

# آموزش کامل تصویری

**Kaspersky Internet SECURITY**

**2013**



تهیه شده توسط **HaD!e6z**

# فهرست

پیش‌گفتار:	۵
مقدمه:	۵
<b>نصب Kaspersky Internet Security 2013</b>	<b>۶</b>
اکتیو کردن بوسیله کلید (key)	۹
آپدیت آفلاین	۱۲
<b>معرفی مختصر پنجره اصلی Kaspersky Internet Security 2013</b>	<b>۱۷</b>
۱- فناوری ابری (Cloud Protection)	۱۸
۲- گزارشات (Reports)	۲۰
۳- تنظیمات (Settings)	۲۱
۴- اسکن (Scan)	۲۲
۵- بروزرسانی (Update)	۲۵
۶- پرداخت و خرید اینترنتی امن (Safe Money)	۲۶
۷- کنترل والدین (Parental Control)	۲۷
۸- برنامه های فعال (Application Activity)	۳۵
۹- نظارت بر شبکه (Network Monitor)	۳۶
۱۰- کیبورد مجازی (Virtual Keyboard)	۴۰
۱۱- قرنطینه (Quarantine)	۴۲
۱۲- ابزار (Toos)	۴۳
۱- دیسک نجات کسپرسکی (Kaspersky Rescue Disk)	۴۳
۲- عیب‌یابی ویندوز (Microsoft Windows Troubleshooting)	۵۱
۳- پاکسازی حریم خصوصی (Microsoft Windows Troubleshooting)	۵۴
۴- پیکربندی مرورگر (Browser Configuration)	۵۷
<b>تنظیمات Kaspersky Internet Security 2013</b>	<b>۶۰</b>
۱- سربرگ Protection Center	۶۰

۶۱.....	۱- تنظیمات عمومی (General Setting)
۶۳.....	۲- آنتی ویروس فایل (File Anti-Virus)
۶۸.....	۳- آنتی ویروس ایمیل (Mail Anti-Virus)
۷۲.....	۴- آنتی ویروس وب (Web Anti-Virus)
۸۰.....	۵- آنتی ویروس مسنجرها (IM Anti-Virus)
۸۱.....	۶- تنظیمات کنترل برنامه (Application Control Setting)
۸۹.....	۷- نگهبان (مراقب ، نظاره گر) سیستم (System Watcher)
۹۱.....	۸- فایروال (دیواره آتش) (Firewall)
۹۵.....	۹- مسدود کننده حملات شبکه ای (Network Attack Blocker)
۹۶.....	۱۰- ضد هرزنامه (Anti- Spam)
۱۰۰.....	۱۱- ضد تبلیغات (Anti-Banner)
۱۰۱.....	۱۲- پول امن (پرداخت و خرید اینترنتی امن) (Safe Money)
۱۰۳.....	۱۳- ورودی داده ها به صورت امن (Secure Data Input)
۱۰۶.....	۲- سربرگ Scan
۱۰۷.....	۱- تنظیمات عمومی (General Settings)
۱۰۹.....	۲- اسکن کامل (Full Scan)
۱۱۴.....	۳- اسکن قسمت‌های بحرانی (Critical Areas Scan)
۱۱۶.....	۴- اسکن سفارشی (Custom Scan)
۱۱۷.....	۵- اسکن آسیب پذیرها (Vulnerability Scan)
۱۱۸.....	۳- سربرگ Update
۱۲۱.....	۴- سربرگ Advanced Setting
۱۲۲.....	۱- تهدیدات و استثنائات (Threats and Exclusions)
۱۲۴.....	<b>اعتماد سازی یک فایل به Kaspersky Internet Security 2013</b>
۱۲۸.....	۲- دفاع از خود (Self-Defense)
۱۲۹.....	۳- صرفه جویی در باتری (Battery Saving)
۱۳۰.....	۴- سازگاری (Compatibility)
۱۳۱.....	۵- شبکه (Network)

۱۳۲.....	۶- اطلاع رسانی ها (Notifications)
۱۳۳ .....	۷- گزارشات و قرنطینه (Reports and Quarantine)
۱۳۴.....	۸- بازخورد (Feedback)
۱۳۵.....	۹- مشخصات بازی (Gaming Profile)
۱۳۶.....	۱۰- نمایش (Appearance)
۱۳۷.....	۱۱- کنترل والدین (Parental Control)
۱۳۸ .....	۱۲- مدیریت تنظیمات (Manage Settings)
۱۴۱.....	<b>آموزش قابلیت‌های موجود در Kaspersky Pure 3</b>
۱۴۲.....	پشتیبان گیری از اطلاعات (Backup)
۱۴۶ .....	Restore data
۱۴۷.....	Data Encryption



## پیش گفتار:

سلام خدمت همه عزیزانی که این فایل آموزشی رو دانلود میکنند .  
بدلیل اینکه **Kaspersky** یکی از پرطرفدارترین آنتی ویروسها در ایران هستش و هیچ منبع آموزشی فارسی جامع برای اون در دسترس نیست، در این فایل آموزشی قصد دارم آموزش کامل تصویری **Kaspersky Internet Security 2013** رو تهیه کنم. قسمت آخر آموزش که امکانات اضافه نسخه **PURE** رو دوست خوبم نیما (**Nima Zapata**) زحمتشو کشیده که براتون ضمیمه آموزش اصلی کردم.

**امیدوارم که مطالب عنوان شده برای تمامی عزیزان مفید واقع بشه.**

در صورت وجود مشکل ، آن را در انجمن مطرح نمائید. (<http://forum.soft98.ir>)

**برقرار و سبز باشید.**

**مرداد ۹۲**

## مقدمه:

کاسپرسکی با نام کامل **لابراتوار کاسپرسکی** (به روسی **Лаборатория Касперского**) شرکتی روسی که در زمینه امنیت کامپیوتر فعال است و محصولات با نامهای ضد ویروس کاسپرسکی آنتی ویروس و آنتی ویروس موبایل را میسازد. این شرکت در سال ۱۹۹۷ توسط **ناتالیا و یوگنی کاسپرسکی** به وجود آمد. دفتر اصلی آن در مسکو در روسیه است و در بریتانیا، فرانسه، آلمان، هلند، لهستان، رومانی، ژاپن، چین، کره جنوبی و آمریکا... نمایندگی دارد. یکی از محصولات پرطرفدار آن **Kaspersky Internet Security 2013** می باشد. اینترنت سکوریتی یکی از قدرتمندترین نرم افزارها امنیتی است که با نصب آن بر روی سیستم محافظت کامل سیستم شما در زمانی که در اینترنت به سر می برید به صورت کامل فراهم می کند. این برنامه قادر است تا مانع نفوذ هکرها به داخل سیستم شما شود و با شیوه های مختلف راه نفوذ آنها را ببندد. همچنین دارا بودن یک دیواره آتش بسیار قوی در این برنامه سبب می شود تا علاوه بر دفع حملات هکرها و فایل های مخرب، تمام اتصالات شبکه و رفت و آمد های اینترنتی شما کنترل شود تا اگر فایل مخربی قصد نفوذ و یا اجرا از طریق نرم افزار مرورگر سیستم را داشت نابود گردد. یکی دیگر از ویژگی های این برنامه قابلیت اسکن اتوماتیک هارد برای شناسایی و حذف ویروس ها و دیگر بد افزارها می باشد. با آپدیت روزانه این اینترنت سکوریتی و دریافت جدیدترین اطلاعات در رابطه با ویروس های جدید از شرکت سازنده، میتوانید نرم افزار امنیتی سیستم خود را در بالاترین حد امنیتی قرار دهید.

کاسپرسکی اینترنت سکوریتی ۲۰۱۳ کاملاً با آخرین نسخه سیستم عامل میکروسافت، ویندوز ۸ سازگار است و با آخرین ابداعات امنیتی میکروسافت یکپارچه شده است.

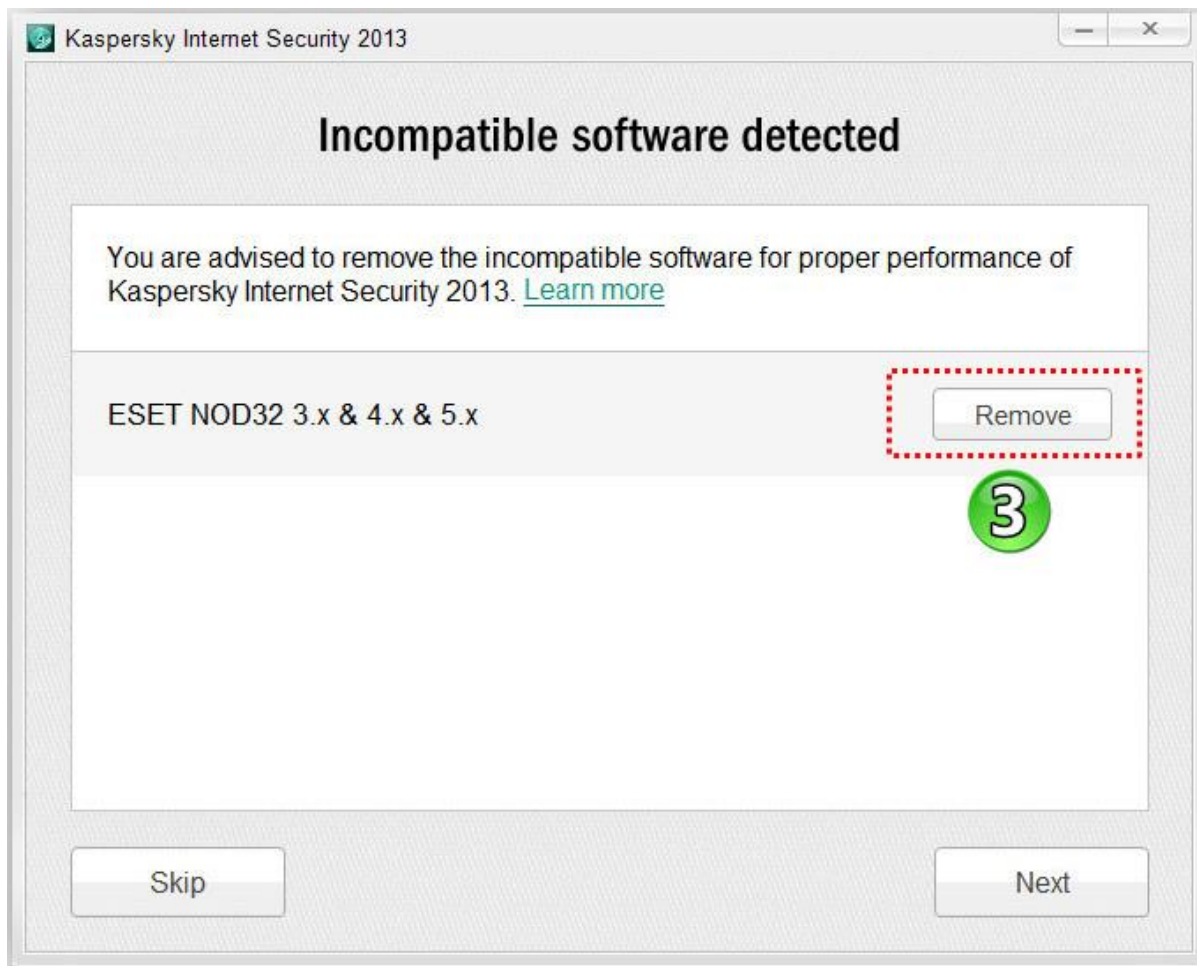
## نصب Kaspersky Internet Security 2013

**نکته:** در طول نصب و معرفی کلید به آنتی ویروس اینترنت خود را قطع کنید چون بعضی از مواقع باعث باطل شدن کلیدها میشود.

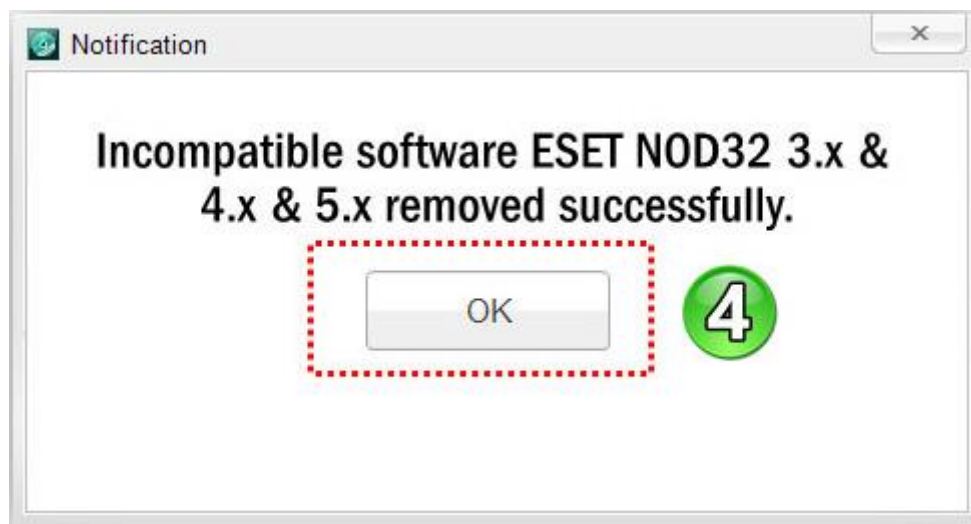
ابتدا بر روی فایل setup.exe کلیک کنید و بقیه مراحل را طبق اسکرین شاتها ادامه دهید.



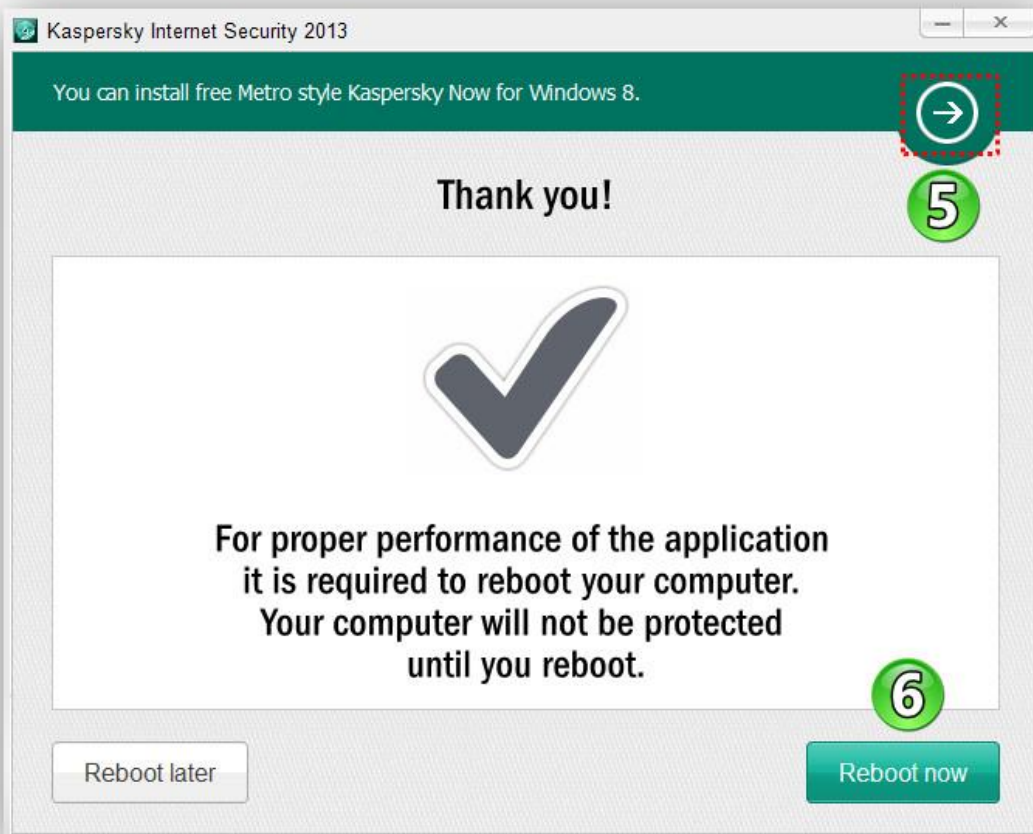
در صورتی که آنتی ویروس نصب دارین ابتدا اونو حذف کنین که در اینجا من ESET SMART SECURITY 6 رو نصب دارم و در مرحله نصب آنتی ویروس همیشه اونو حذف کرد یا کاری به کارش نداشت ولی بهتره برای جلوگیری از تداخل آنتی ویروسها، آنتی ویروس قبلی رو حذف کرد.



بعد از حذف آنتی ویروس پیغامی مبنی بر موفقیت آمیز بودن حذف آنتی ویروس قبلی داده میشود که ok نموده و Next بزنید و بعد از آن از شما درخواست Reboot شدن کامپیوتر را میکنند(در صورتی ک آنتی ویروس قبلی رو در مراحل نصب Kaspersky ، حذف کنید نیاز به Reboot میشود.



بعد از ریستارت ادامه نصب بصورت اتوماتیک آغاز میشود.  
بعد از اتمام نصب آنتی ویروس دوباره درخواست ریستارت مجدد میکنند(البته میتوان Reboot شدن سیستم را به بعدا موکول کرد).



در شماره ۵ چون من ویندوز ۸ نصب دارم پیشنهاد Metro Style به من می‌ده که اگه من قبول کنم به صفحه STORE هدایت میشم که فعلا من از این کار اجتناب میکنم. بعد از ریستارت سیستم و بالا آمدن آنتی ویرس نوبت به فعال سازی آنتی ویرس میرسد. بدلیل اینکه آپدیت اولیه دارای حجم زیادی میباشد(البته برای ما ک نت ذغالی داریم) بهتره که اول آنتی ویرس بصورت آفلاین آپدیت بشه و بعدا آپدیت آنلاینش بکنیم.

