## Policyهای 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

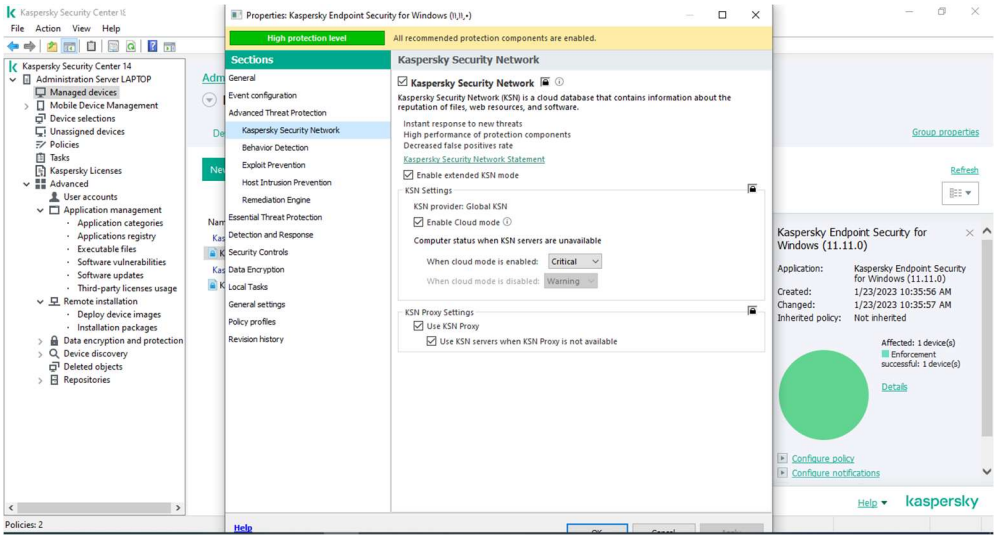
با یکبار کلیک کردن بر روی قفل حالت قفل تغییر خواهد کرد، این قفل دسترسی کاربران را مشخص می کند هر

قسمتی که قفل باز داشته باشد توسط کاربر قابل تغییر می باشد.در ادامه چند نمونه از این Component ها را

توضیح خواهیم داد.

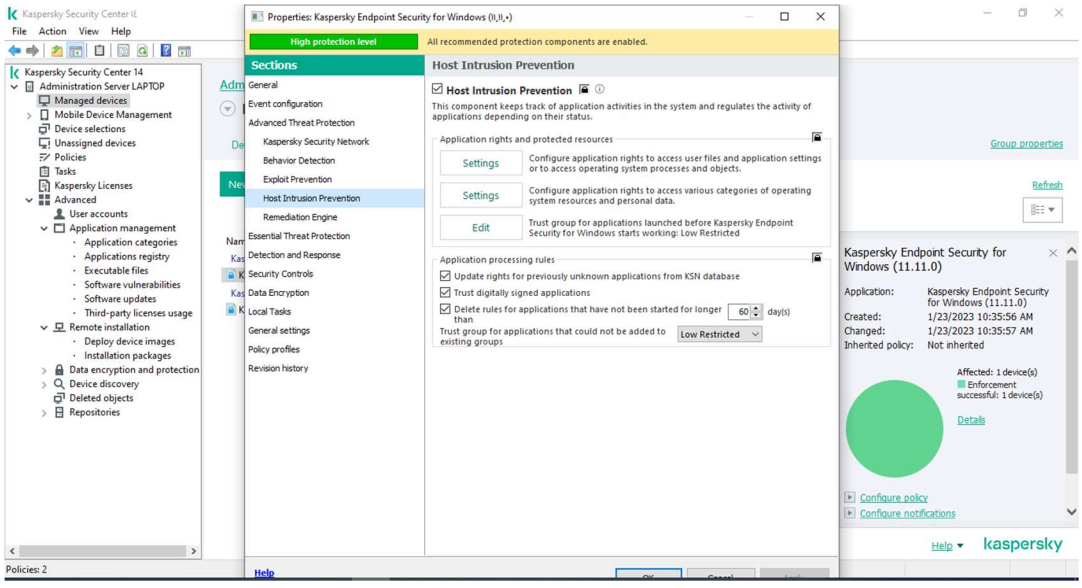
## KSN Setting

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 کند و 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.



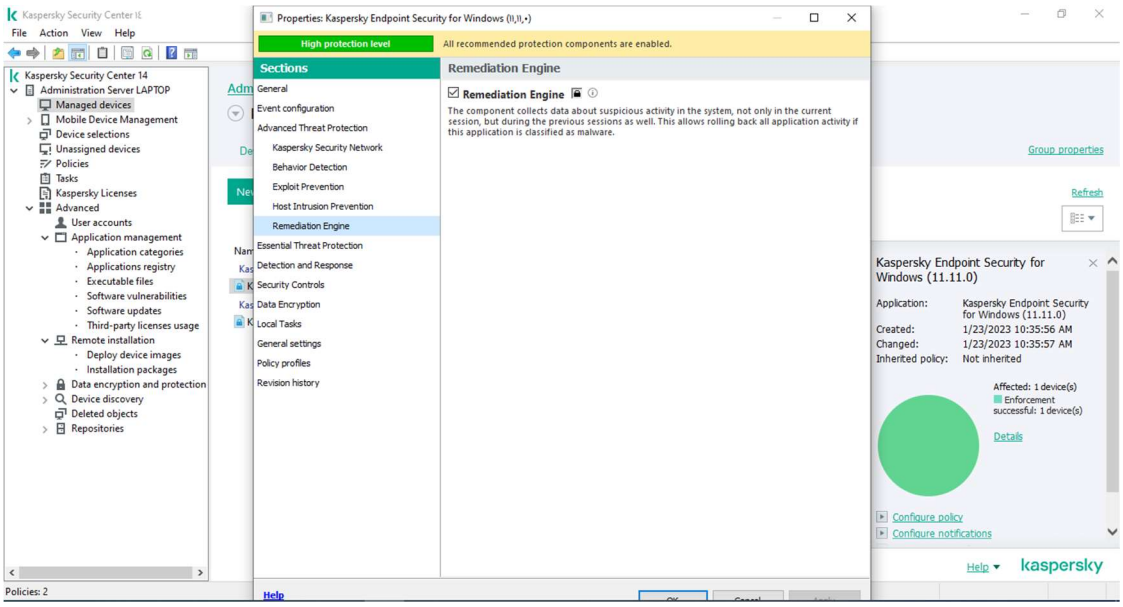

## Host Intrusion Prevention

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 High restricted , Low ,restricted, Untrusted, Trusted اجازه فعالیت را بر اساس گروه بندی انجام شده به آن Application می دهد.به Application Rule رفته برای این کار بروی Setting در قسمت Application Privilege control رفته و نرم افزار های مد نظر خود را در هر سطحی که لازم میدانید اضافه کنید.



