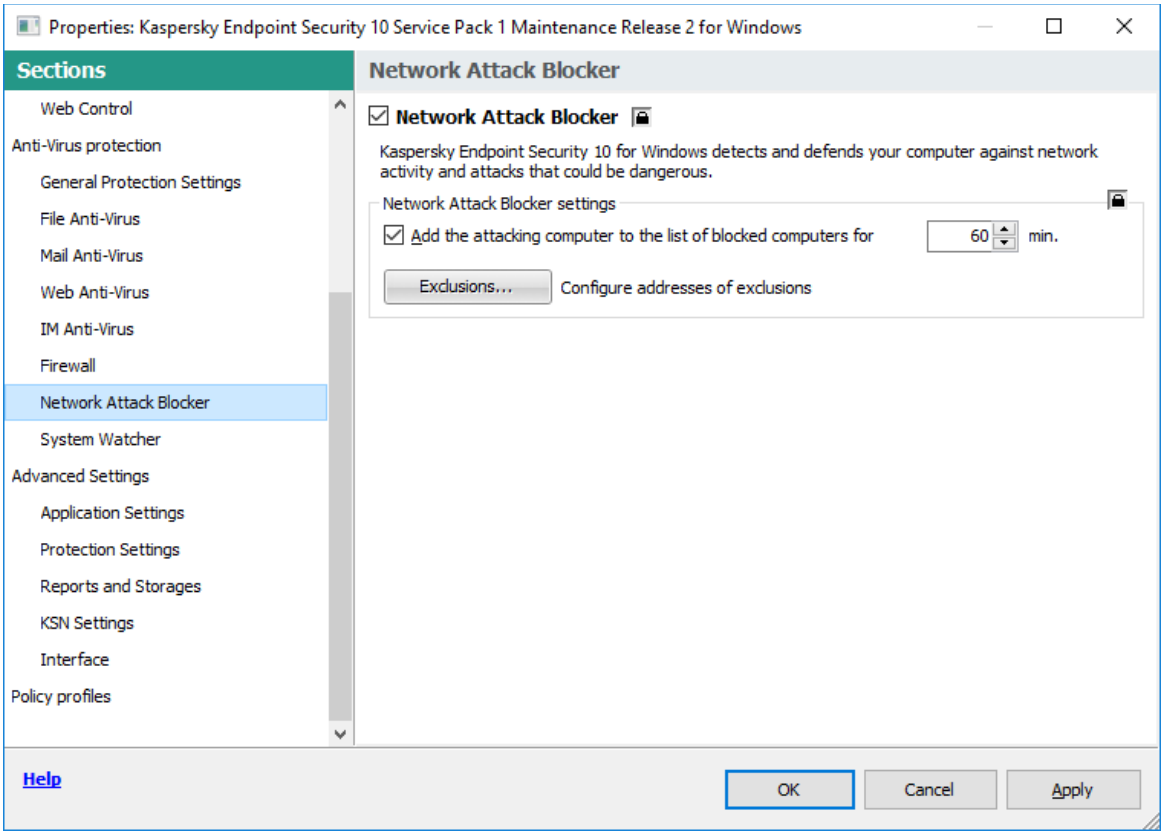


در این قسمت شما باید رنج شبکه خود را بعد از نصب Security Center وارد نمایید براین کار در قسمت Available Network، Setting را زده و با زدن دکمه Addپنجره زیر باز خواهد شد به عنوان مثال اگر رنج شبکه شما ۱۹۲,۱۶۸,۱,۰ تا ۱۹۲,۱۶۸,۱,۲۵۵ باشد برای وارد کردن اطلاعات به صورت زیر اعمال نمایید