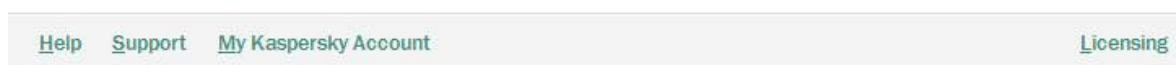


### Application is not activated

Preset activation code is available. The application will be activated as soon as Internet connection is available.



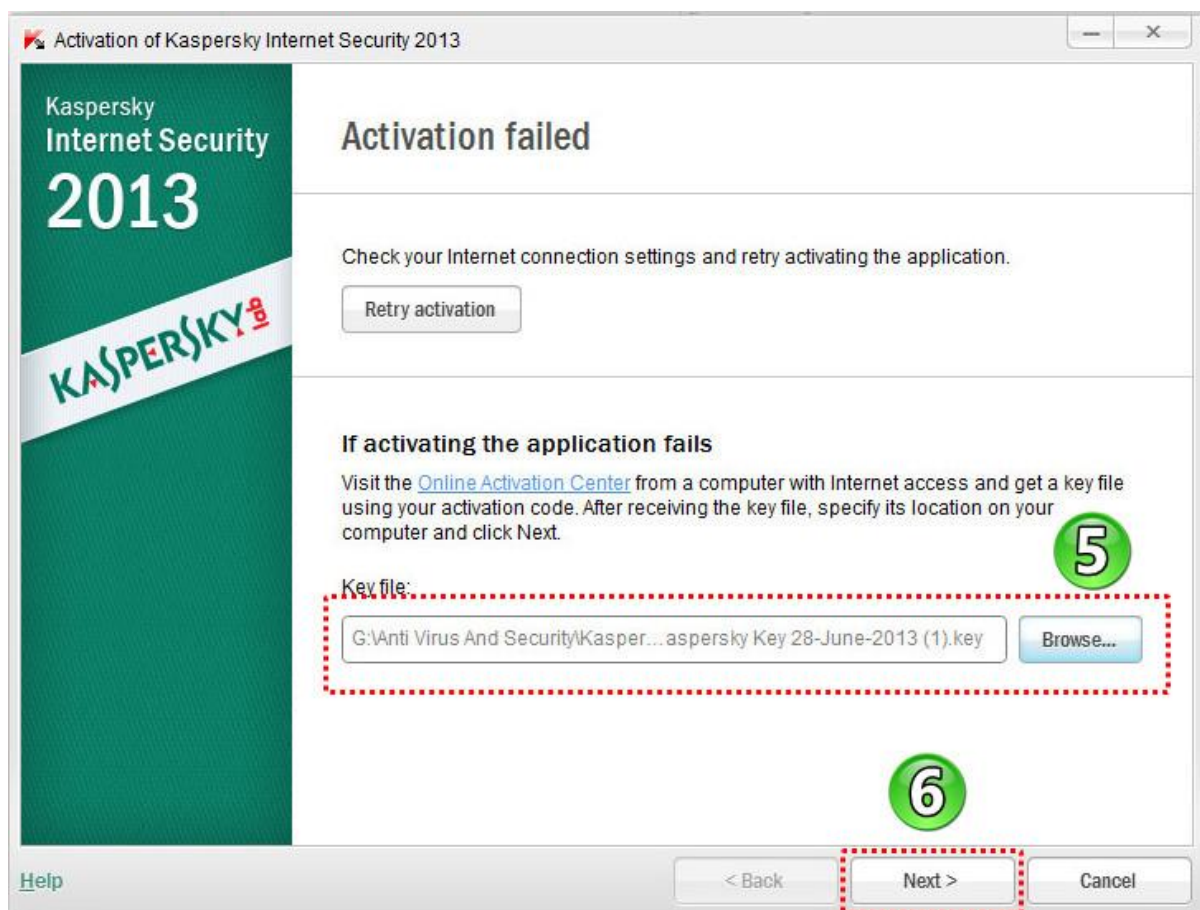
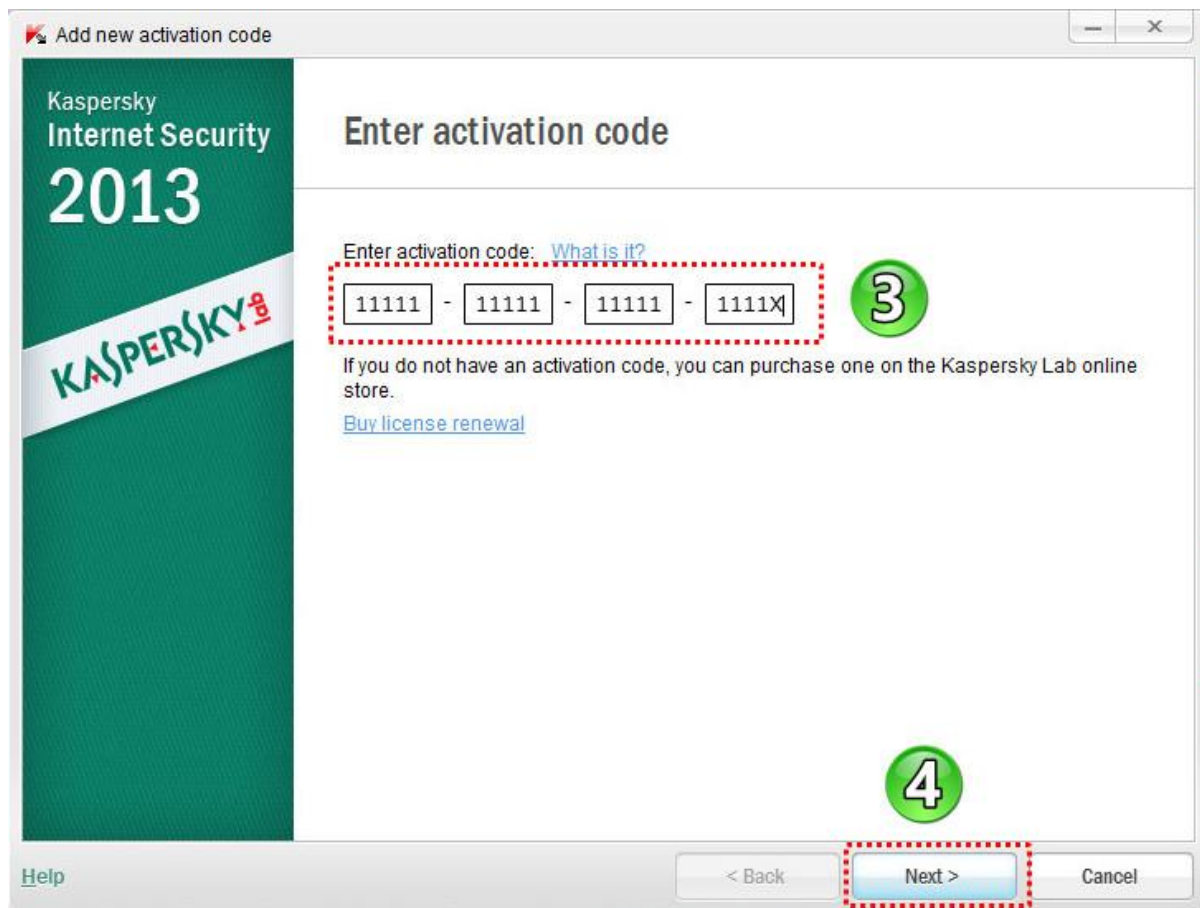
2





از سریال زیر استفاده نموده و بر روی دکمه Next کلیک نمایید:

Activation Vode: 11111-11111-11111-1111X



Kaspersky  
Internet Security  
2013

KASPERSKY

Thank you



Activation completed successfully



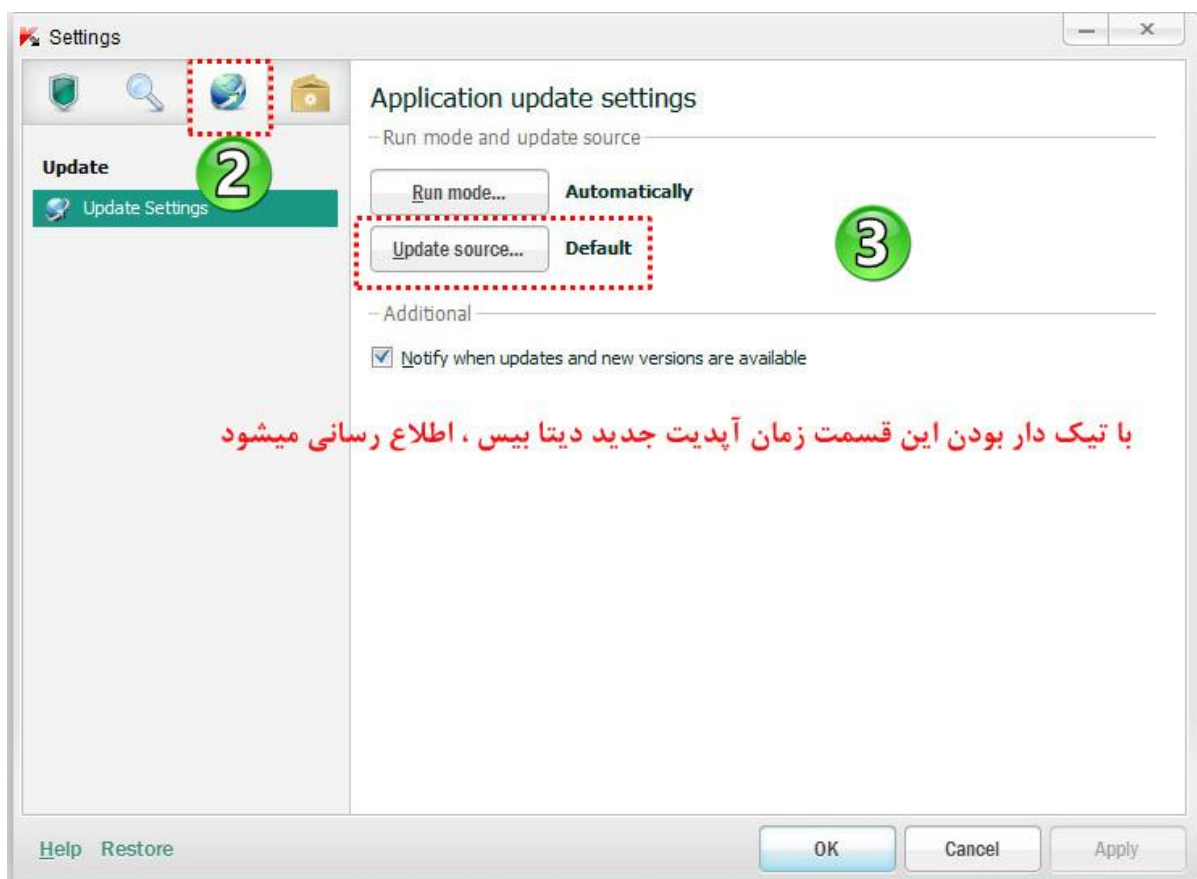
< Back

Finish

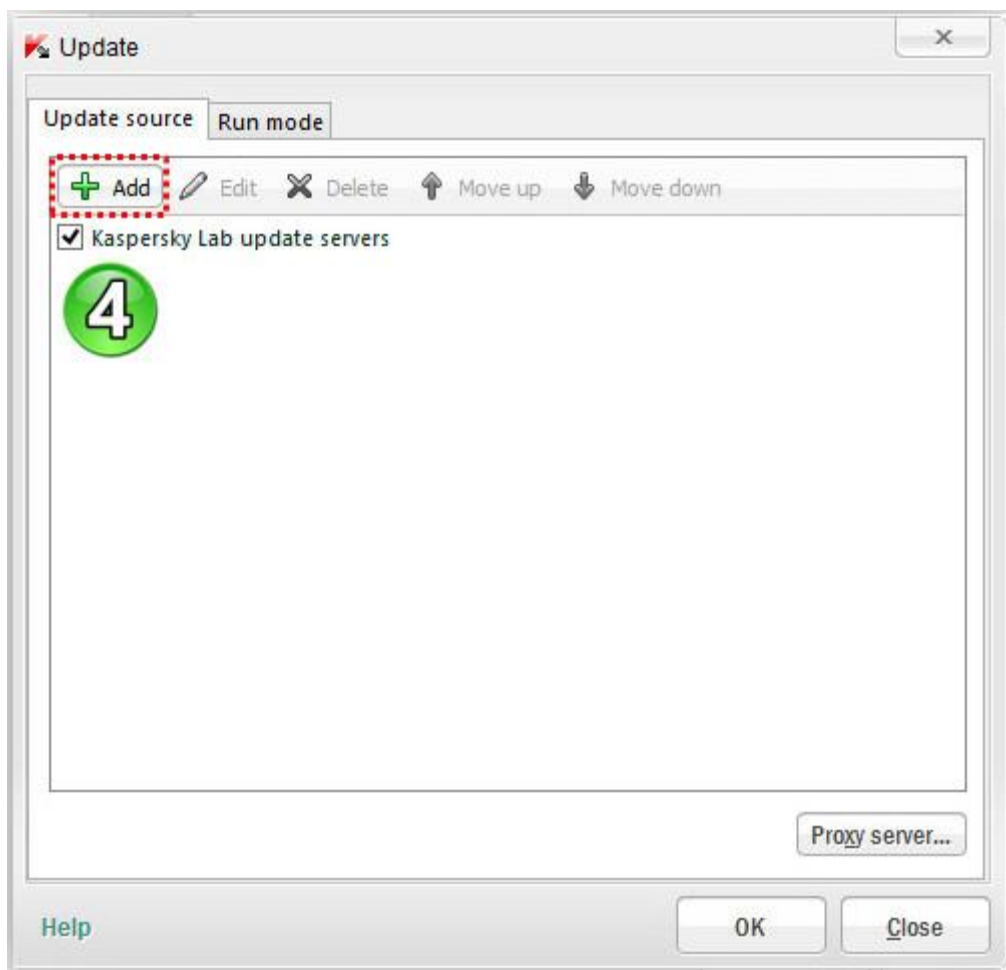
Cancel

## آپدیت آفلاین

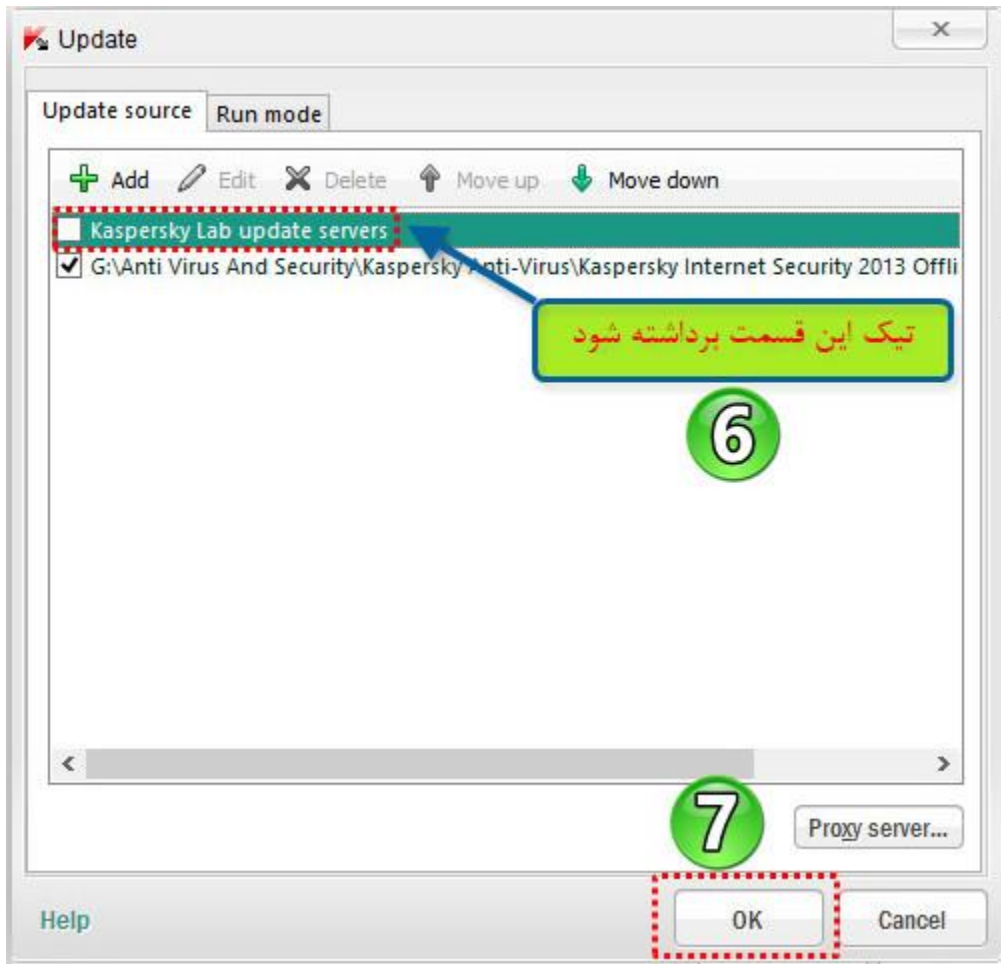
برای آپدیت آفلاین طبق اسکرین شاتها عمل نمایید.








**توجه:** در مرحله بعد باید تیک مربوط به server آپدیت آنلاین Kaspersky برداشته شود.




KASPERSKY  INTERNET SECURITY 2013

Cloud protection


Reports Settings


Back Update

 **Databases and the application are obsolete**

By default, Kaspersky Internet Security regularly checks for updates, and will automatically download and install new database signatures. You can also run an update manually at any time.