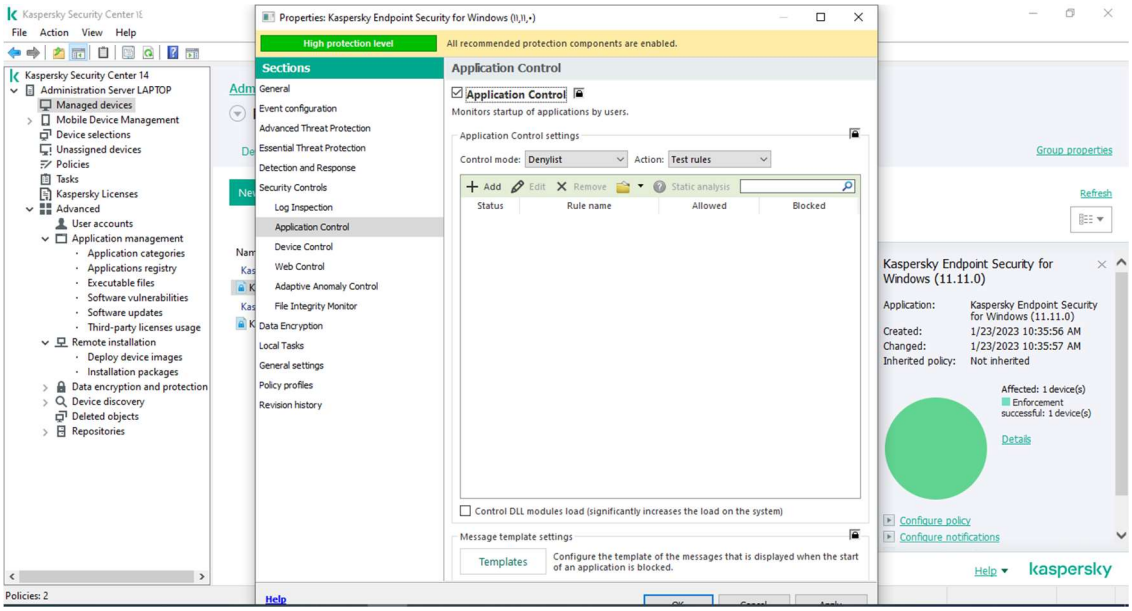
## Remediation Engine

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.



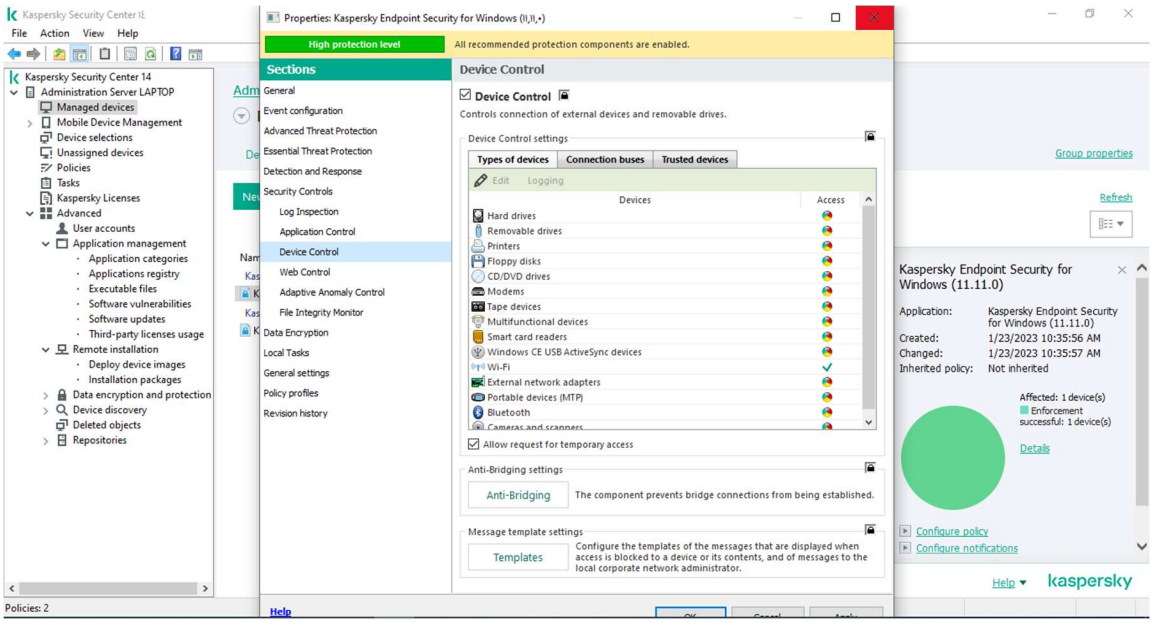

## Application control:

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 Management یک Category ایجاد کنید که در قسمت های قبلی توضیح به طور کامل داده شده است .سپس برای استفاده ازاین 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 .




## 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.

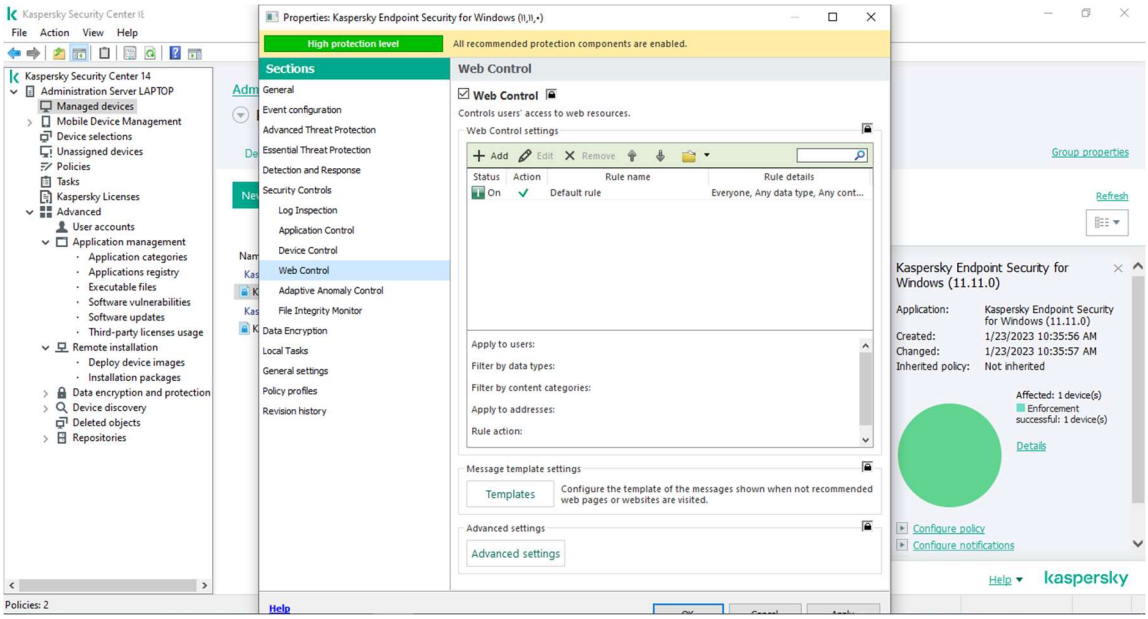


بروی Removable drives کلیک کرده و به صورت پیش فرض در قسمت Access ، Depend On bus می باشد که میتوانید Allow یا blockرا انتخاب نمایید و یا می توانید برای تعیین دسترسی برای تعدادی از کاربران دکمه Edit را بزنید و با اضافه کردن کاربران دسترسی Read ,Write مشخص کنید.