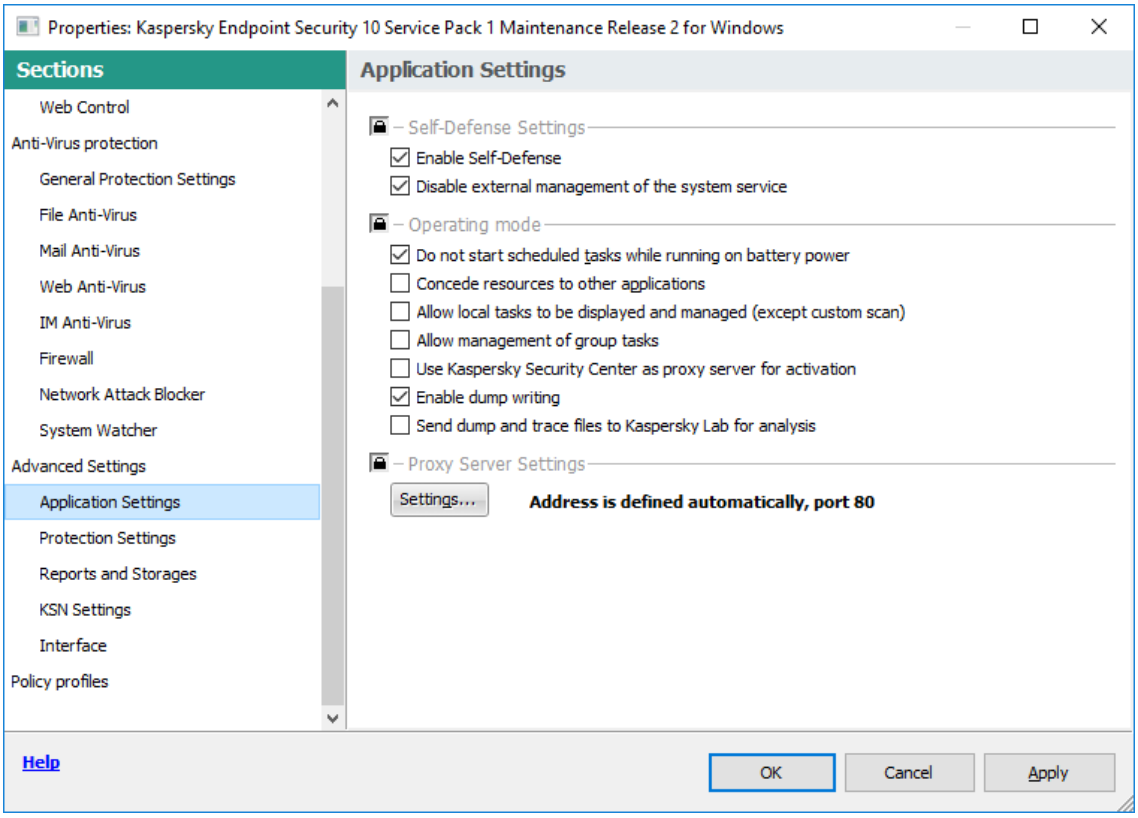
Network Attack Blocker

این component ازشبکه شما دربرابرحملات داخلی و خارجی که ممکن است برای سیستم های شبکه خطرناک باشد، حفاظت می کند.