Last update: [unknown](#)  
Signatures: 7,644,486  
Run mode: [automatically](#)

Run update 



[Virus activity review](#)


Help Support [My Kaspersky Account](#) [Licensing](#)

KASPERSKY  INTERNET SECURITY 2013

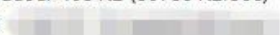
Cloud protection

Reports Settings

Back Update

 **Updating databases and application (15%)...**

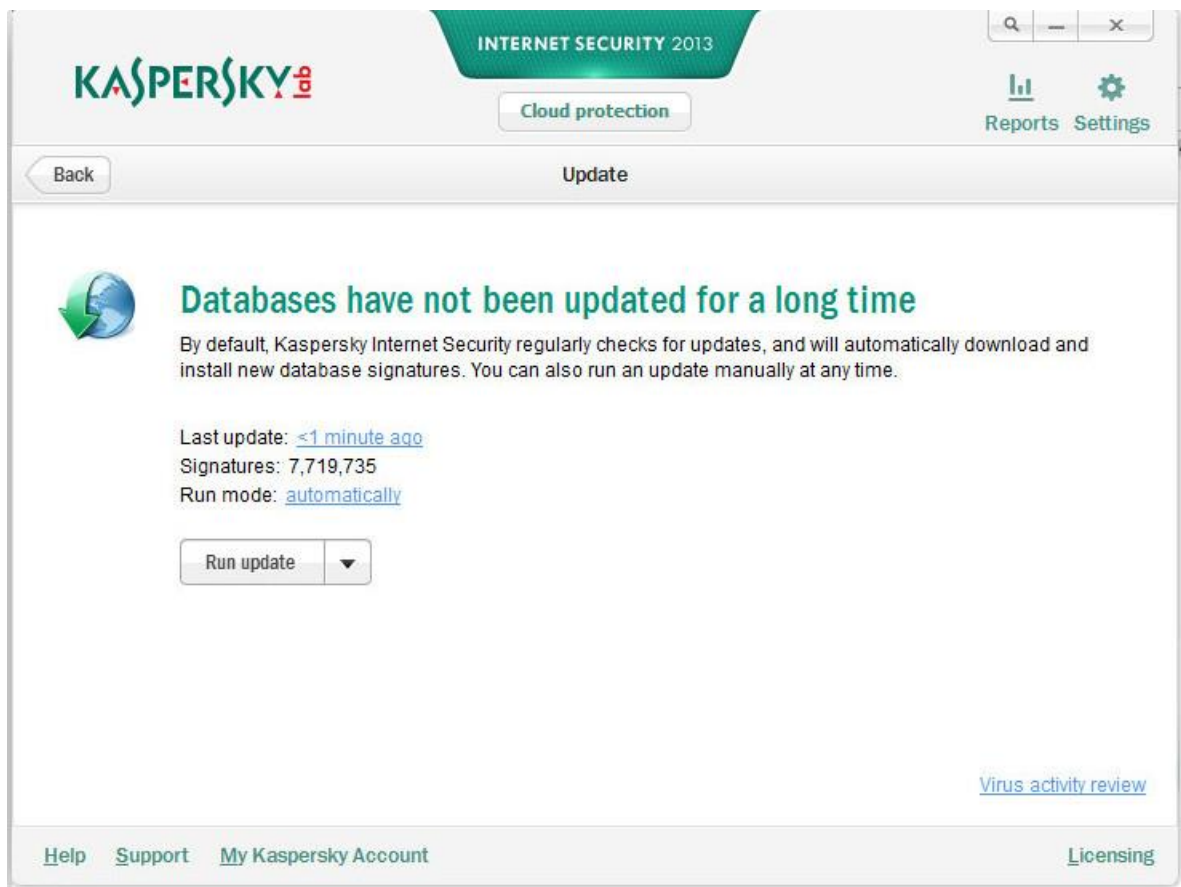
By default, Kaspersky Internet Security regularly checks for updates, and will automatically download and install new database signatures. You can also run an update manually at any time.

Status: processing files  
Downloaded: 403 KB (80789 KB/sec)  
Source: 

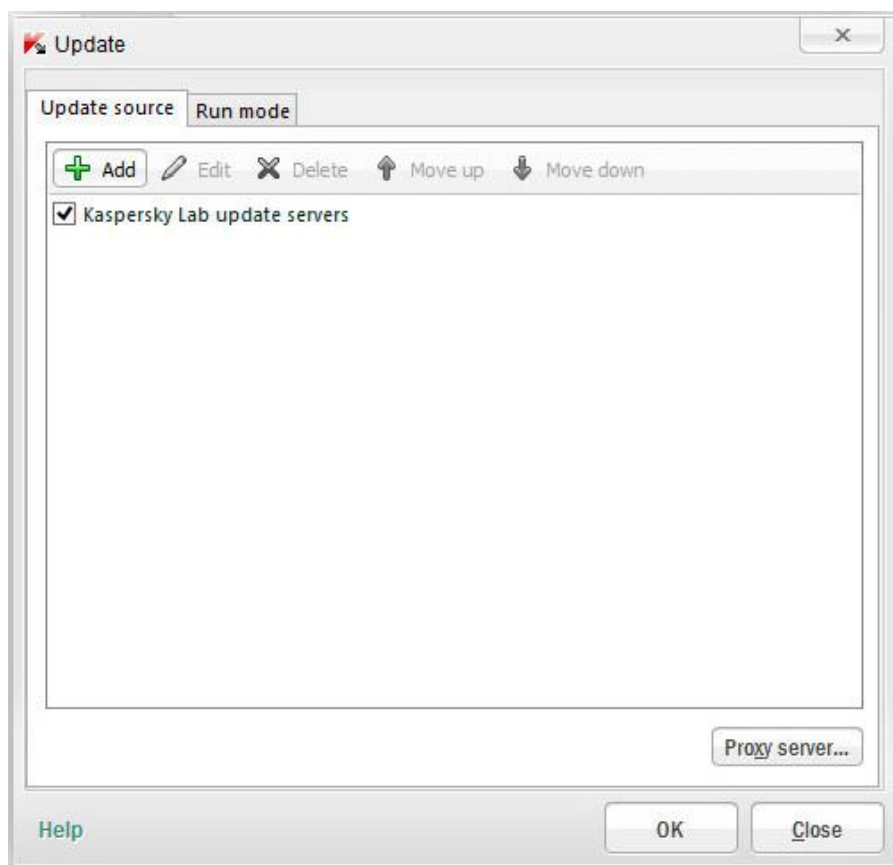
Stop

[Virus activity review](#)

Help Support [My Kaspersky Account](#) [Licensing](#)



**توجه:** بعد از اتمام آپدیت آفلاین تنظیمات رو به حالت اولیه برگردونید و یک بار هم آنلاین اقدام به آپدیت نمایید.





# معرفی مختصر پنجره اصلی Kaspersky Internet Security 2013

The image displays the main interface of Kaspersky Internet Security 2013, divided into two sections. The top section shows the 'Computer is protected' status with a checklist of security features. The bottom section shows a grid of 13 numbered icons representing different security tools, each with a Persian translation.

**Top Section: Computer is protected**

- 1** Cloud protection: فناوری حفاظت ابری
- 2** Reports: گزارشات
- 3** Settings: تنظیمات

**Computer is protected**

- ✓ Threats: none
- ✓ Protection components: main enabled
- ✓ Databases: up to date
- ✓ License: 192 days remaining

**Bottom Section: Security Tools**

- 4** Scan: اسکن
- 5** Update: بروزرسانی
- 6** Safe Money: پرداخت و خرید اینترنتی امن
- 7** Parental Control: کنترل والدین
- 8** Applications Activity: برنامه های فعال
- 9** Network Monitor: مانیتورینگ شبکه
- 10** Virtual Keyboard: کیبورد مجازی
- 11** Quarantine: قرنطینه
- 12** Tools: ابزار
- 13** Licensing: لایسنس

## ۱- فناوری ابری ( Cloud Protection )

برنامه های آنتی ویروس استاندارد حداقل ۴ ساعت برای جلوگیری از (شناسایی و ثبت به پایگاه داده در امضا) بیشتر از ۳۵,۰۰۰ برنامه مخرب که هر روز ظهور میکند ، نیاز دارند. برای حصول اطمینان از سرعت و حفاظت موثر در برابر آخرین تهدیدات روشهای فعال جایگزین و فن آوری های ابری علاوه بر امضاء سنتی، مورد نیاز هست. کارشناسان آزمایشگاه کسپرسکی با حفاظت "هیبرید" که ترکیبی از ابزارهای ضد تروجان سنتی با فن آوری ابری آمده اند. این فن آوری حفاظت ابری بر اساس داده های جمع آوری شده در چارچوب شبکه امنیت کسپرسکی میباشد.

شبکه امنیت کسپرسکی (KSN) برای میلیون ها نفر از کاربران در سراسر جهان ، شناسایی تهدیدات جدید، تعیین اعتبار برنامه ها و وب سایت را به سرعت به ارمغان می آورد. در صورت موافقت شما، اطلاعات مورد تلاش کننده(منظور همان ویروس ، تروجان ، کرم و ... میباشد) برای آلوده کردن کامپیوتر شما و فعالیت های برنامه مشکوک به لابراتوار کسپرسکی فرستاده میشود. این اطلاعات بلافاصله توسط سیستم تخصصی و خودکار پردازش شده و تنها در ۴۰ ثانیه داده ها در تهدیدهای نوظهور قرار گرفته و منابع خود را در دسترس برای استفاده تمام کاربران محصولات لابراتوار کسپرسکی قرار میدهند .

### فن آوری های ابری (KSN) :

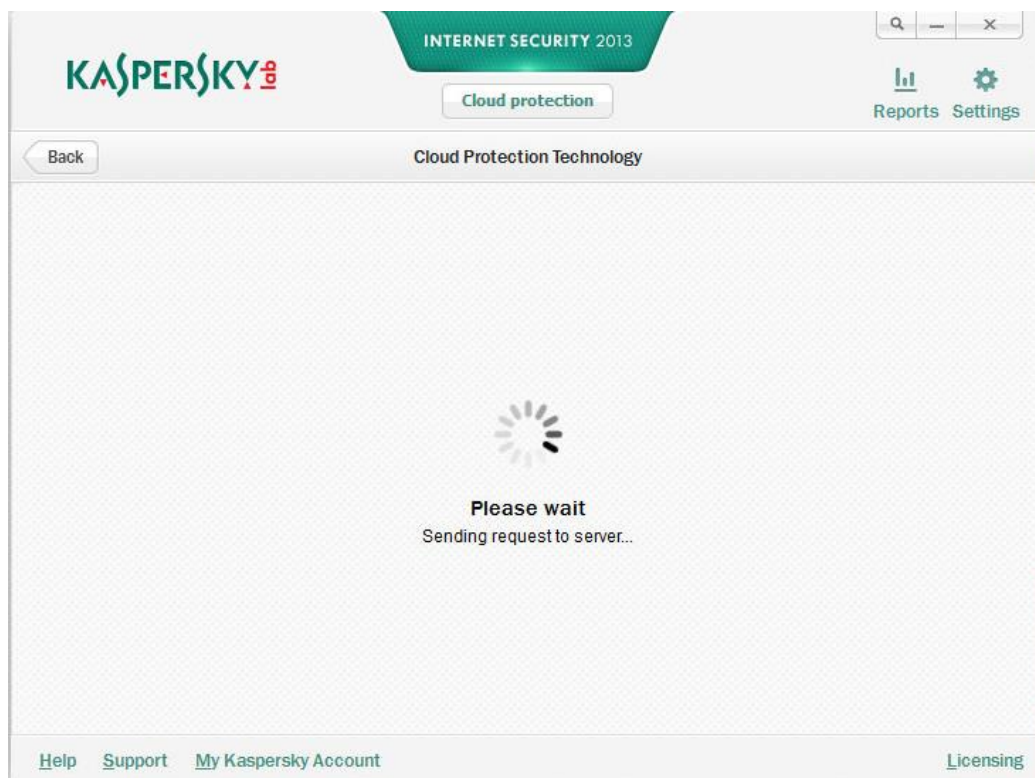
حفاظت در برابر آخرین تهدیدات فراهم می کند .

فضای رایگان بر روی دیسک سخت، به عنوان پایگاه داده های ابری بر روی کامپیوتر شما ذخیره می شود.

کاهش ترافیک در هنگام به روز رسانی پایگاه داده های آنتی ویروس

بهبود عملکرد کامپیوتر: ابر مبتنی بر اطلاعات به معنی بدون نیاز به تجزیه و تحلیل تمام فعالیت های نرم افزار است.

در پنجره اصلی Kaspersky Internet Security 2013 با کلیک بر روی دکمه cloud protection میتوانید به حفاظت ابر دسترسی پیدا کنید. این پنجره شامل اطلاعات مربوط به امنیت کار شبکه کسپرسکی میشود و این اجازه را به شما می دهد تا به مشاهده و بهره مندی از فن آوری های حفاظت ابری شوید.



۱- در قسمت سمت چپ پنجره فناوری حفاظت ابری، خواهید دید که شبکه امنیت کسپرسکی فعال است.

۲- آمار فعلی شبکه امنیت کسپرسکی KSN در ۲۴ ساعت گذشته

**Safe data** : اطلاعات امن

**Dangerous data** : اطلاعات خطرناک

**Processing** : مواردی که بر روی سرورهای لابراتوار کسپرسکی در حال پردازش میباشند.

**Protected KSN participants** : تعداد کاربران حفاظت شده توسط KSN در ۲۴ ساعت گذشته

**threats neutralized** : تهدیدات خنثی شده در ۲۴ ساعت گذشته

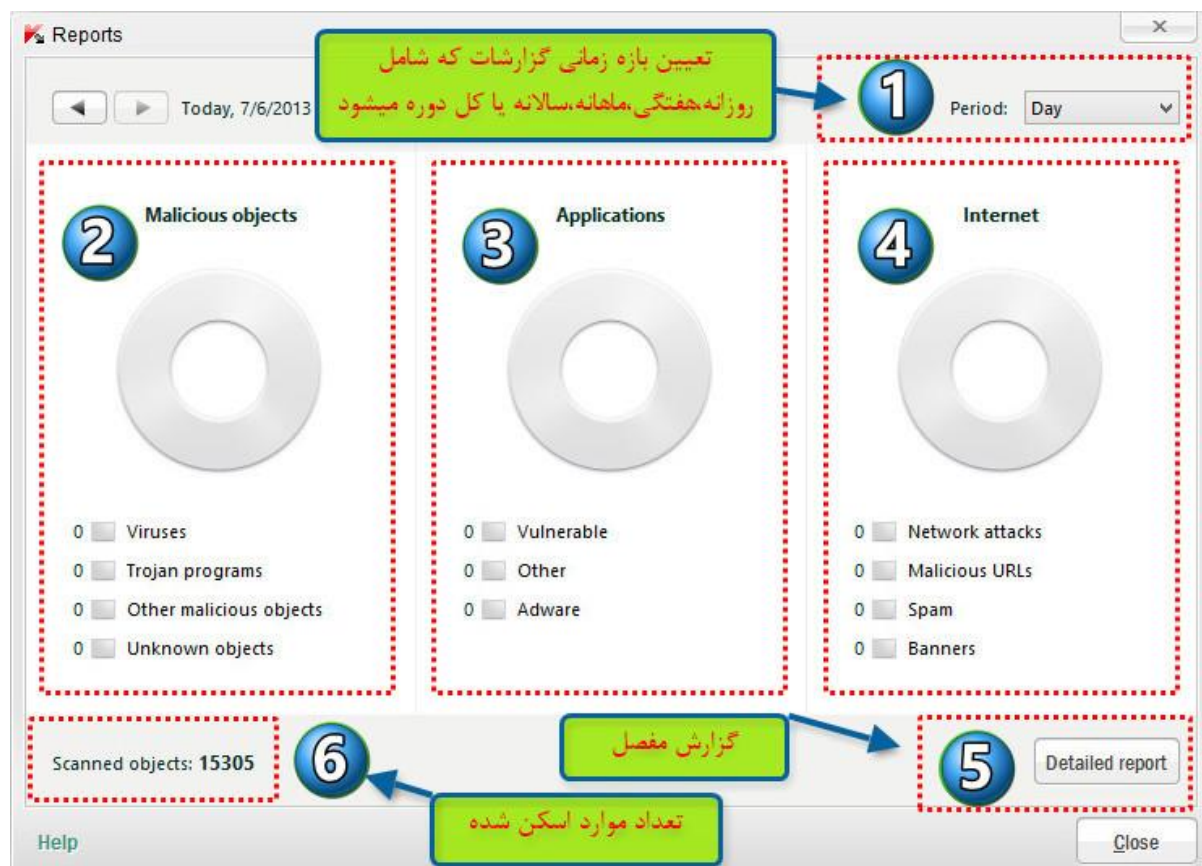
شبکه امنیت کسپرسکی به دلایل زیر میتواند قطع باشد:

اتصال به اینترنت برقرار نیست. اتصال اینترنت خود را با باز کردن وب سایت رسمی کسپرسکی در مرورگر خود تست کنید.  
در شبکه امنیت کسپرسکی شرکت ندارید. در مورد چگونگی فعال کردن / غیر فعال کردن مشارکت در شبکه امنیت کسپرسکی می توانید دستورالعمل و اطلاعاتی دقیق در KB6635 پیدا کنید.



## ۲- گزارشات ( Reports )

Kaspersky Internet Security گزارش عملکرد هر یک از اجزای حفاظت را نگه میدارد. با استفاده از گزارش، شما می‌توانید اطلاعات آماری در مورد عملکرد برنامه‌ها بدست آورید. (برای مثال، یاد ببینید که چگونه بسیاری از موارد مخرب، تشخیص داده شده است و برای یک دوره زمانی مشخص خنثی شده است و برای همان دوره زمانی چند بار برنامه به روز رسانی شده است و اینکه چگونه بسیاری از پیام‌های هرزنامه تشخیص داده شده است و موارد دیگر از این قبیل)



موارد ۱ و ۵ و ۶ در تصویر توضیح داده شده است. بقیه موارد در زیر توضیح داده خواهد شد.