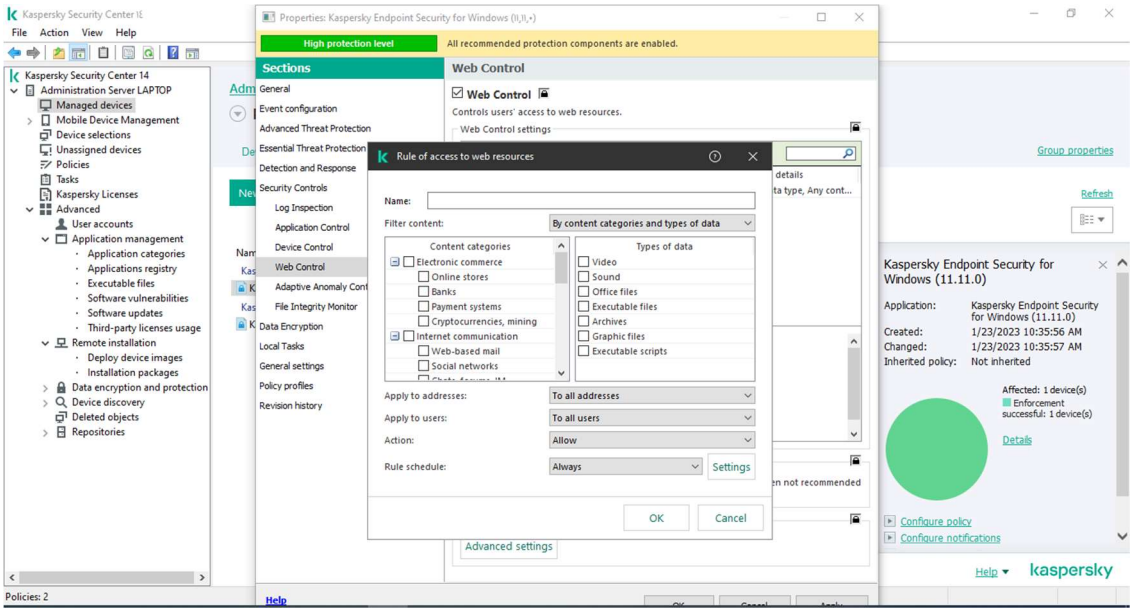
با توجه به اینکه ممکن است در شبکه های نیاز داشته باشیم که USB ها بسته باشد ممکن است نتوان از پرینتر و دستگاه های که به درگاه USB متصل میشوند استفاده کرد به همین منظور باید از تب Trusted Devices آن تجهیز مورد نظر را Trust دهیم تا بتوانیم از آن استفاده کنیم .

## Web Control

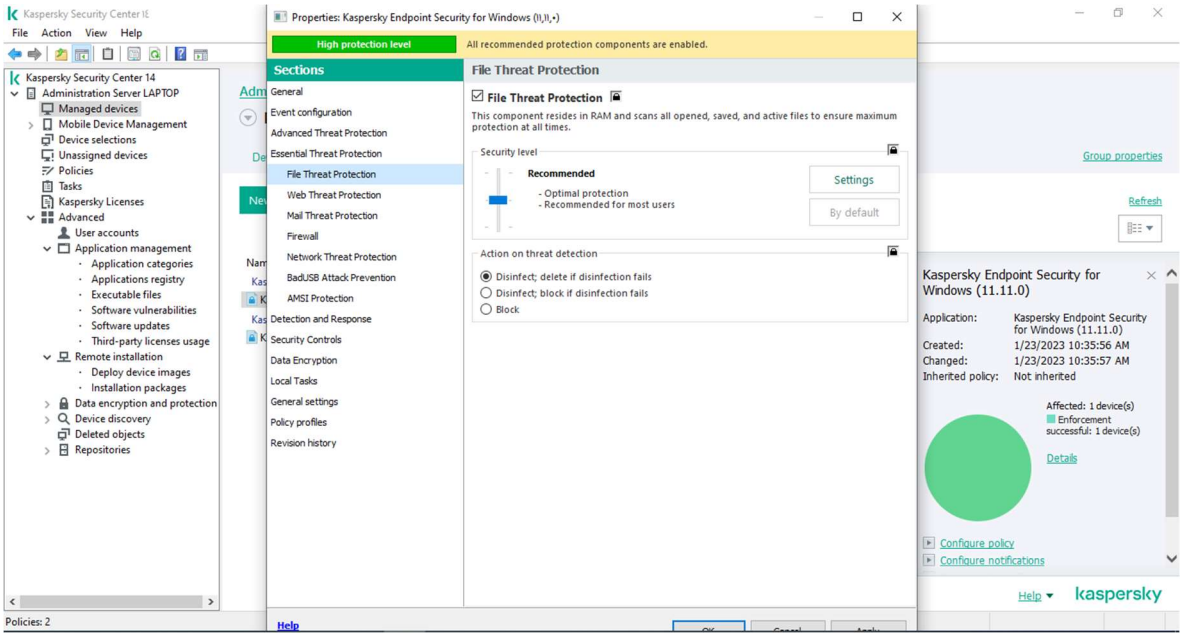
این Component این امکان را به شما می دهد تا از طریق آن دسترسی کاربران به وب سایت های خاصی را براساس Content و یا بر اساس نوع داده( به طور مثال video, sound,....) ویا بر اساس URL ، مدیریت کنید.




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.