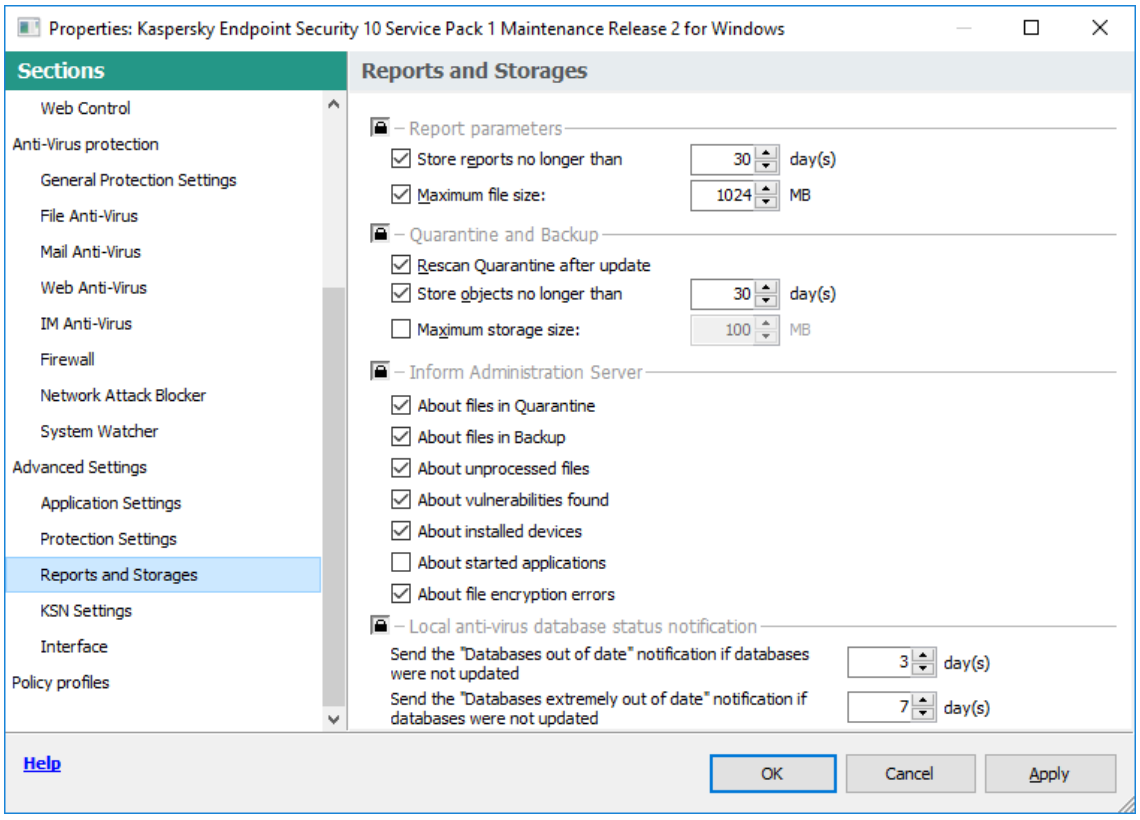
Application Setting

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.



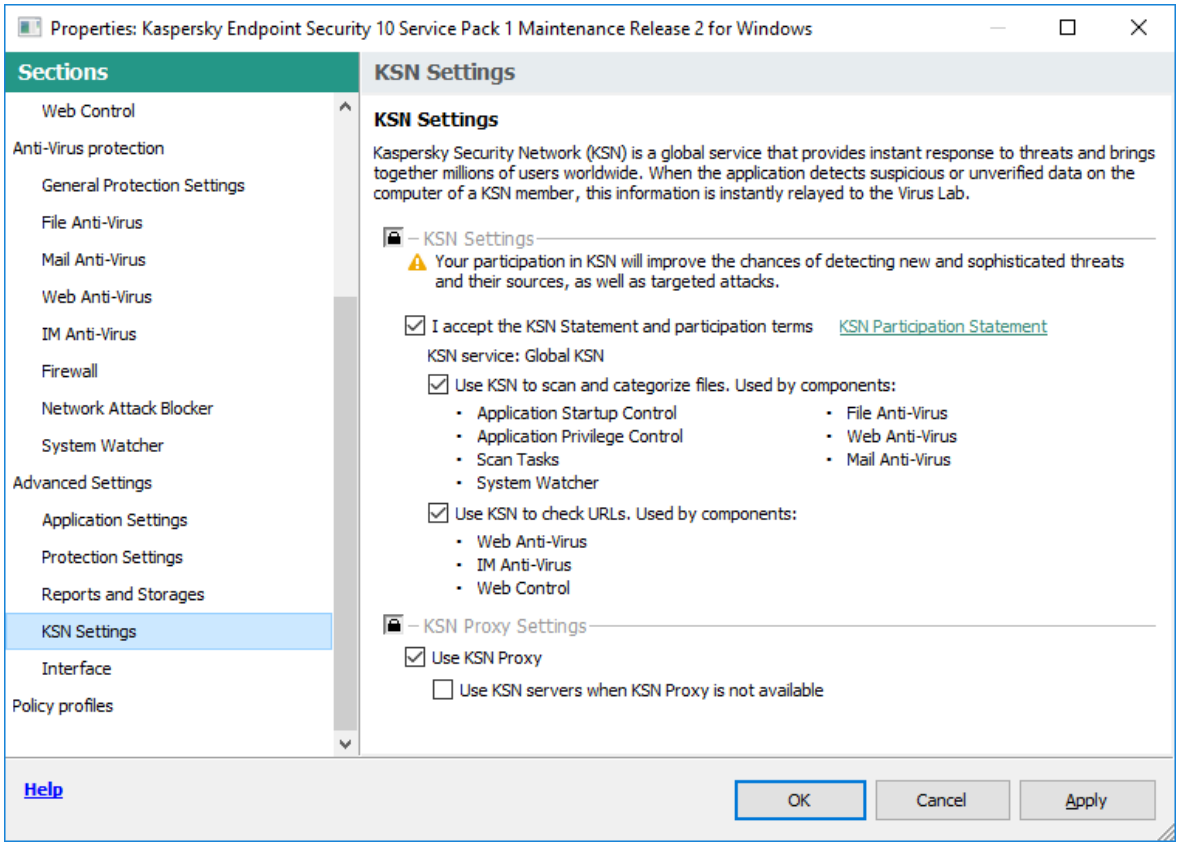
Reports and storages

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 اطلاعلت به سرعت برای لابراتوار شناسایی ویروس ها فرستاده می شود.



موفق باشید

پشتیبانی فنی شرکت ایدکو