- ۲- موارد مخرب (Malicious): که شامل ویروسها، برنامه‌های تروجان، موارد مخرب دیگر و موارد ناشناخته میشود.
- ۳- برنامه‌ها (Applications): که شامل برنامه‌های آسیب پذیر (در معرض خطر)، دیگر و ابزارهای تبلیغاتی مزاحم میشود.
- ۴- گزارشات اینترنت (Internet): تعداد حملات شبکه، URLهای مخرب، ایمیل‌های ناخواسته (هرزنامه‌ها) و آگهی‌ها توسط برنامه در طول دوره زمانی انتخاب شده از فعالیت‌های اینترنتی کاربر را تشخیص میدهد.



## ۵- گزارش مفصل ( Detailed report ) :

The screenshot shows the 'Detailed report' window in Windows Security Center. The left sidebar lists components like File Anti-Virus, Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Application Control, System Watcher, Firewall, Network Attack Blocker, Anti-Spam, and Anti-Banner. The 'Update' component is selected and highlighted in green. The main pane shows a table of update events for 'Today, 7/6/2013' with a period of 'Day'. The table has columns for Event, Object, and Time. Four update events are listed, each with a plus icon to expand details. A red dashed box highlights the table area. A blue arrow points from the 'Update' component in the sidebar to the table. A green box with Persian text 'ذخیره کردن گزارشات' (Save reports) has an arrow pointing to the 'Save...' button at the bottom. A red Persian text overlay reads 'گزارش مفصل کلیه قسمتها برای اطلاع از جزئیات بیشتر' (Detailed report of all parts for more details).

Event	Object	Time
+ Update: completed 6 hours ago, updates size: 445.6 KB, average speed: 14 KB/sec (154)		
+ Update: completed 4 hours ago, updates size: 252 KB, average speed: 12 KB/sec (117)		
+ Update: completed 2 hours ago, updates size: 78.6 KB, average speed: 5 KB/sec (56)		
+ Update: completed 2 minutes ago, updates size: 92.7 KB, average speed: 1 KB/sec (78)		

Group: Update  
Events: 154

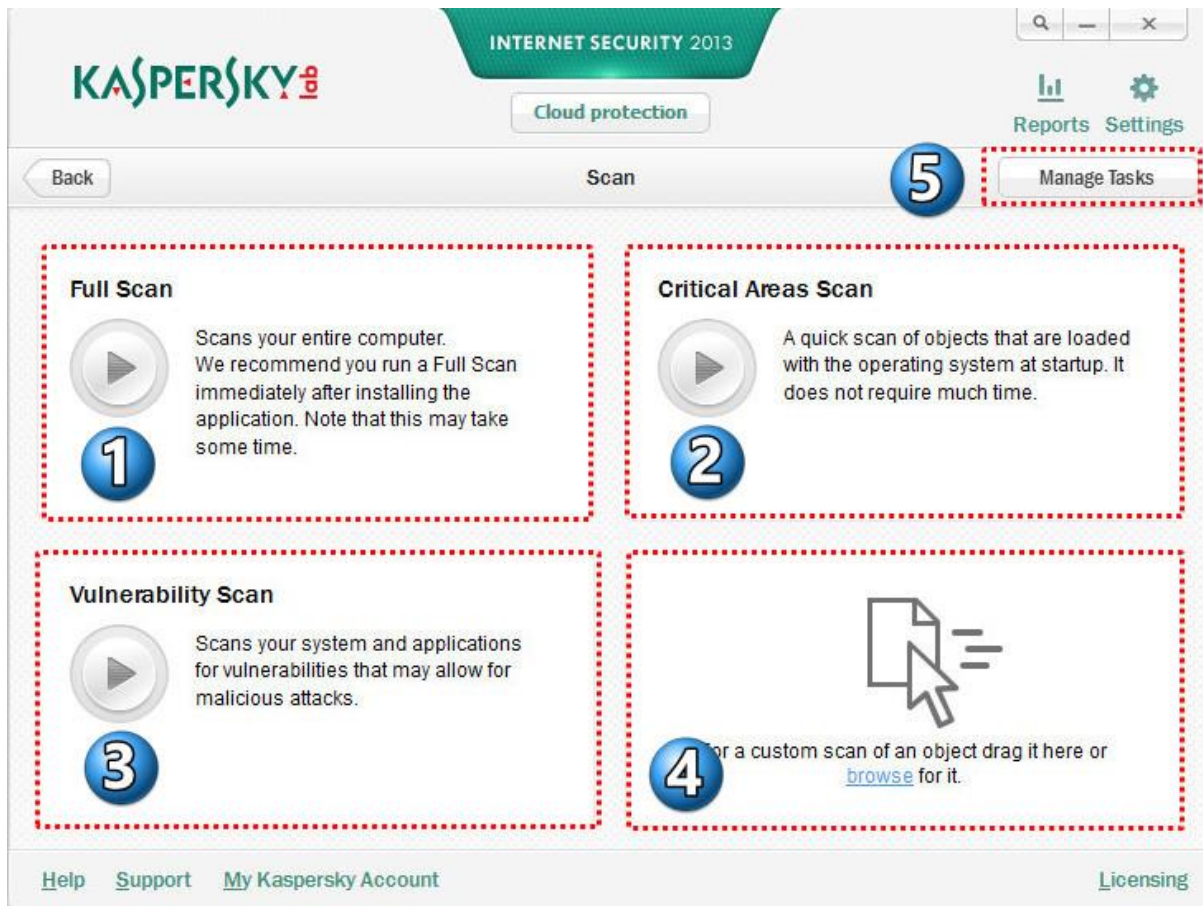
Help Save... Close

## ۳- تنظیمات ( Settings )

قسمت تنظیمات رو فعلا توضیح نمیدم چون خیلی زیاده ولی در قسمتهای بعدی بصورت کاملا مفصل و جزء به جزء بهش میپردازیم.

## ۴- اسکن ( Scan )

گزینه های قسمت اسکن طبق شماره گذاری توضیح داده میشود.



۱- اسکن کامل ( Full Scan ) : در طول یک اسکن کامل، Kaspersky Internet Security موارد زیر را به طور پیش

فرض اسکن میکند :

۱- حافظه سیستم

۲- مواردی که در هنگام راه اندازی سیستم عامل بارگذاری می شود ( startup سیستم عامل )

۳- پشتیبان سیستم

۴- هارد درایو و درایوهای removable (فلش ، هاردهای اکسترنال ، مموری کارت و ...)

توصیه میشود بلافاصله بعد از نصب Kaspersky Internet Security بر روی کامپیوتر یک اسکن کامل انجام بگیرد.

برای شروع یک اسکن کامل در این پنجره برنامه روی دکمه  کلیک کنید.

۲- اسکن مناطق بحرانی ( Critical Areas Scan ) : اسکن مناطق بحرانی به معنای اسکن موارد زیر است

۱- حافظه سیستم

۲- مواردی که در هنگام راه اندازی سیستم عامل بارگذاری می شود ( startup سیستم عامل )

۳- بوت سکتورهای دیسک ( boot sectors )

برای شروع یک اسکن کامل در این پنجره برنامه روی دکمه  کلیک کنید.

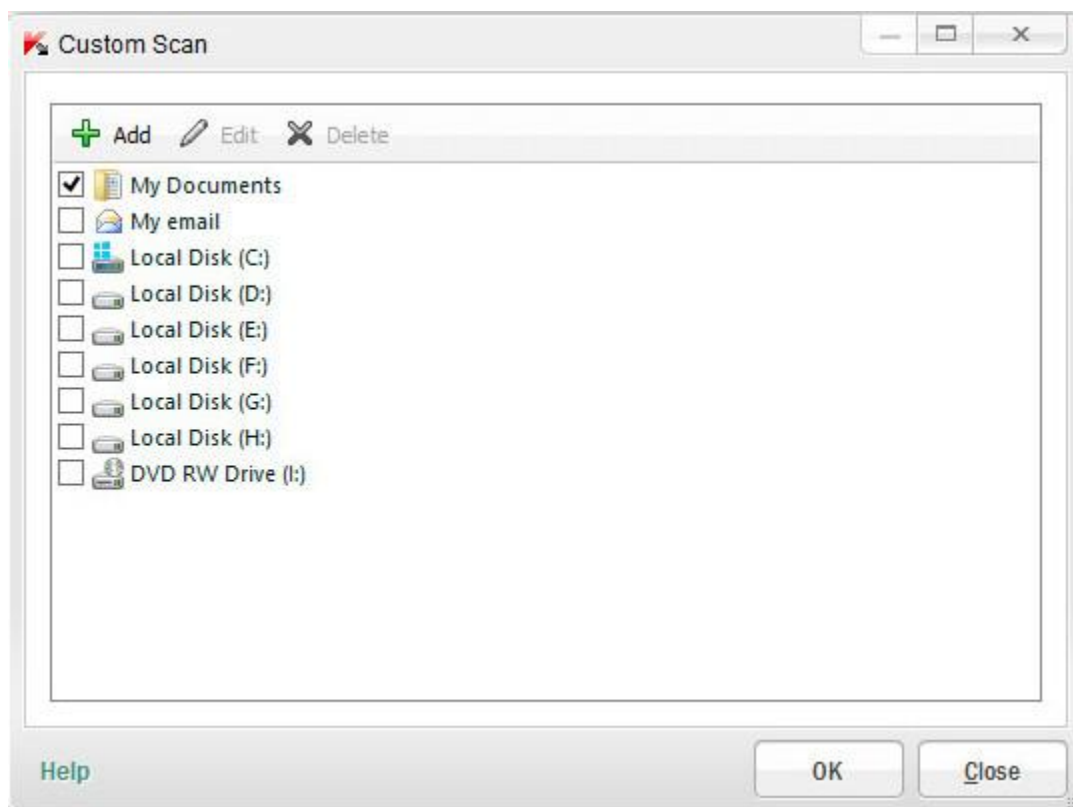
۳- اسکن آسیب پذیری ( **Vulnerability Scan** ) : آسیب پذیریها در بخش های محافظت نشده از کد نرم افزار هستند که مزاحمان ممکن است عمداً برای اهداف خود از آنها استفاده کنند. با کلیک بر روی این گزینه سیستم و برنامه های شما را از آسیب پذیریهایی که ممکن است برای حملات مخرب اجازه دهد ، اسکن میکند و یک لیست از آسیب پذیری سیستم تشخیص داده و برنامه های کاربردی آسیب پذیر را نمایش می دهد .

برای شروع یک اسکن کامل در این پنجره برنامه روی دکمه  کلیک کنید.

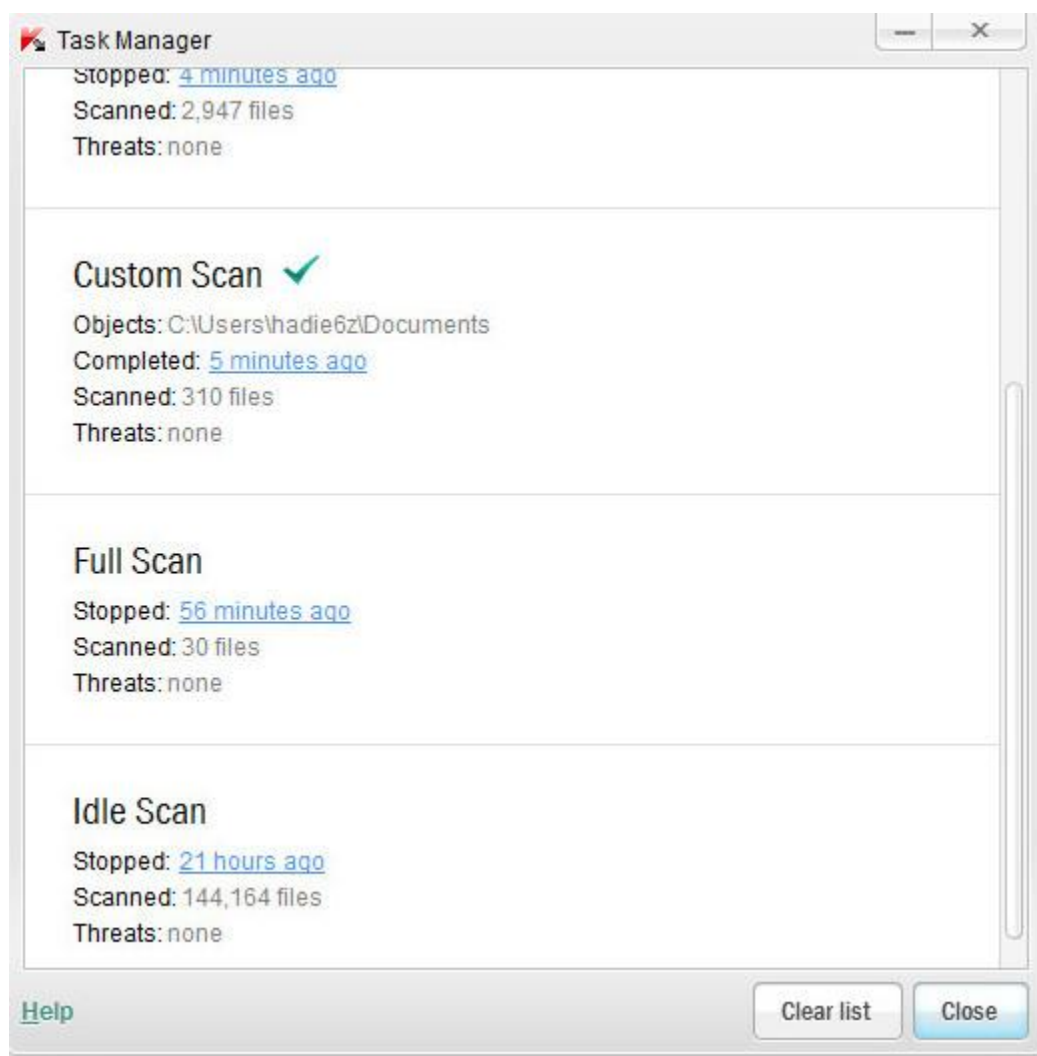
۴- اسکن سفارشی ( **Custom Scan** ) : بخش اسکن سفارشی (بدون هدر) برای شروع اسکن سفارشی از پوشه ها و فایل ها طراحی شده است .

برای اسکن یک فایل یا پوشه باید موارد که میخواهیم اسکن شود رو داخل اونجا **Drage** کنیم یا اینکه روی لینک **browse** باید کلیک کرد.

پوشه **My Documents** به طور پیش فرض جزو موارد اسکن تیک خورده است.



۵-مدیریت وظایف ( **Manage Tasks** ) : با کلیک کردن روی این دکمه ، پنجره مدیریت وظیفه باز میشود که برای مشاهده اطلاعات مربوط به تمام وظایف فعلی و در حال اجرا و در مورد نحوه مدیریت آنها طراحی شده است. (برای مثال، در مورد اسکن کامل، اسکن آسیب پذیری، اسکن rootkit ها)



## ۵-بروزرسانی ( Update )

این قسمت جهت بروزرسانی دیتابیس نرم افزار مورد استفاده قرار میگیرد و دارای دو نوع آپدیت (آفلاین و آنلاین) می باشد. **بروزرسانی آفلاین** : در صورتی که به اینترنت پرسرعت دسترسی نباشد و همچنین برای بروزرسانی اولیه (بدلیل حجم بالا) نرم افزار کاربرد دارد. در این حالت با معرفی فایل های بروزرسانی عمل بروزرسانی آفلاین صورت میگیرد. توضیحات کامل و نحوه بروزرسانی آفلاین نرم افزار بصورت جداگانه بعد از مبحث معرفی کلید ، توضیح داده شده است. **بروزرسانی آنلاین** : در این نوع بروزرسانی ، فایل های بروزرسانی از سرور اصلی کسپر دانلود میشود و بعد از بروزرسانی اولیه ، فایل های بروزرسانی دارای حجم کمی میباشد.

**Updating databases and application (15%)...**

By default, Kaspersky Internet Security regularly checks for updates, and will automatically download and install new database signatures. You can also run an update manually at any time.