## File Threat Protection

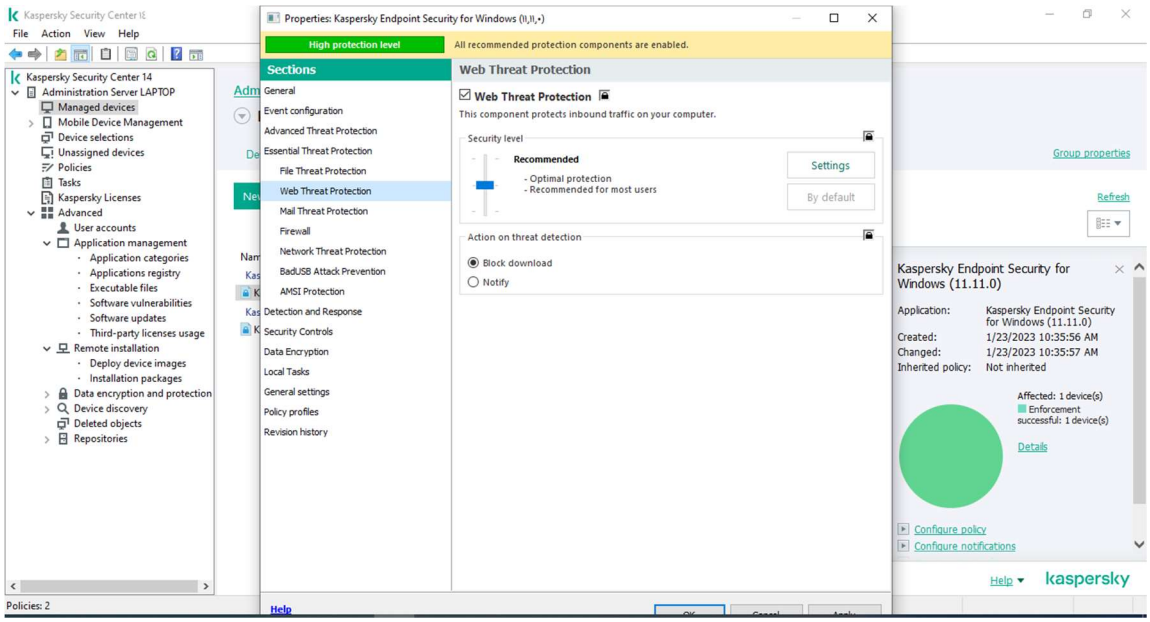



همان طور که مشاهده می کنید قفل ها به صورت پیش فرض بسته است و بنا به نیاز می توانیدآنها را باز کنید، با گذاشتن یا برداشتن تیک گزینه Enable File Threat Protection می توانید این Component را روی سیستم ها فعال یا غیر فعال کنید.

در قسمت Security level سطح امنیتی این Component را تعیین می کنیم و 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 بر چگونگی 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.

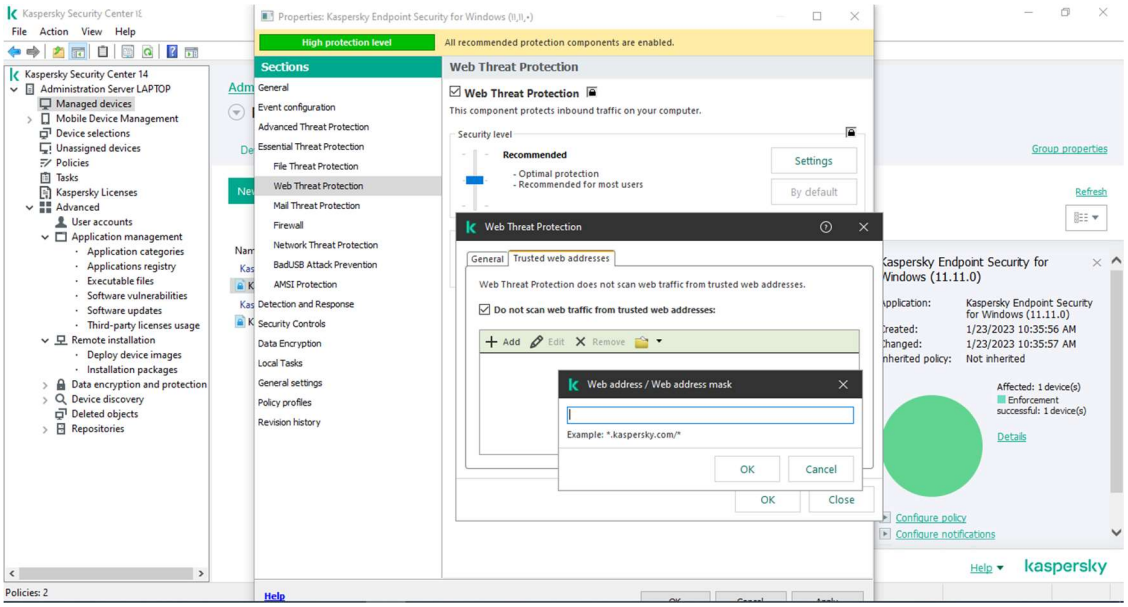
Disinfect: با انتخاب این گزینه در صورتیکه تنها قسمتی از فایل آلوده شده باشد، آنتی ویروس تنها قسمت آلوده را پاک می کند (حذف ویروس) Delete if disinfection fails در صورتیکه عملیات Disinfect انجام نشود آنتی ویروس کل فایل را پاک خواهد نمود.

## Web Threat Protection



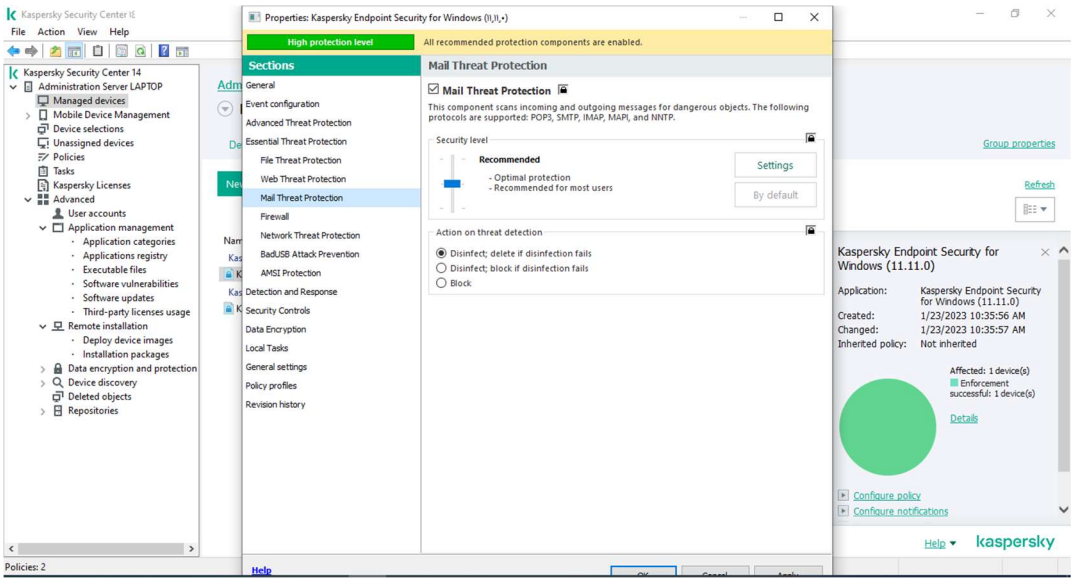

برای Web آنتی ویروس Action را به حالت Block می گذاریم و در قسمت setting می توانیم URL های Trust مورد نظر خود را مطابق نمونه تعریف کنیم.

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



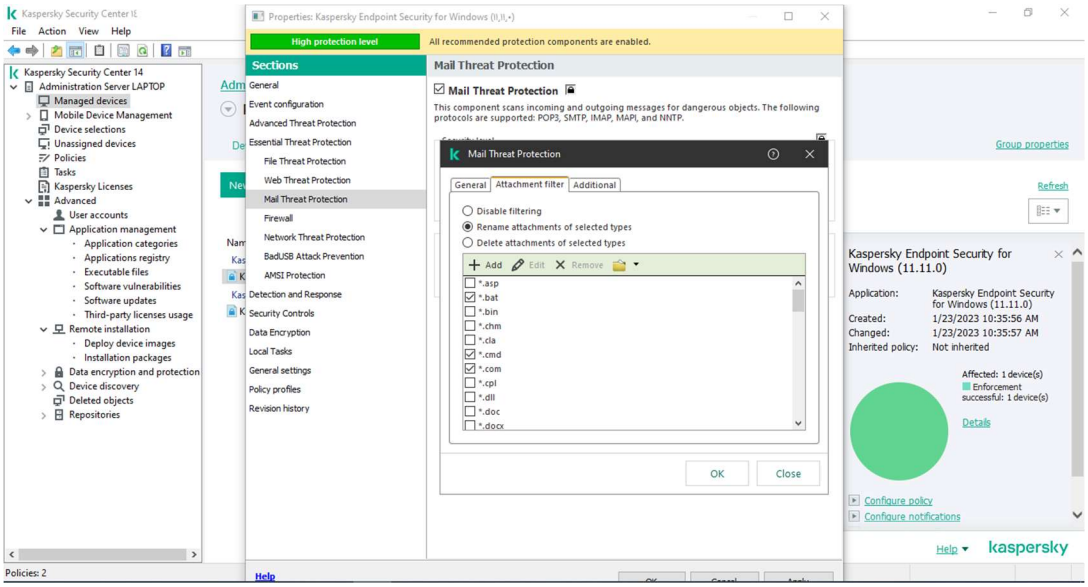

## Mail Threat Protection

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.



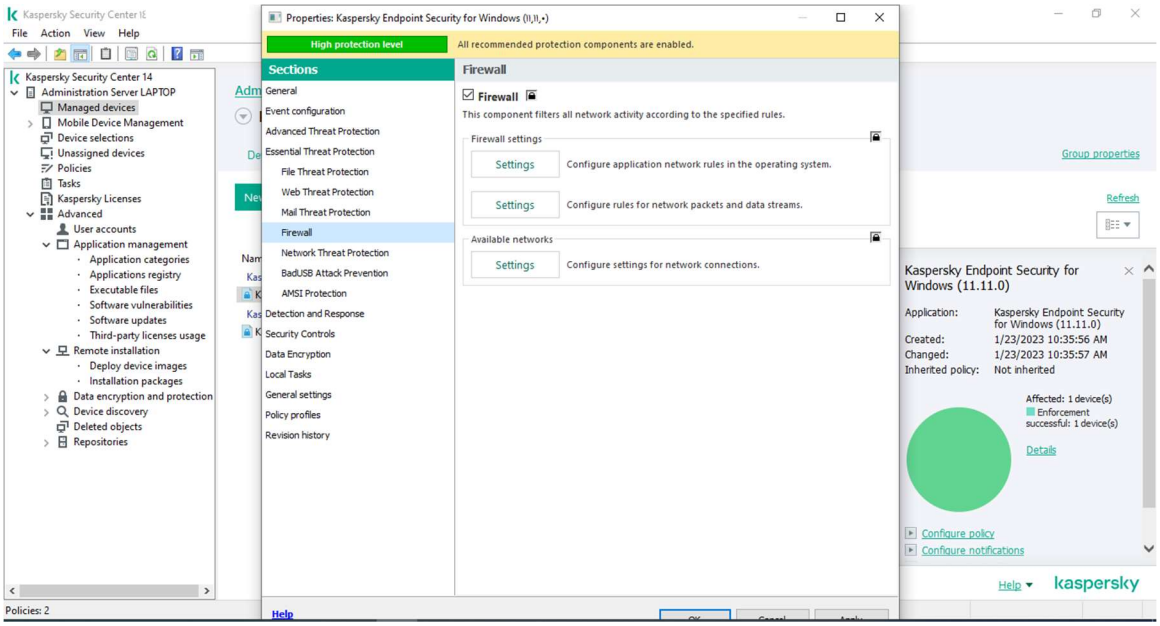

با انتخاب گزینه ی Disable filtering ، هیچ Filtering روی ایمیل‌ها اعمال نمی شود.

همچنین با انتخاب گزینه ی Rename attachments of selected 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.)

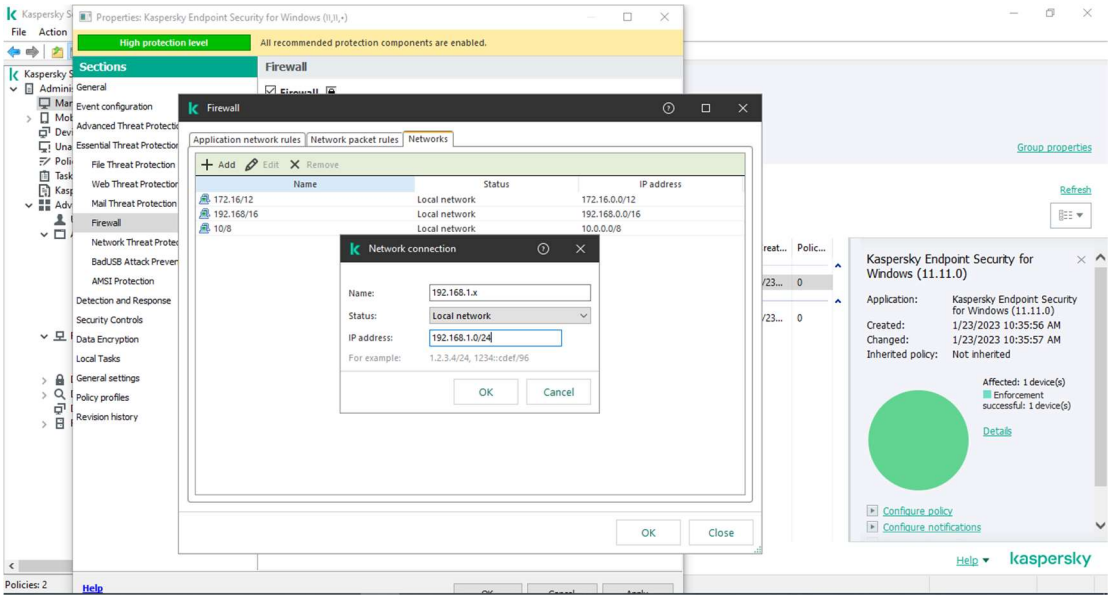
در صورتی که بخواهید Attachment ی با پسوند های خاصی هنگام دریافت به صورت اتوماتیک Delete شوند می توانید با انتخاب گزینه ی Delete attachment of selected types و انتخاب پسوند های مورد نظر از لیست مربوطه آنها را delete کنید.