Status: processing files  
Downloaded: 0 KB (3 KB/sec)  
Source: <http://dnl-12.geo.kaspersky.com/>

Stop

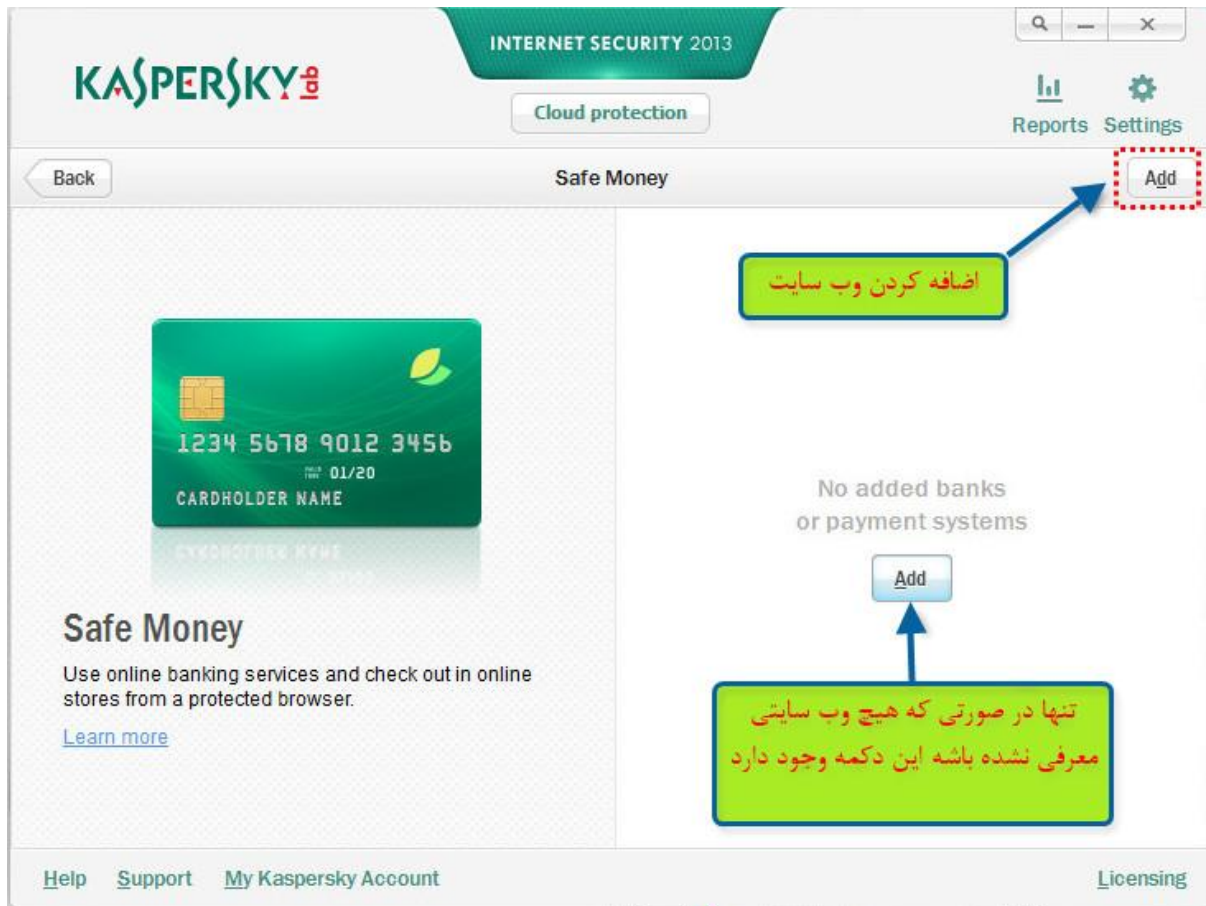
[Virus activity review](#)

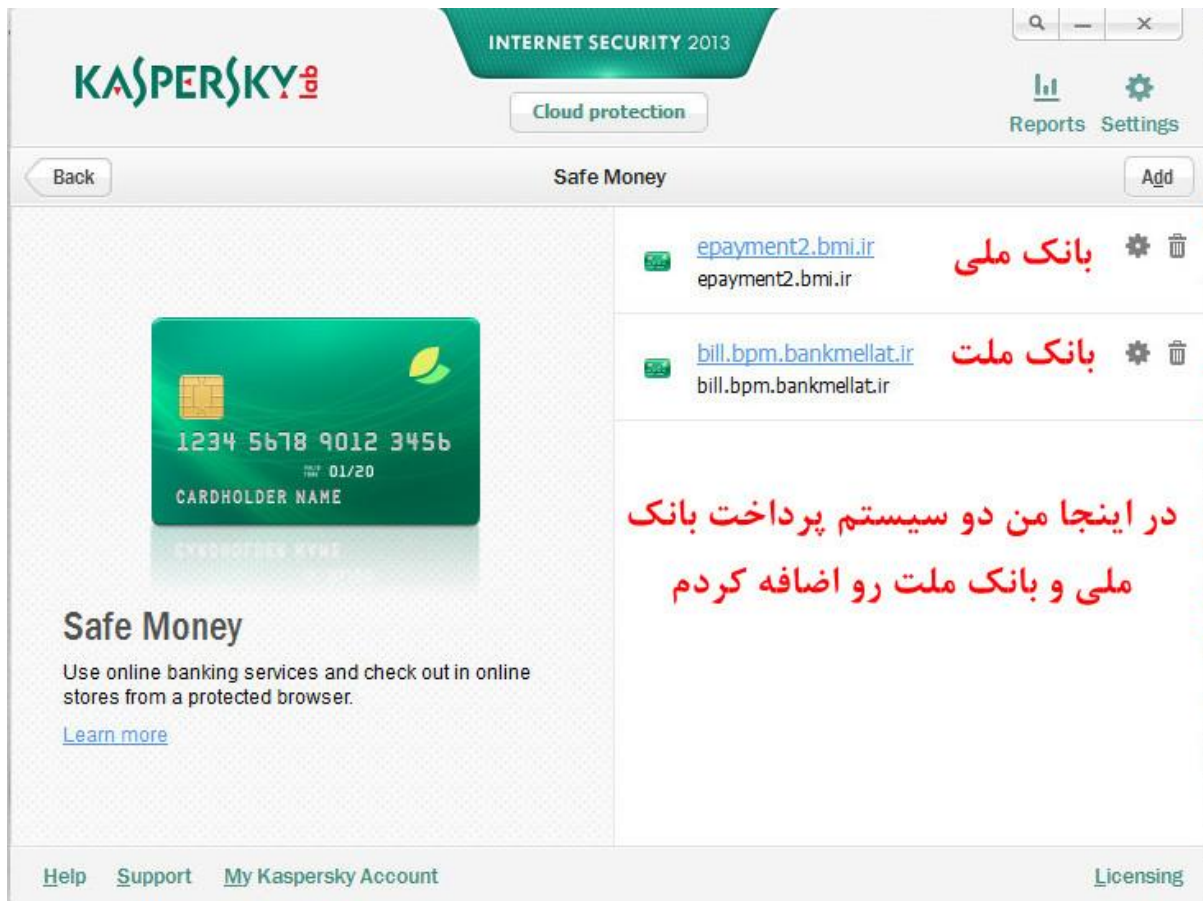
Help Support My Kaspersky Account Licensing



## ۶- پرداخت و خرید اینترنتی امن ( Safe Money )

با کلیک کردن روی این دکمه پنجره پول امن باز می شود. در این پنجره می توان وب سایت یک بانک یا یک سیستم پرداخت اینترنتی را به آن معرفی کرد.





## ۷- کنترل والدین ( Parental Control )

این قسمت جهت اعمال محدودیتهایی از جانب والدین برای فرزندانشان کاربرد دارد. در زمان راه اندازی کنترل والدین ، در صورتی که دسترسی با کلمه عبور محافظت شده باشد باید فیلد را پر کرد و به تنظیمات دسترسی پیدا کرد. در غیر اینصورت باید پسورد را برای اولین بار در نرم افزار وارد و تأیید کرد تا کسی به تنظیمات این قسمت دسترسی پیدا نکند. ( بهتره از پسورد قوی استفاده بشه چون خودتون میدونین بچه این دوره نمونه رو همیشه با یه پسورد ضعیف دور زد 😊 )

KASPERSKY LAB INTERNET SECURITY 2013

Cloud protection

Reports Settings

Back Parental Control

## Password protection

Before configuring Parental Control, we recommend you create a password to protect the settings against modification by other users.

Password:

Confirm:

Continue Skip







Help Support My Kaspersky Account Licensing

KASPERSKY LAB INTERNET SECURITY 2013

Cloud protection

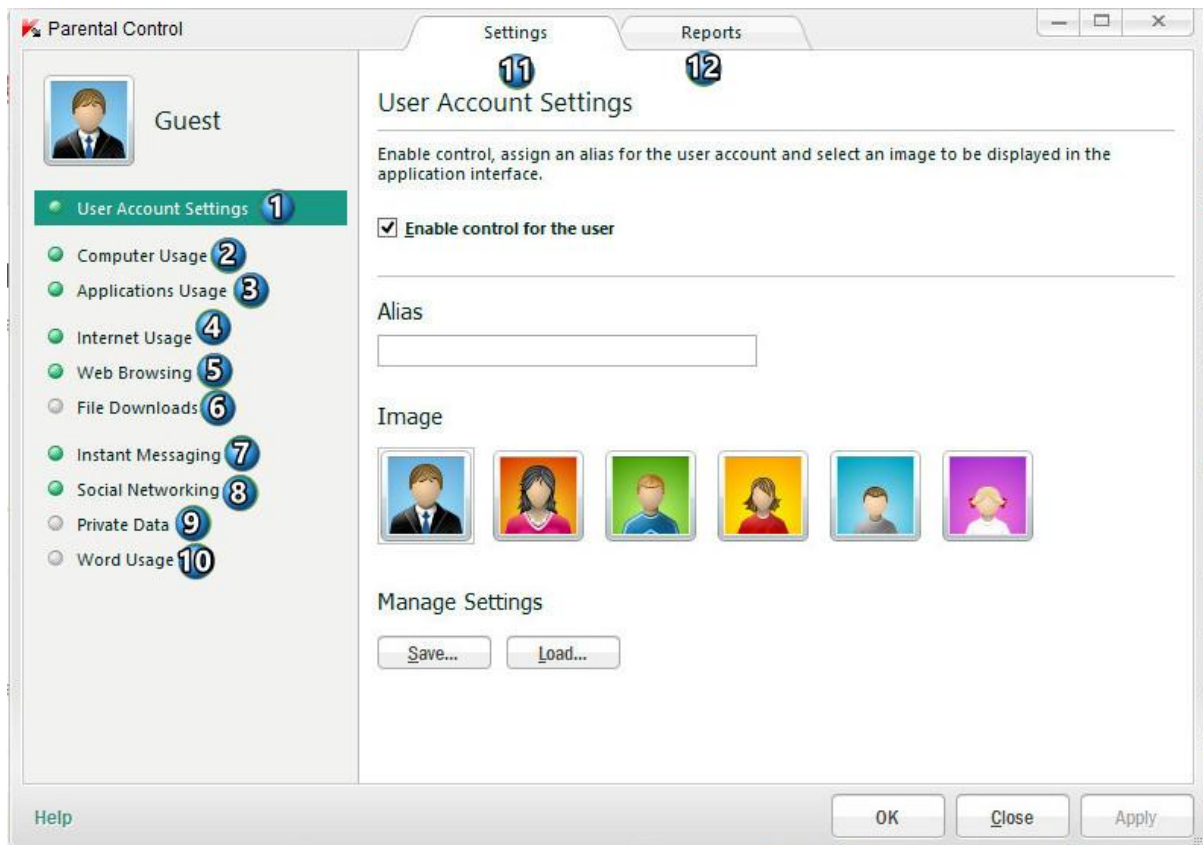
Reports Settings

Back Parental Control

	<b>Administrator</b> ● Control disabled	<b>ورود به تنظیمات بوزر مورد نظر</b>	Enable 
	<b>Guest</b> ● Control disabled	<b>بوزرهای که بر روی سیستم فعال هستند</b>	Enable 
	<b>hadie6z</b> ● Control disabled	<b>فعال کردن بوزر مورد نظر</b>	Enable 

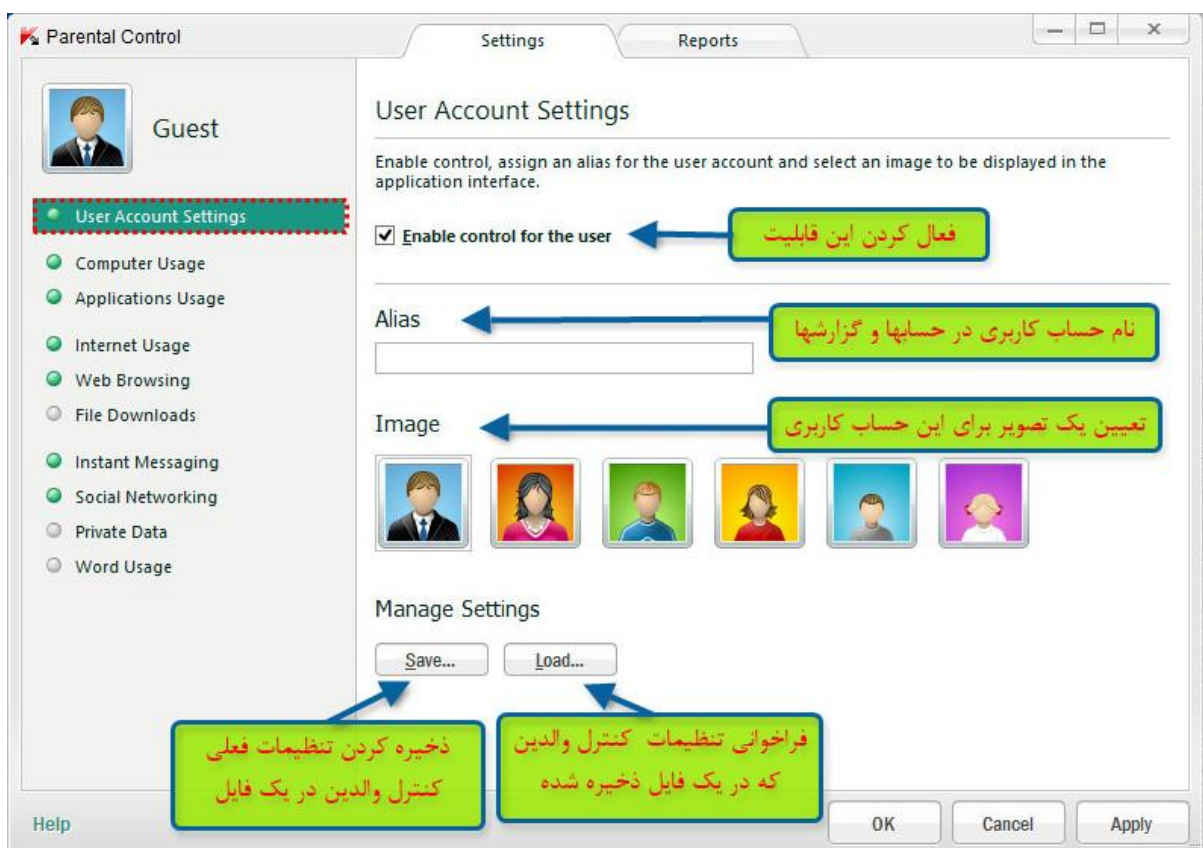
Help Support My Kaspersky Account Licensing