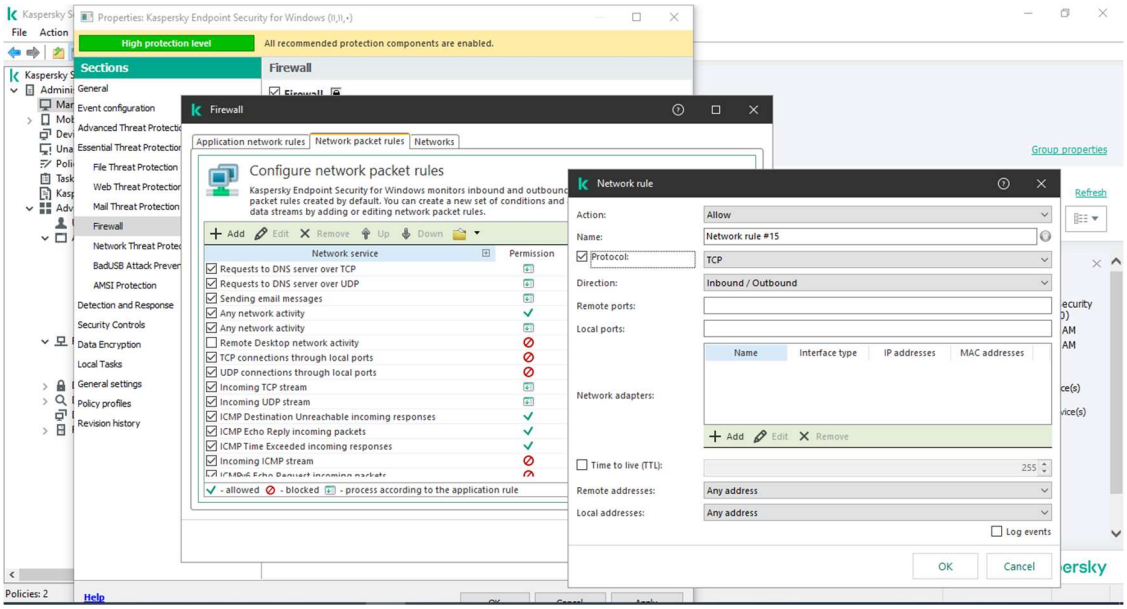
**Firewall:**

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.



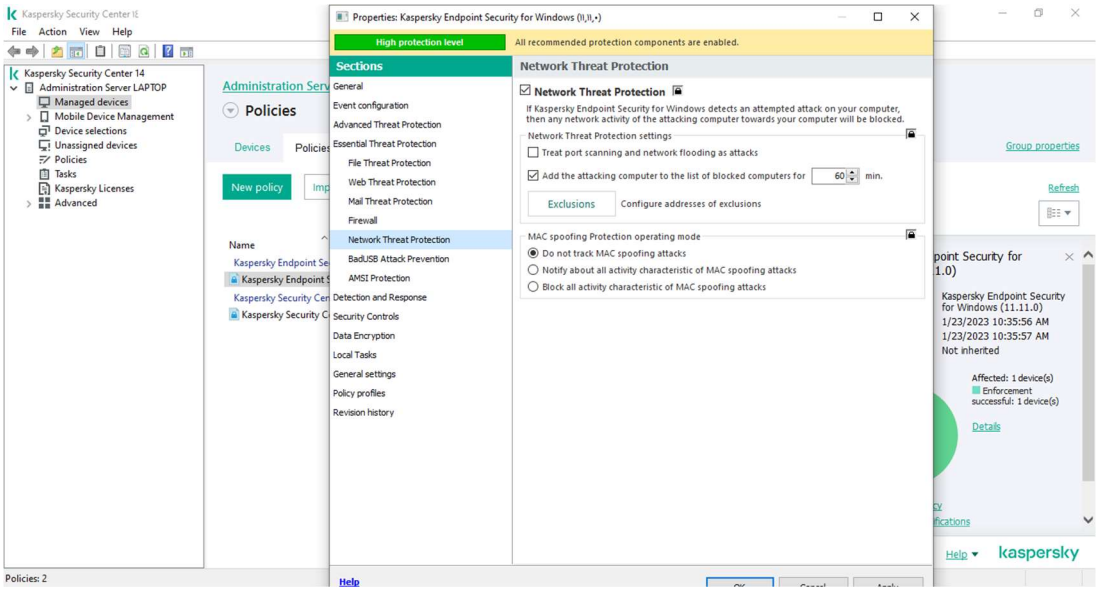

در این قسمت شما باید رنج شبکه خود را بعد از نصب Security Center وارد نمایید براین کار در قسمت Setting، Available Network را زده و با زدن دکمه Addپنجره زیر باز خواهد شد به عنوان مثال اگر رنج شبکه شما 192.168.1.0 تا 192.168.1.255 باشد برای وارد کردن اطلاعات به صورت زیر اعمال نمایید





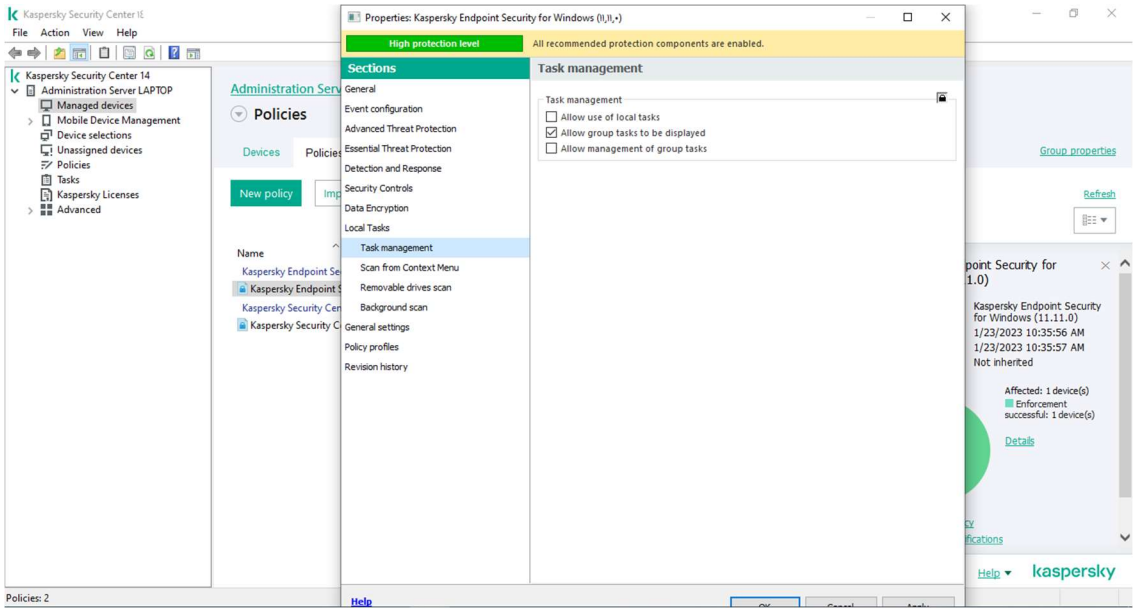

## Network Threat Protection

این component ازشبکه شما دربرابرحملات داخلی و خارجی که ممکن است برای سیستم های شبکه خطرناک باشد، حفاظت می کند. و به مدت 60 دقیقه کامپیوتر را در لیست بلاک قرار میدهد