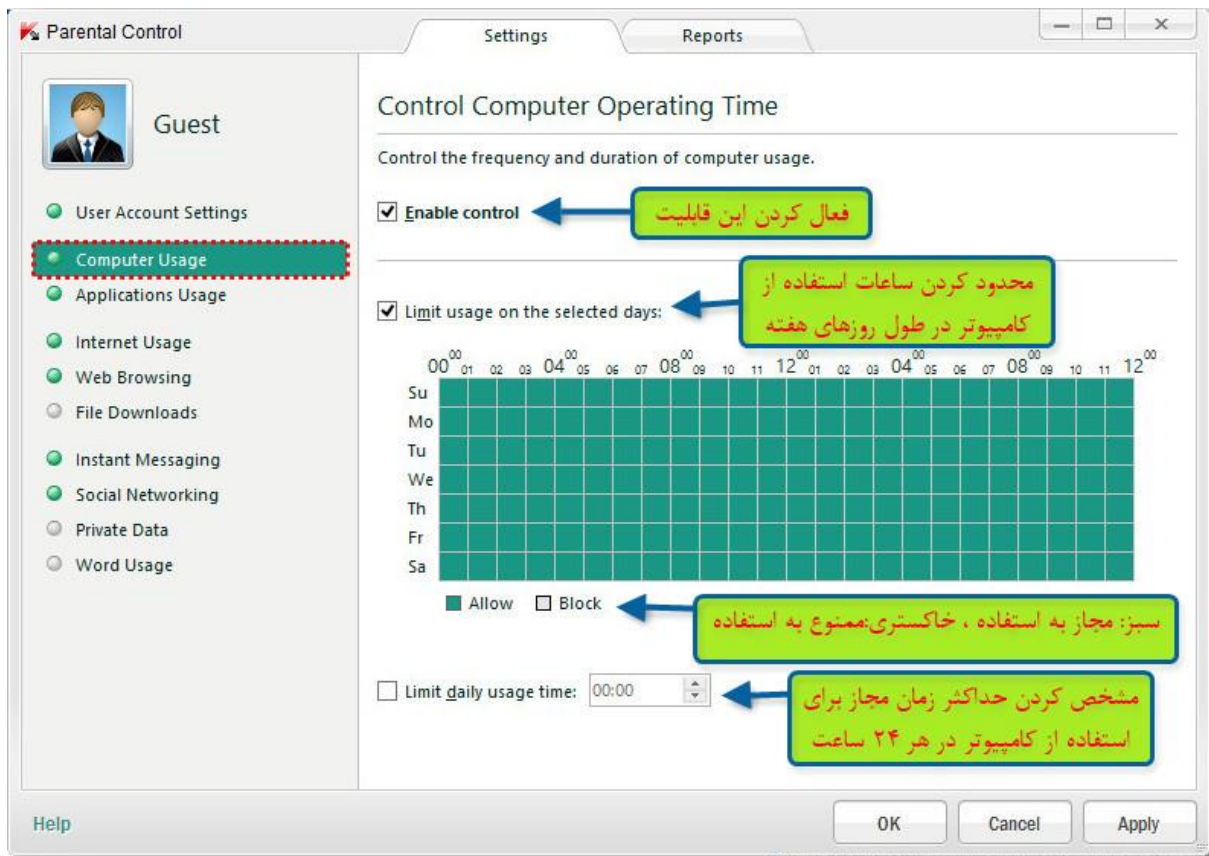


توضیحات هر شماره بصورت تصویری داده شده

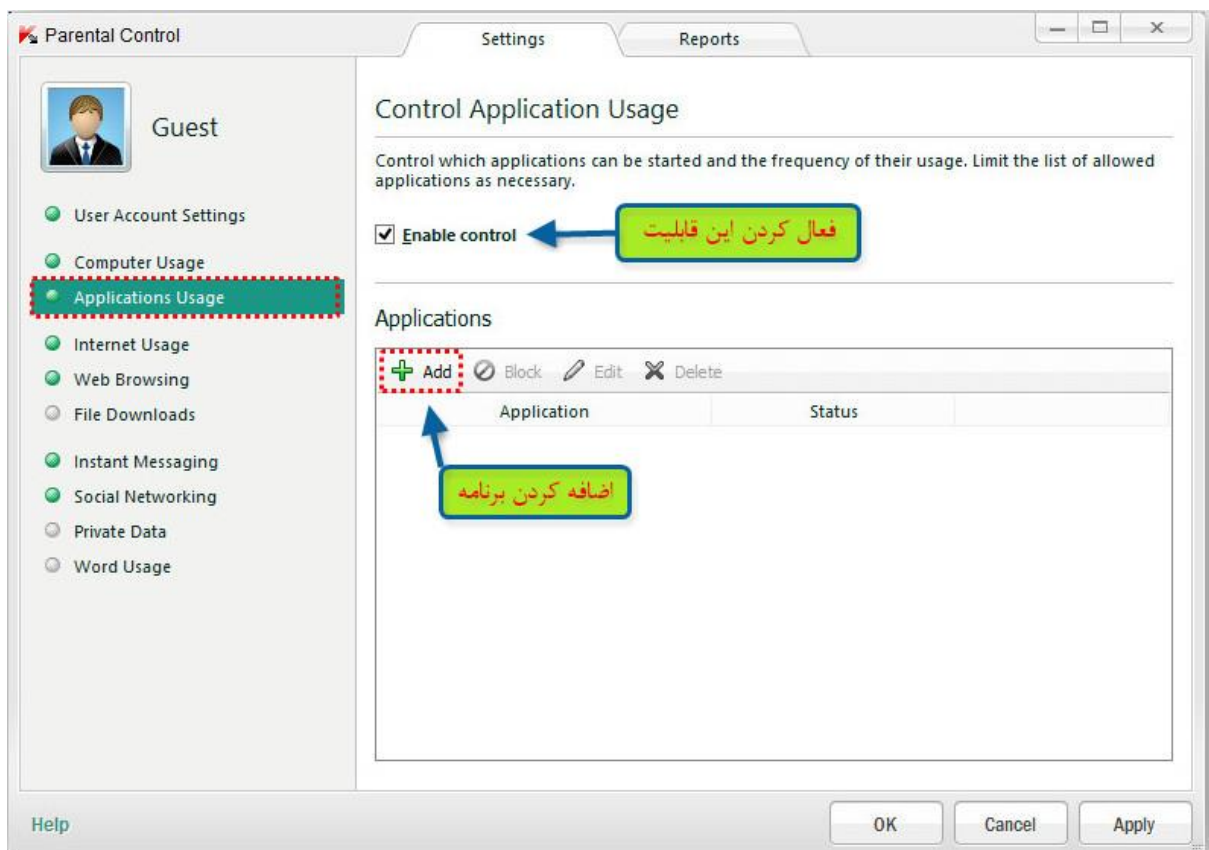
۱- تنظیمات حساب کاربری:

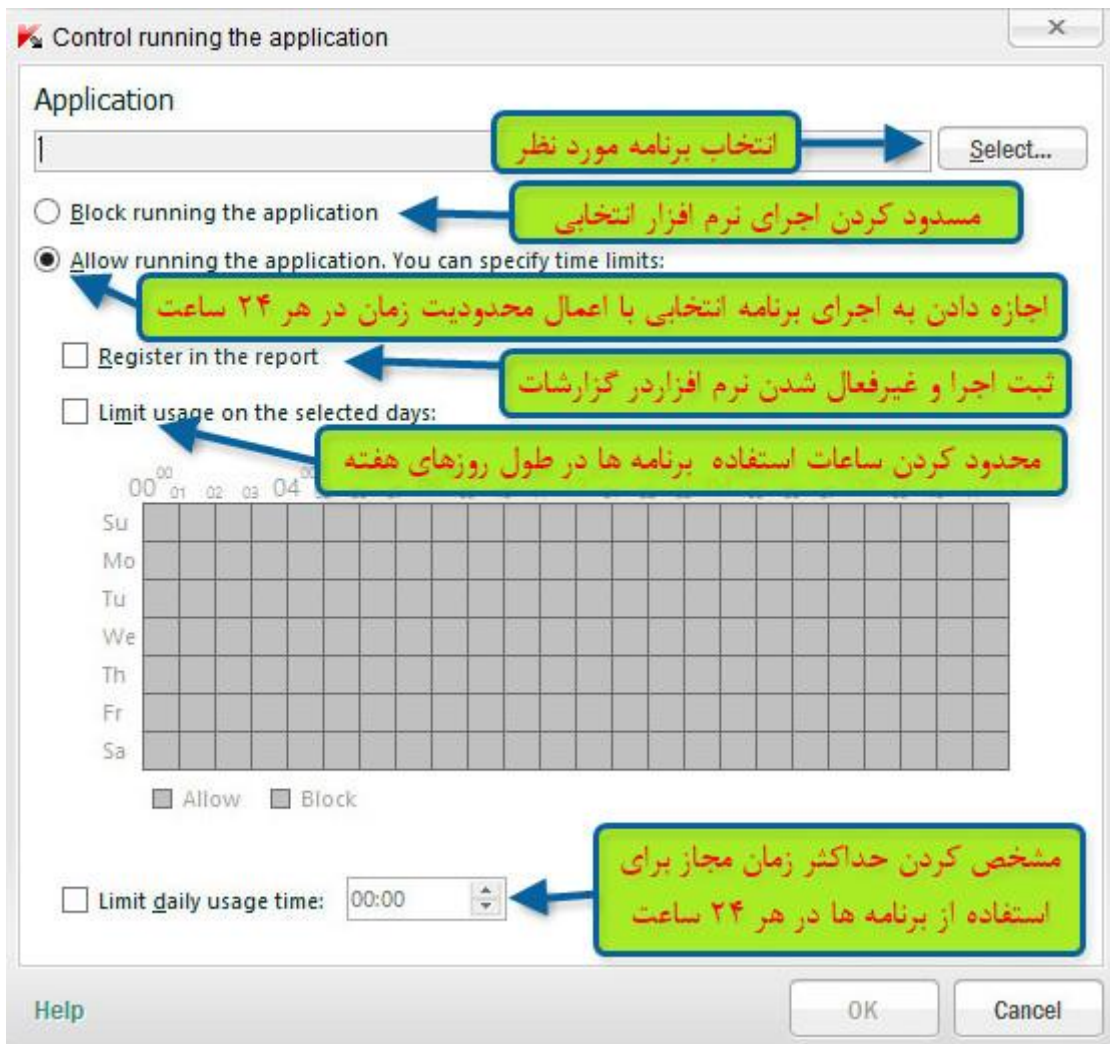


۲- محدود کردن زمان استفاده از کامپیوتر

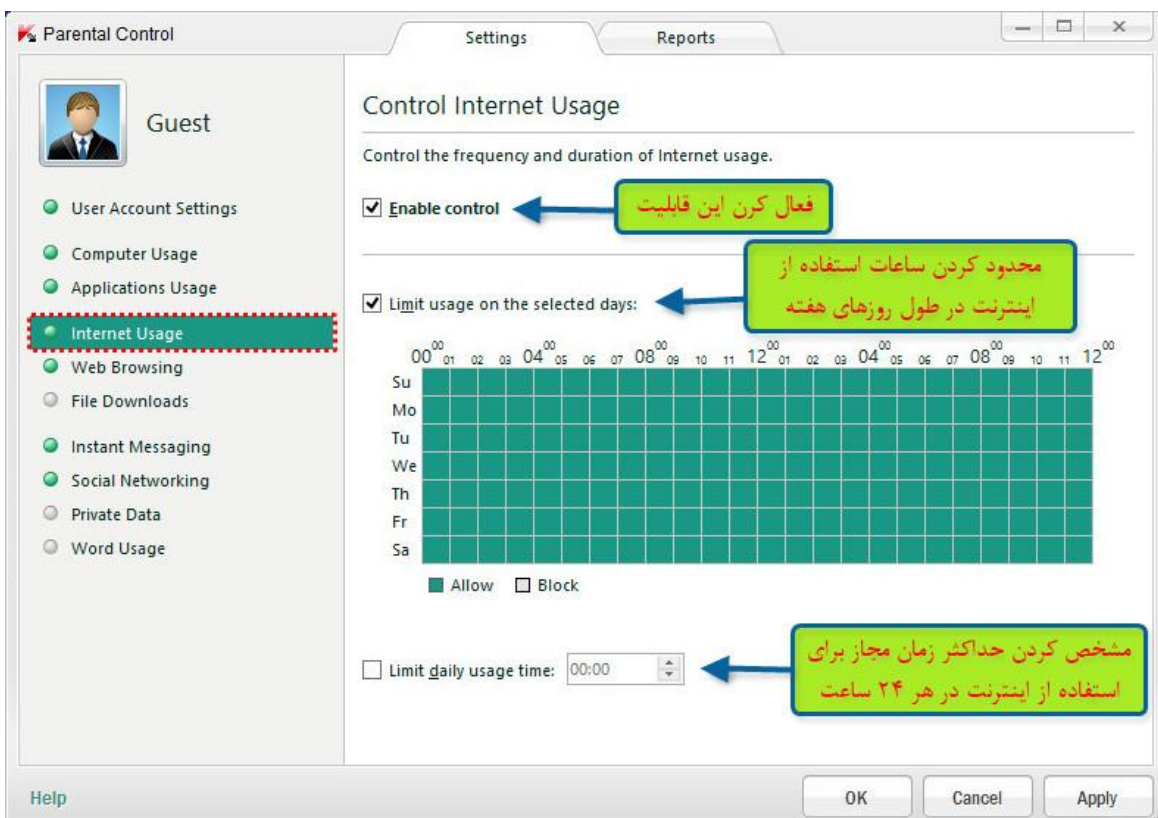


۳- جلوگیری از شروع بکار برنامه ها یا تعیین محدودیت زمانی برای اجرای برنامه های کاربردی