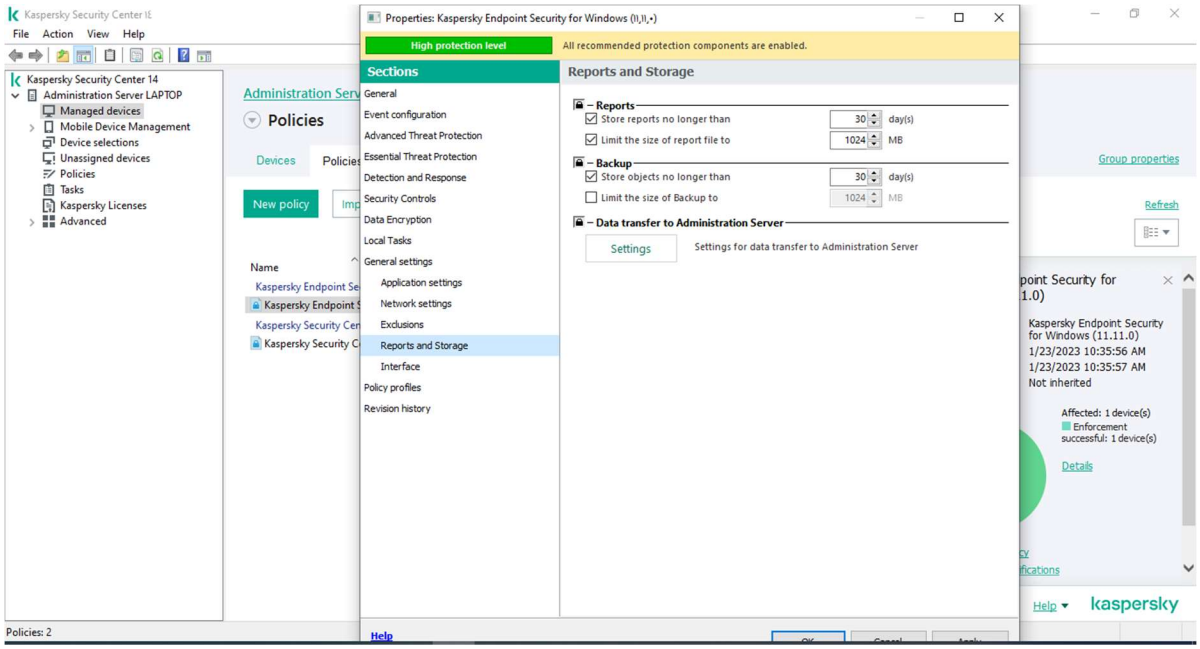

## Task Management

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

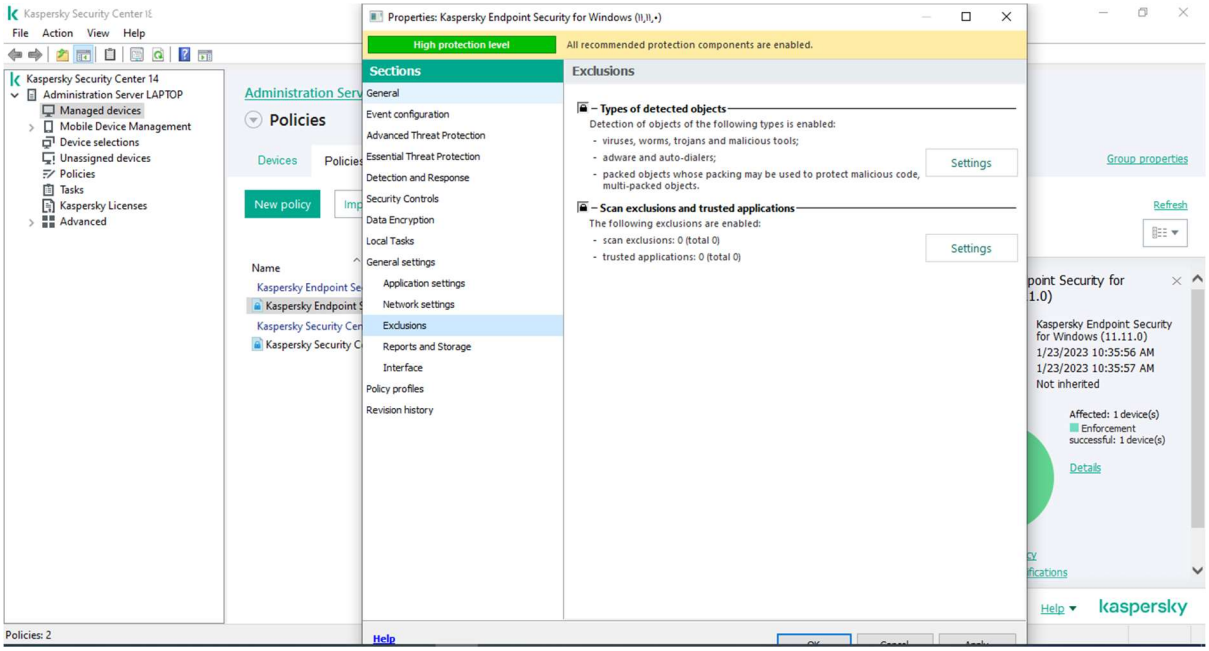


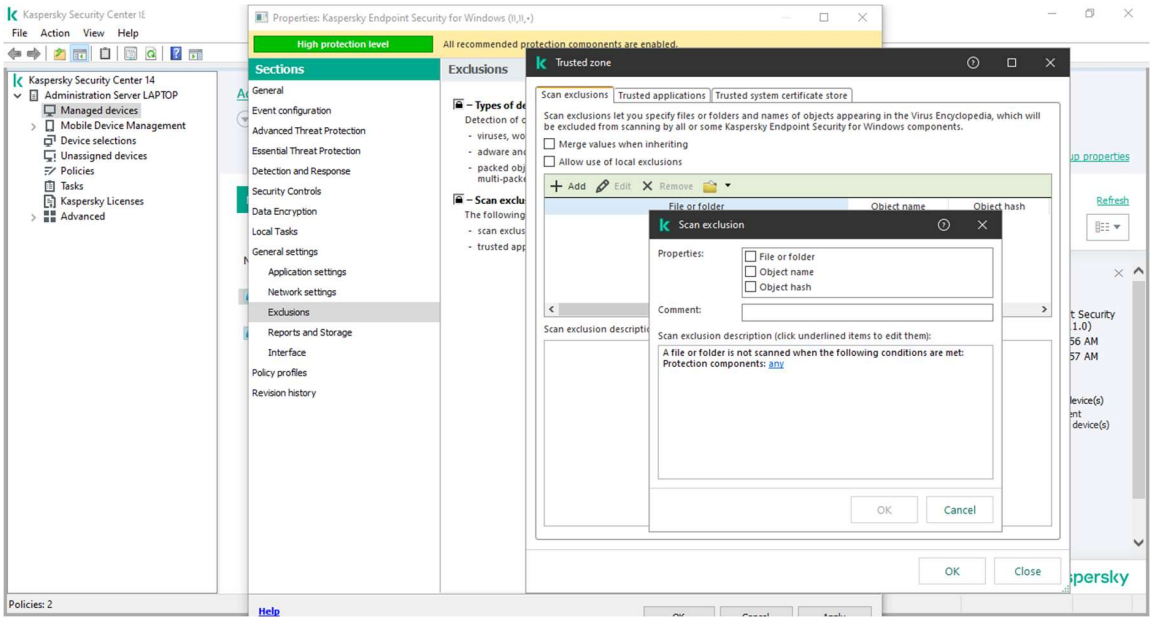
## Reports and storages

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




## General Protection Setting



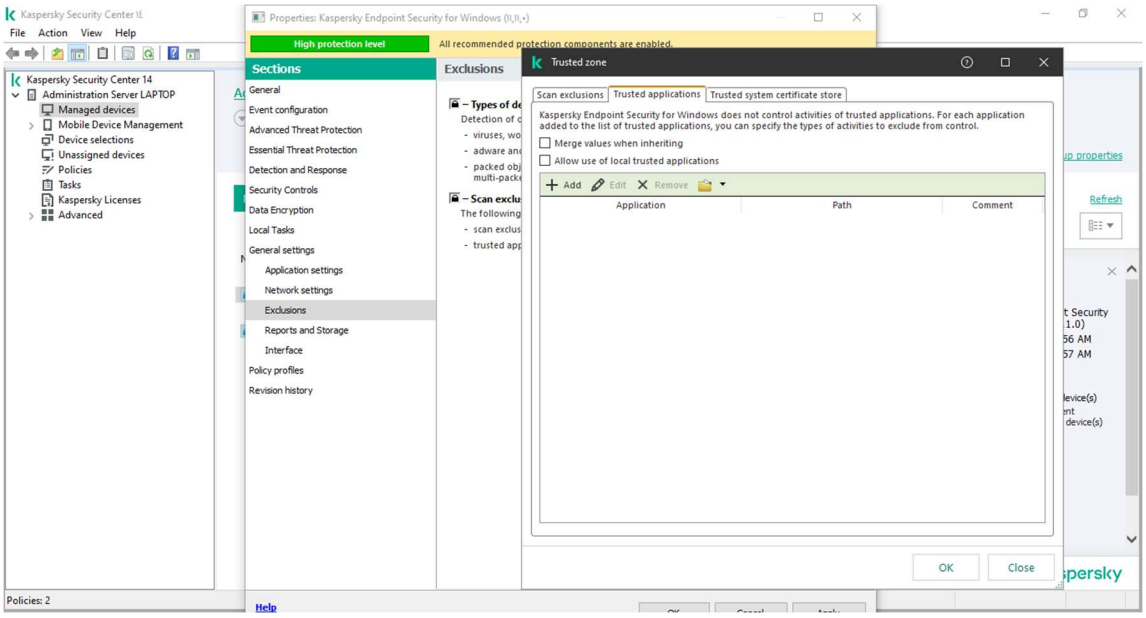



امکان بسیار خوبی که این Component در اختیار شما می گذارد این است که در قسمت Exclusions and trusted zone می توانید یک Application یا یک Folder را Exclude کنید که چه Component هایی از آنتی ویروس بر روی آن فعال نباشد(و یا حتی تمامیComponentهای آنتی ویروس بر روی آن غیر فعال باشد).