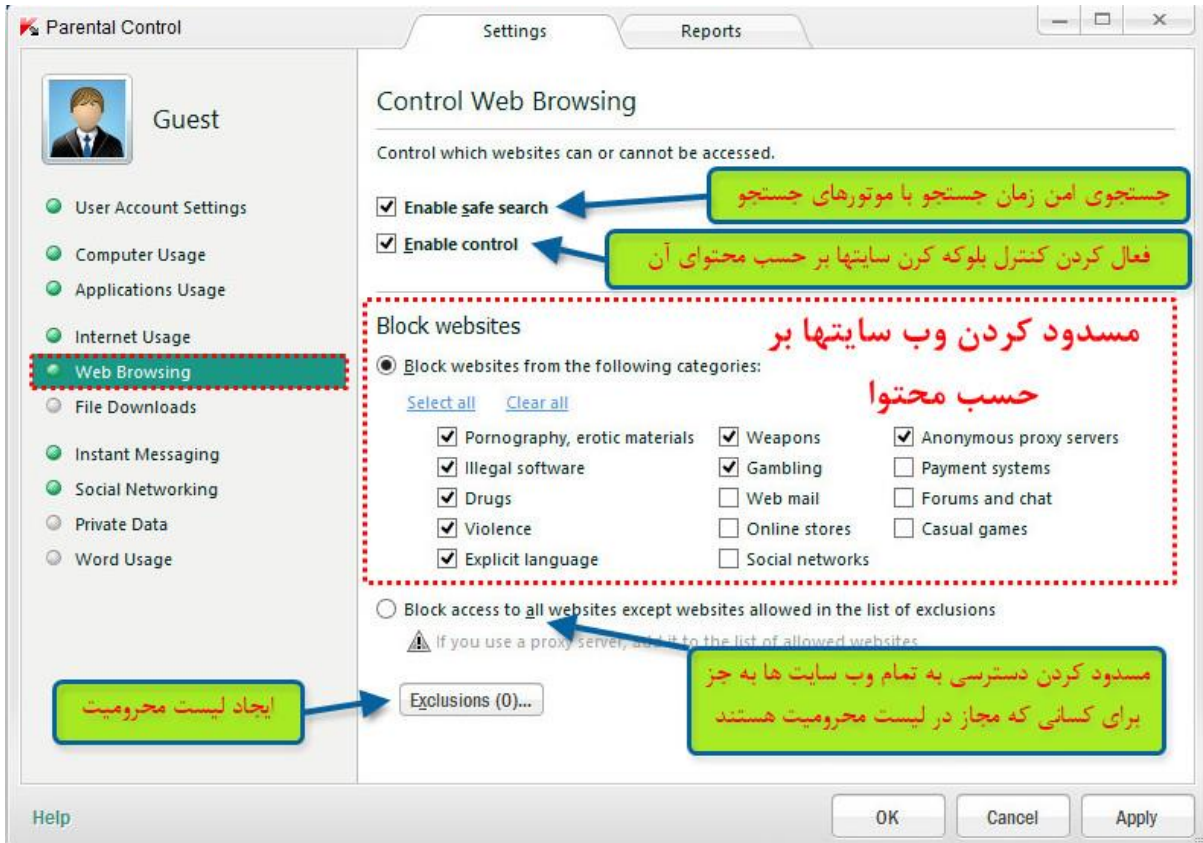




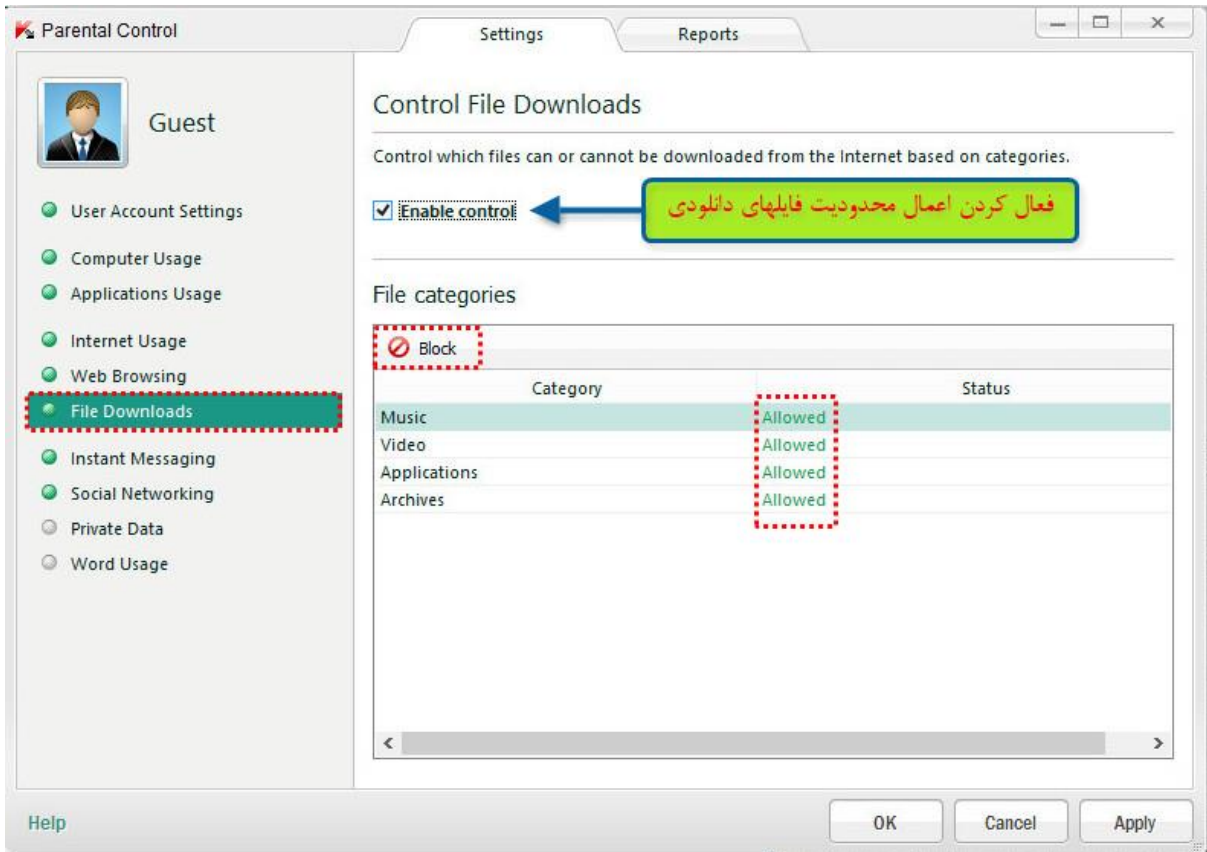
۴- محدود کردن زمان استفاده از اینترنت



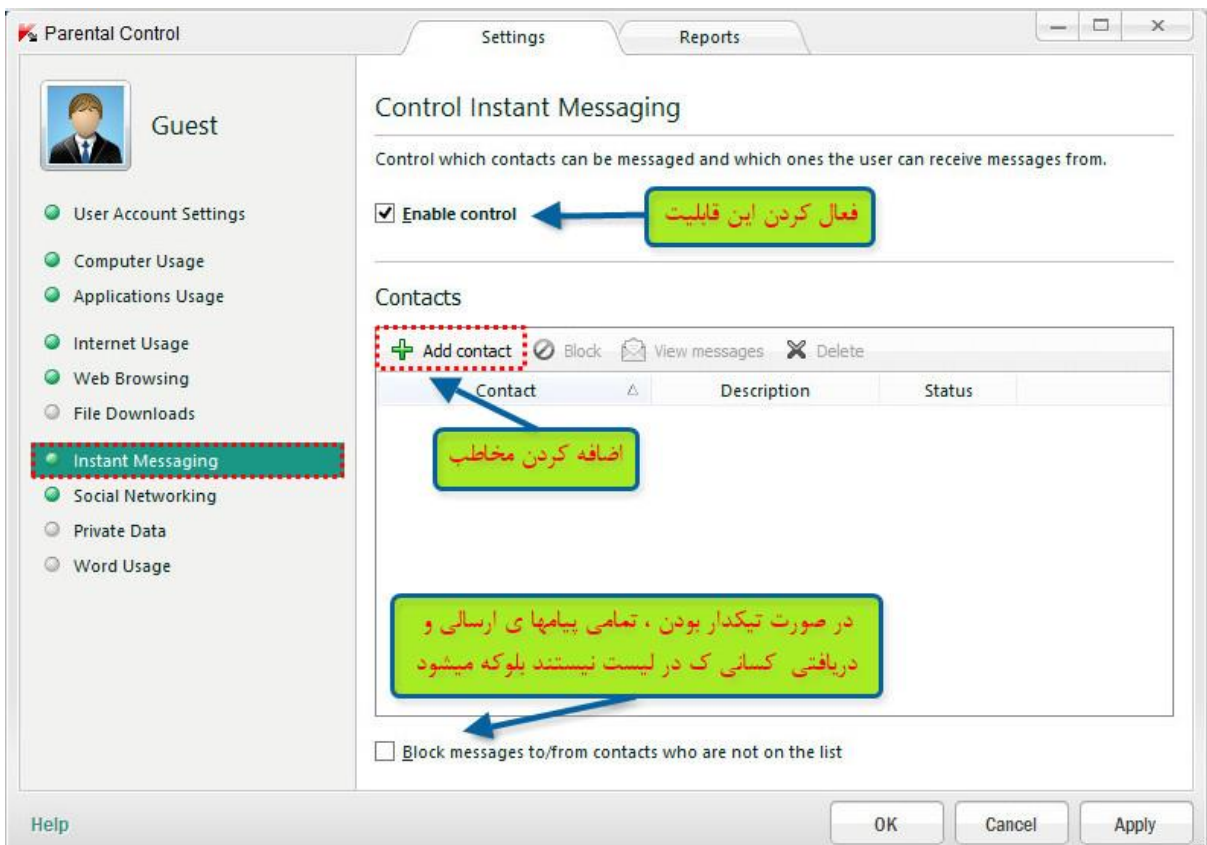




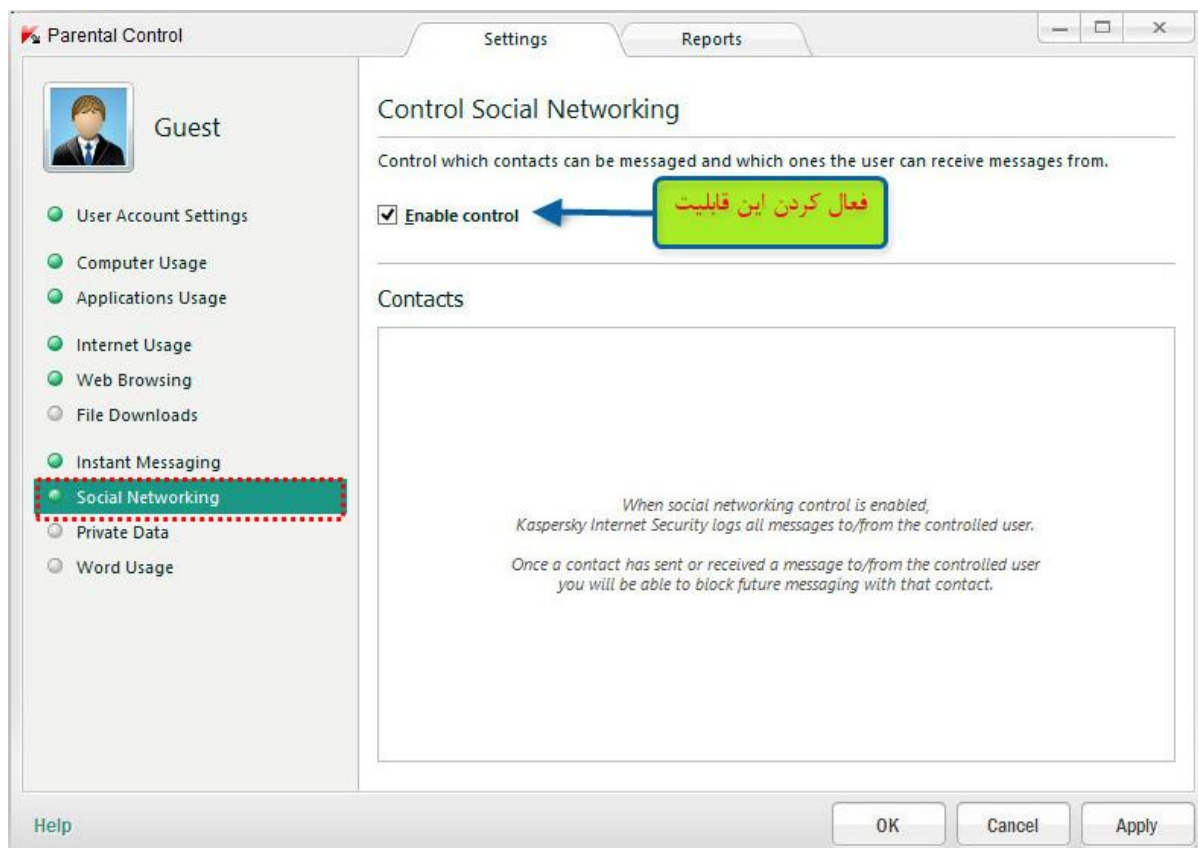
۶- محدود کردن فایل‌های دانلودی بر حسب محتوا (موزیک، فیلم، برنامه و ...)



۷- کنترل پیام‌های فوری



۸- کنترل بخش شبکه های اجتماعی : در این قسمت می توان پیام های کاربر را در شبکه های اجتماعی محدود کرد.



۹- بخش کنترل به اشتراک گذاری داده های خصوصی : شما می توانید انتقال از داده های شخصی ، توسط کاربر از طریق مشتریان IM، شبکه های اجتماعی، و ارسال داده ها را به وب سایتها محدود کنید.

۱۰- بخش کنترل استفاده کلمه : شما می توانید بر استفاده از واژه ها و ترکیب کلمه مشخص شده در پیام به کاربر را از طریق مشتریان IM، شبکه های اجتماعی، و هنگام ارسال داده ها به وب سایت نظارت داشته باشید.

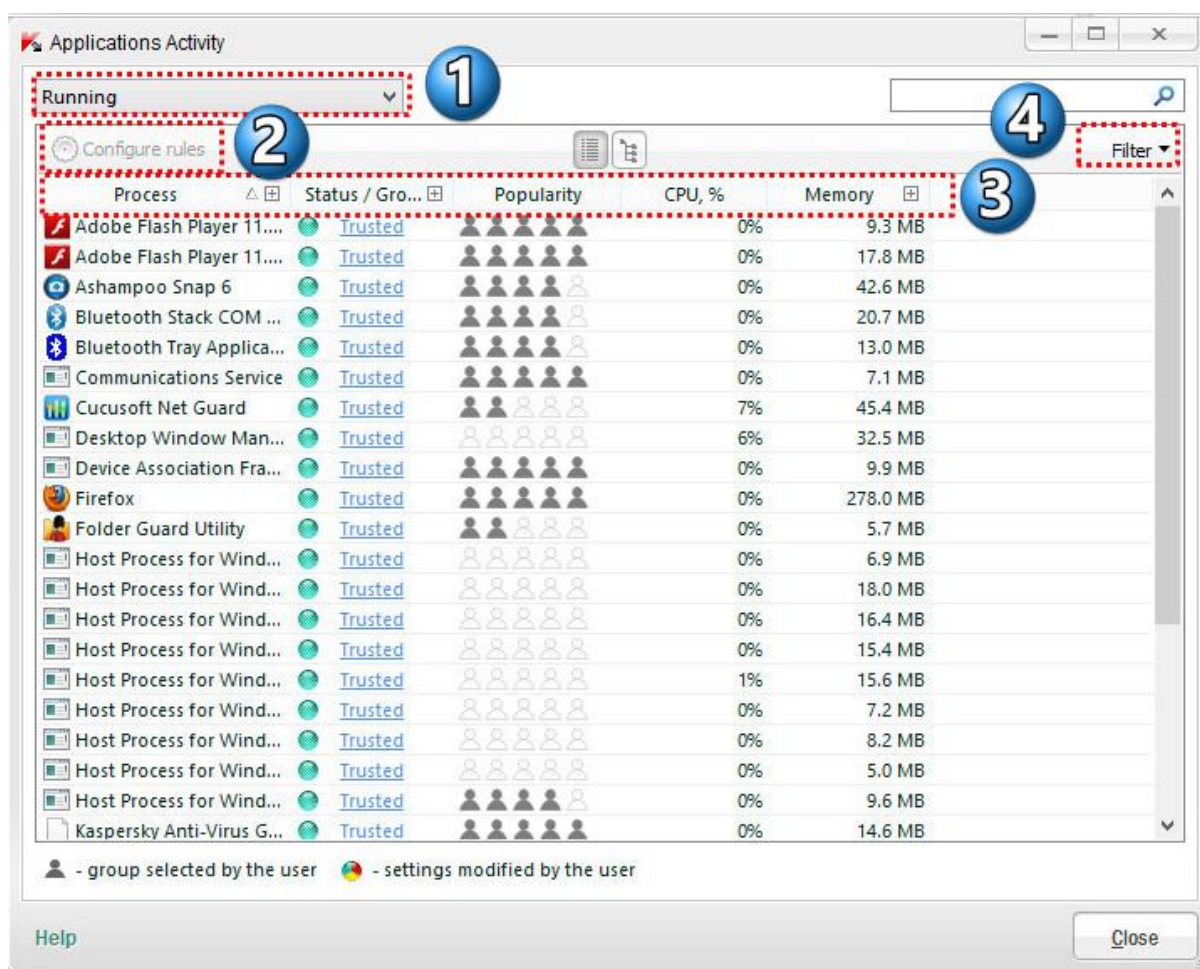
۱۱- تنظیمات مربوط به هر قسمت

۱۲- گزارشات مربوط به هر قسمت



## ۸- برنامه های فعال (Application Activity)

این پنجره یک لیست، شامل اطلاعات مربوط به فعالیت برنامه های کاربردی نصب شده بر روی کامپیوتر شما می باشد.



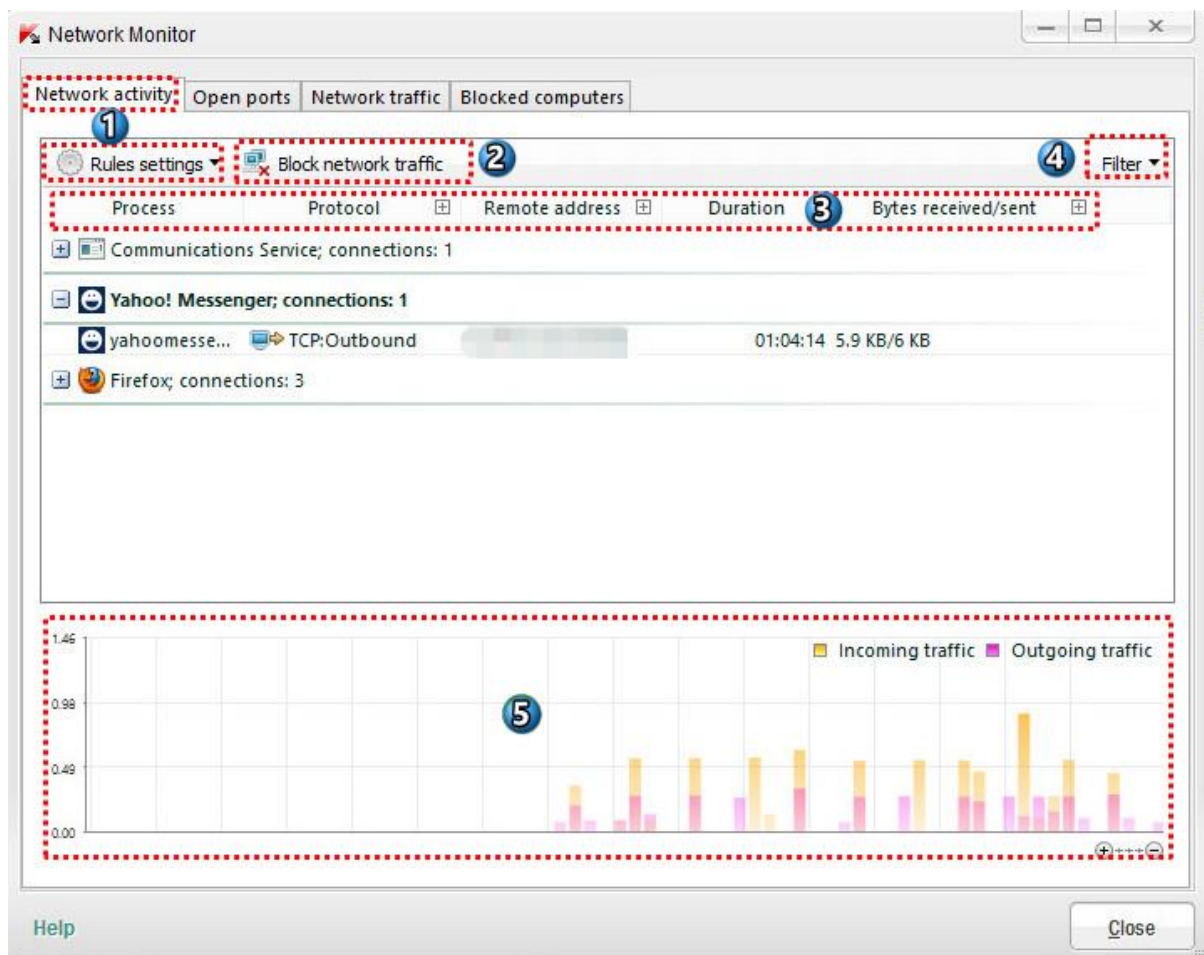
- ۱- این لیست برای اعمال دو نوع فیلتر فعالیت برنامه های کاربردی استفاده میشود:  
**در حال اجرا (Running)** - لیست اطلاعات برنامه هایی که در حال حاضر در حال اجرا هستند را نشان می دهد.  
**همه (All)** - لیست اطلاعات تمام برنامه های نصب شده بر روی کامپیوتر شما را نشان می دهد.
- ۲- **پیکربندی قوانین (Configure rules)** - با کلیک بر روی این دکمه پنجره کاربرد قوانین باز می شود. در این پنجره، شما می توانید قوانینی برای مدیریت فعالیت های برنامه انتخاب شده ایجاد کنید.  
**این بخش بعداً بصورت کاملتر توضیح داده خواهد شد.**
- ۳- توضیحات موارد بصورت تکی در زیر  
**Process (فرایند)**: ستونی از برنامه های کاربردی لیست فعالیت، که نام برنامه و یا یک فرآیند را نمایش می دهد.  
**Status / Group (وضعیت / گروه)**: نمایش وضعیت برنامه تعیین شده و گروه مطمئن  
**سبز**: برنامه های گروه مطمئن نمایش داده می شود.  
**زرد**: برنامه های گروه کم اطمینان نمایش داده می شود.  
**قرمز**: برنامه های گروه غیر قابل اطمینان نمایش داده می شود.  
**Popularity (محبوبیت)** - نمایش تعداد کاربرانی از آن برنامه استفاده میکنند.  
**CPU, % (پردازشگر)** - نمایش میزان استفاده برنامه از پردازشگر  
**Memory (حافظه)** - نمایش میزان استفاده برنامه از حافظه

۴- **فیلتر (Filter)** - با کلیک بر روی این دکمه یک منو کشویی باز میشود که در آن میتوان فیلترهای زیر را اعمال کرد:  
**Run on startup (اجرا در راه اندازی)** - فرآیندهایی که زمان راه اندازی سیستم عامل اجرا شده اند.  
**System processes (فرآیندهای سیستم)** - فرآیندهای لازم برای فعالیت سیستم عامل  
**Kaspersky Internet Security processes (فرآیندهای کسپر سکی)** - فرآیندهای اجرا شده توسط کسپرسکی  
اینترنت سکیوریتی

## ۹- نظارت بر شبکه ( Network Monitor )

این لیست شامل تمام اتصالات فعال شبکه که در حال حاضر بر روی کامپیوتر در حال فعالیت هستند.

سربرگ **Network activity (فعالیت های شبکه):**



۱- **تنظیمات قوانین (Rules settings):** با کلیک بر روی این دکمه یک منو باز می شود که شامل موارد زیر است:  
**All network rules (تمام قوانین شبکه)** - تمامی پنجره های باز فایروال ، جایی که در آن شما می توانید برای برنامه های انتخاب شده از لیست قوانین بسته را پیکربندی کنید.  
**Application network rules (قوانین برنامه شبکه)** - پنجره قوانین برنامه های باز، جایی که در آن شما می توانید برای برنامه های انتخاب شده از لیست قوانین شبکه را پیکربندی کنید.  
**۲- مسدود کردن ترافیک شبکه (Block network traffic):** با کلیک کردن روی این دکمه فایروال تمامی پروسه های فعال روی شبکه را مسدود میکند.  
در صورتی که شما روی این دکمه یک بار کلیک کنید اسم آن به **Unblock network traffic (غیرفعال کردن مسدود سازی شبکه)** که اگر بر روی آن کلیک کنید فایروال به تمامی پروسه ها اجازه میدهد به حالت طبیعی برگردند.