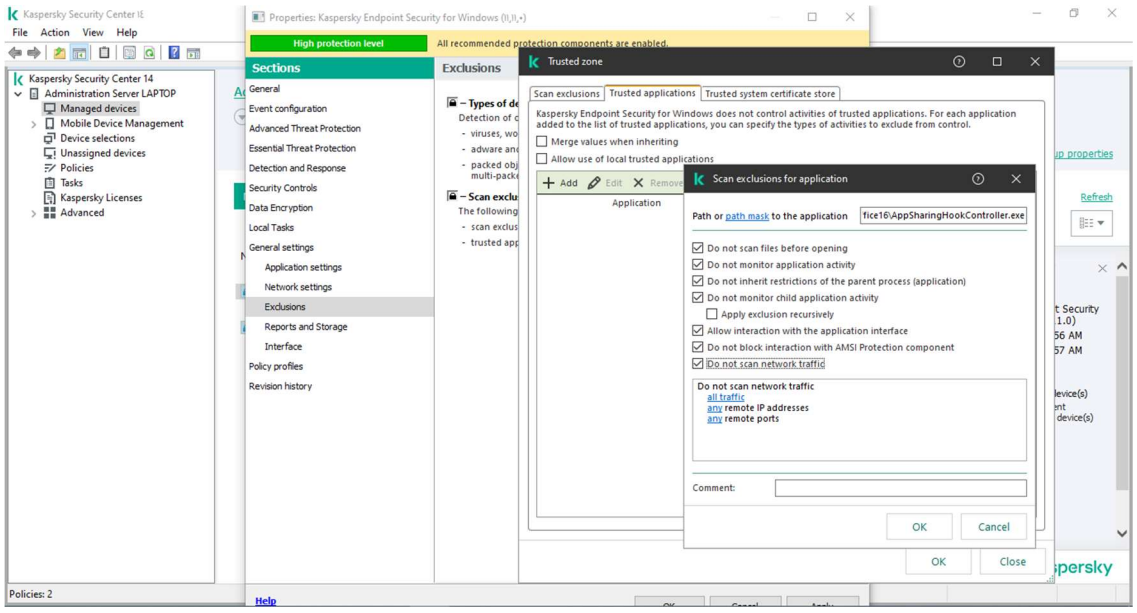
از این ویژگی زمانی استفاده می شودکه به طور مثال نرم افزاری که تحت شبکه کار می کند پس از نصب آنتی به کندی کار کند و یا به عنوان ویروس شناخته شود یا به نحوی جلوی یکسری فعالیت های آن گرفته شودو موجب شود قسمتی ازآن کار نکند.همچنین در مواردی که Crack های یک نرم افزار به عنوان ویروس شناخته می شود، از این ویژگی 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. با زدن تیک Do not منجر به عدم اسکن و عدم توجه آنتی ویروس کسپرسکی به آن اپلیکشن خواهد شد.




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.