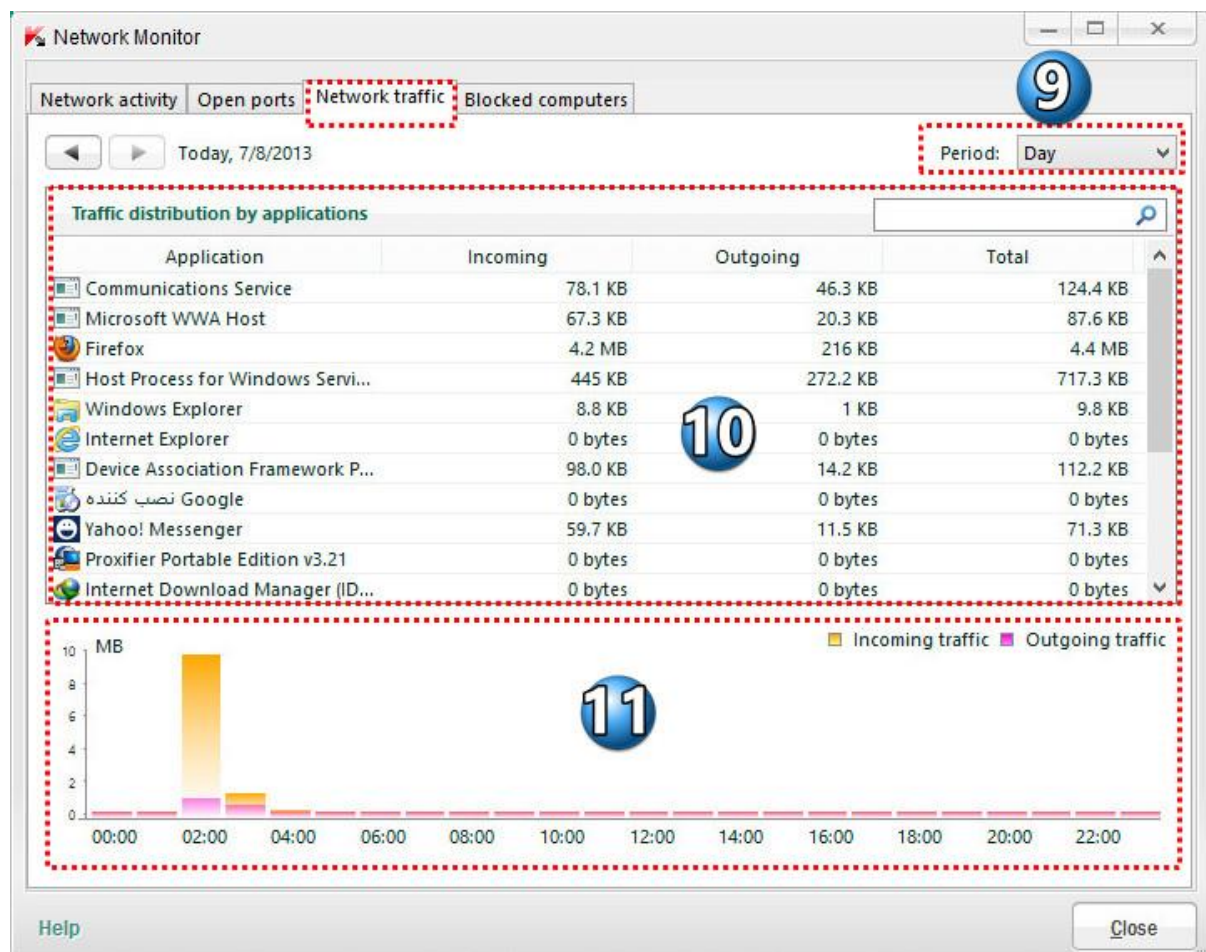
۶- تنظیمات قوانین (Rules settings): با کلیک بر روی این دکمه یک منو باز می شود که شامل موارد زیر است:  
**All network rules (تمام قوانین شبکه)** - تمامی پنجره های باز فایروال ، جایی که در آن شما می توانید برای برنامه های انتخاب شده از لیست قوانین بسته را پیکربندی کنید.  
**Application network rules (قوانین برنامه شبکه)** - پنجره قوانین برنامه های باز، جایی که در آن شما می توانید برای برنامه های انتخاب شده از لیست قوانین شبکه را پیکربندی کنید.

۷- اطلاعات زیر برای هر اتصال نمایش داده می شود: اطلاعات مربوط به تمام پورت های باز هر پروسه که اطلاعات زیر برای هر پورت نمایش داده میشود :

نام پروسه ای که از پورت استفاده میکند (نرم افزار، سرویس، سرور) تعداد پورت، IP آدرس محلی پروسه پروتکل مورد استفاده مدت زمانی که در طی آن پورت برای اتصال باز است.

۸- فیلتر (Filter) : با کلیک بر روی این دکمه یک منو باز می شود که شامل موارد زیر است:  
**All open ports (تمام پورت های باز)** - نمایش لیست تمامی پورت های باز کامپیوتر شما  
**All except loopback** - نمایش لیست تمام پورت ها به جز کسانی که از نرم افزار شبکه ای برای سیستم عامل خود استفاده میکنند.

## سربرگ Network traffic (ترافیک های شبکه):



۹- دوره زمانی (Period): با کلیک بر روی این دکمه یک منو باز می شود که این لیست شامل فواصل زمانی برای مشاهده توزیع ترافیک شبکه برای برنامه انتخاب شده است.

روز

هفته

ماه

سال

تمام مدت

#### ۱۰- توزیع ترافیک توسط لیست برنامه های کاربردی (Traffic distribution by applications):

شامل اطلاعات در مورد حجم همه اتصالات ورودی و خروجی ایجاد شده بین کامپیوتر شما و کامپیوترهای دیگر و اینترنت می باشد.

جزئیات بصورت زیر نشان داده میشود:

Applications (اسم برنامه)

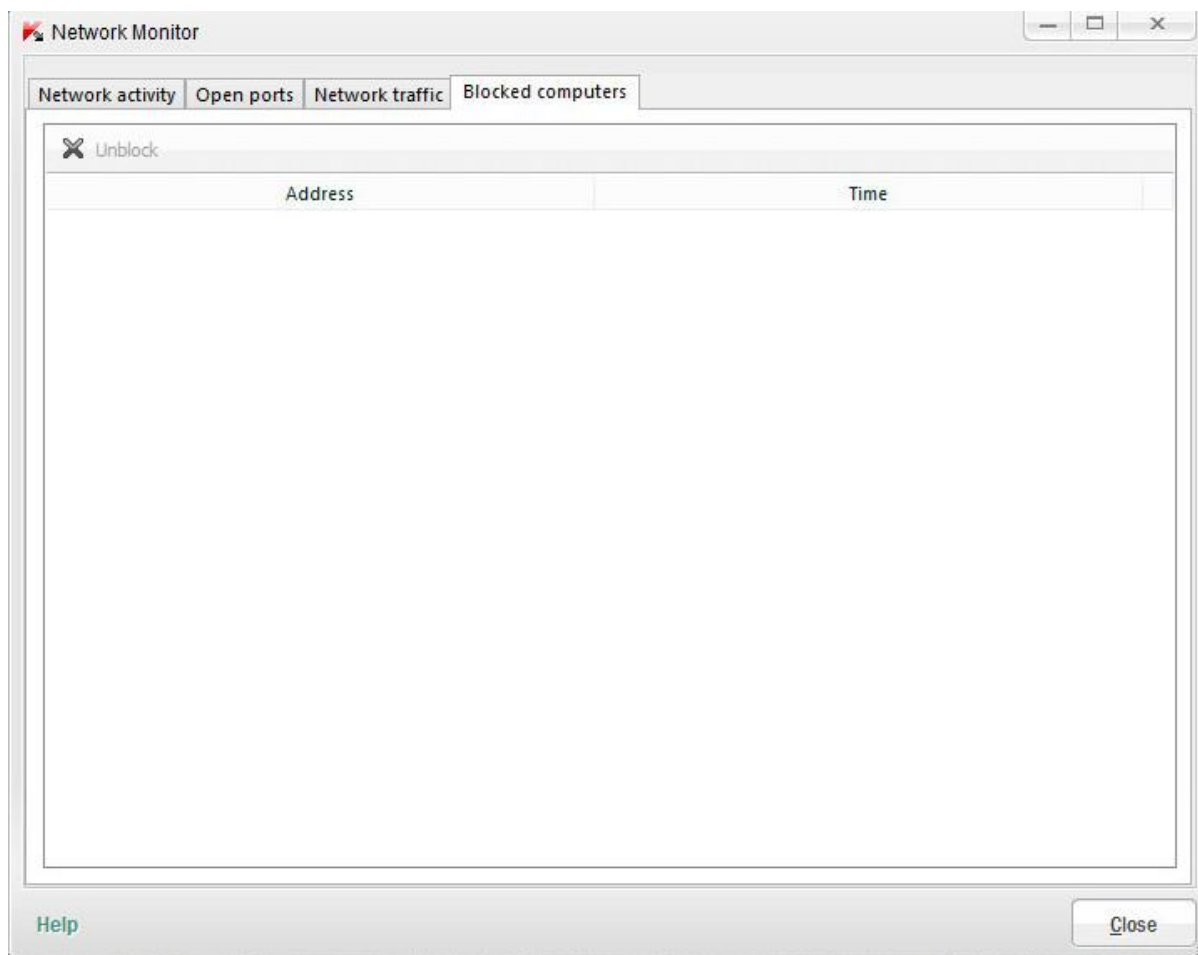
Incoming (حجم ترافیک ورودی)

Outgoing (حجم ترافیک خروجی)

Total (مجموع ترافیک مصرفی)

۱۱- در این قسمت یک نمودار توزیع ترافیک را در بازه زمانی های مختلف (طبق بازه زمانی که در Period انتخاب میشود) نشان میدهد.

#### سربرگ Blocked Computer (کامپیوترهای مسدود شده):

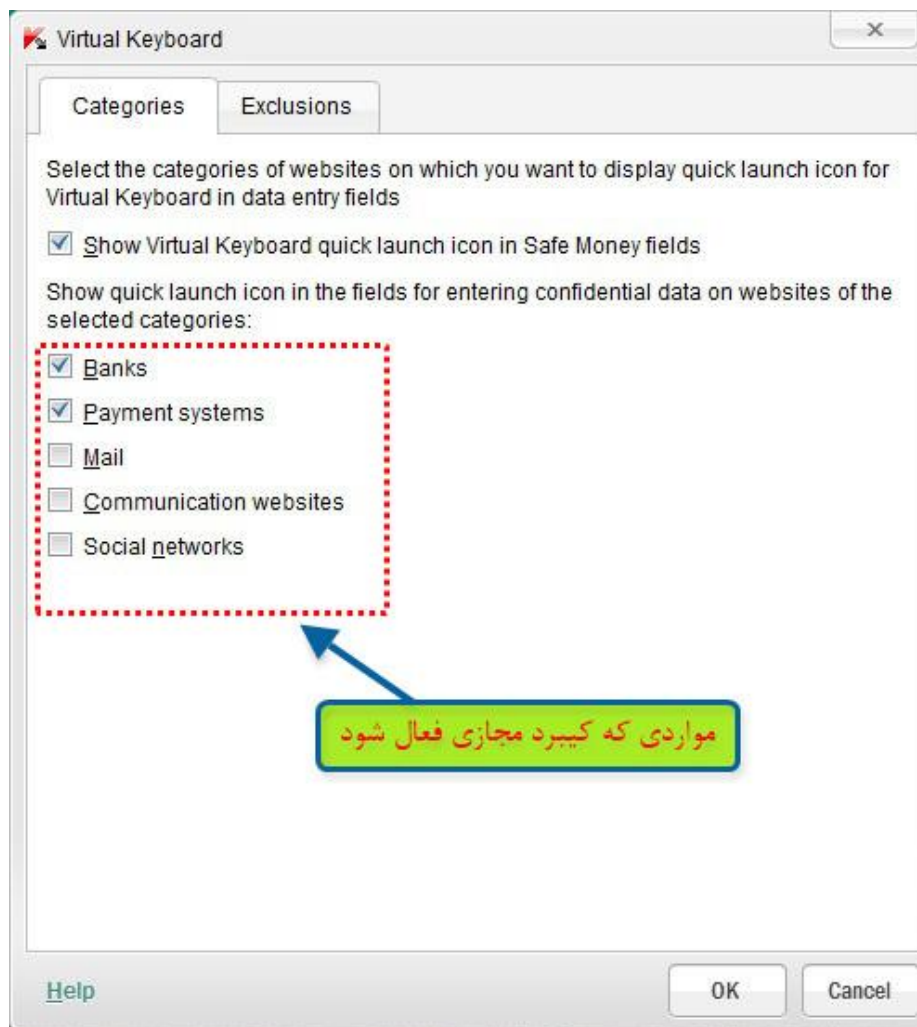


شامل اطلاعات در مورد host هایی که با هدف حمله به کامپیوتر شما، مسدود کرده است، میشود. که شامل IP آدرس host مسدود شده و زمان حمله میشود.

## ۱۰- کیبرد مجازی ( Virtual Keyboard )

همانطور که از اسمش پیداست یک کیبرد مجازی در اختیار کاربر قرار میدهد و در موارد زیر کاربرد دارد:

- ۱- وب سایت بانکها ( Banks )
- ۲- ورود به وب سایت سیستم های پرداخت ( Payment systems )
- ۳- ورود در وب سایت های ارائه دهنده خدمات ایمیل ( Mail )
- ۴- ورود در وب سایت های طراحی شده برای ارتباطات کاربران اینترنت ( Communication websites )
- ۵- ورود به وب سایت های شبکه های اجتماعی ( Social networks )

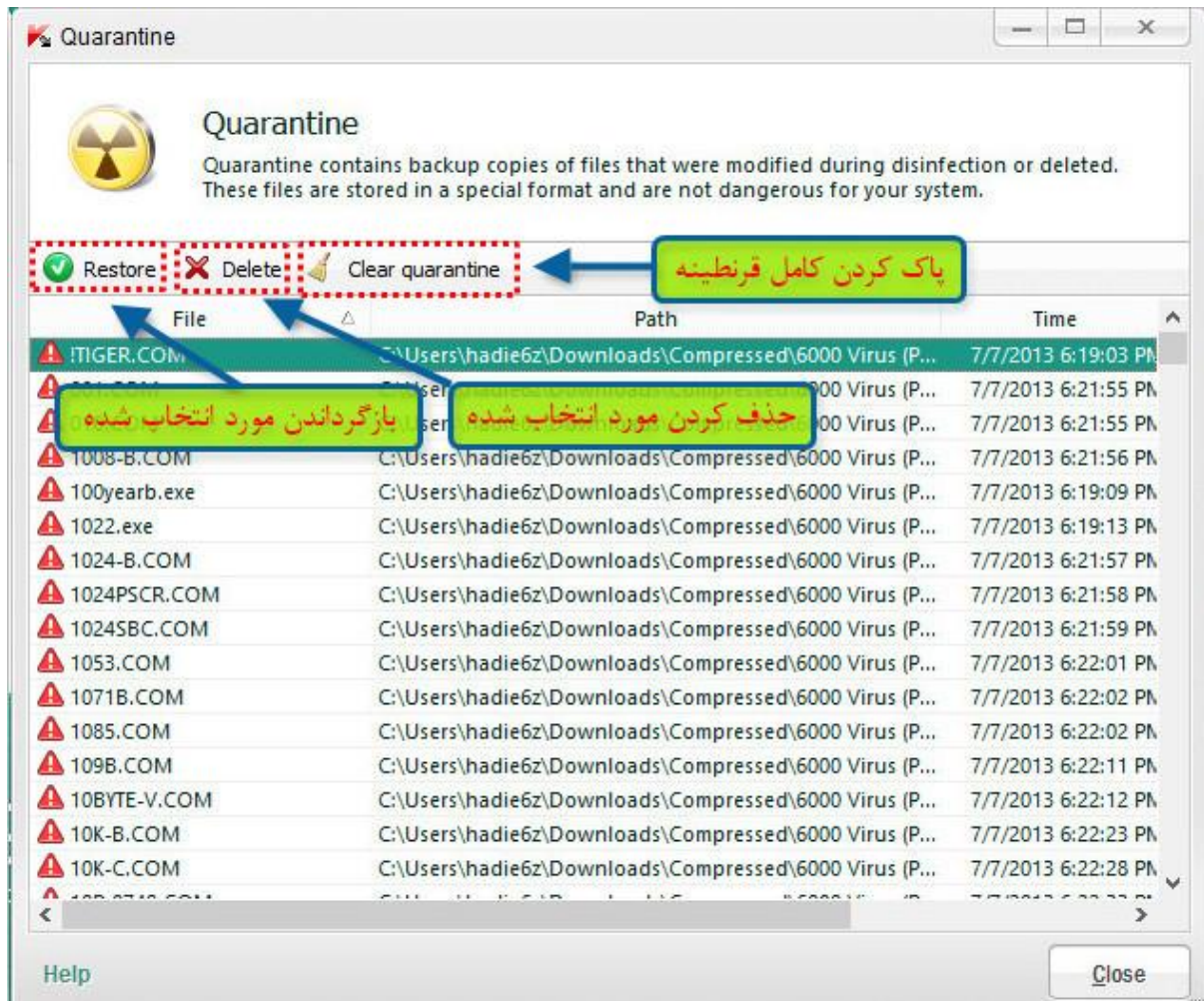






## ۱۱- قرنطینه ( Quarantine )

فایل های آلوده یا مشکوک به آلودگی به قرنطینه منتقل میشود. قرنطینه برای ذخیره سازی نسخه پشتیبان از فایل های حذف و یا اصلاح شده، طراحی شده است.



The screenshot displays the 'Tools' section of the Kaspersky Internet Security 2013 interface. It features a list of four tools, each with an icon, a numbered title, a brief description, and a corresponding action button:

- 1 Kaspersky Rescue Disk**: Create a bootable CD or USB flash drive containing a set of tools for efficiently detecting and eliminating computer infections. Button: **Create**
- 2 Microsoft Windows Troubleshooting**: Search for damaged and irregular settings caused by such things as malware activity, system failures or incorrectly functioning system utilities. Button: **Start**
- 3 Privacy Cleaner**: Clear your PC history of recent commands and accessed files, cookies, caches, logs and other data, keeping your user activity private. Button: **Start**
- 4 Browser Configuration**: Analyze Microsoft Internet Explorer settings from security viewpoint. Button: **Start**

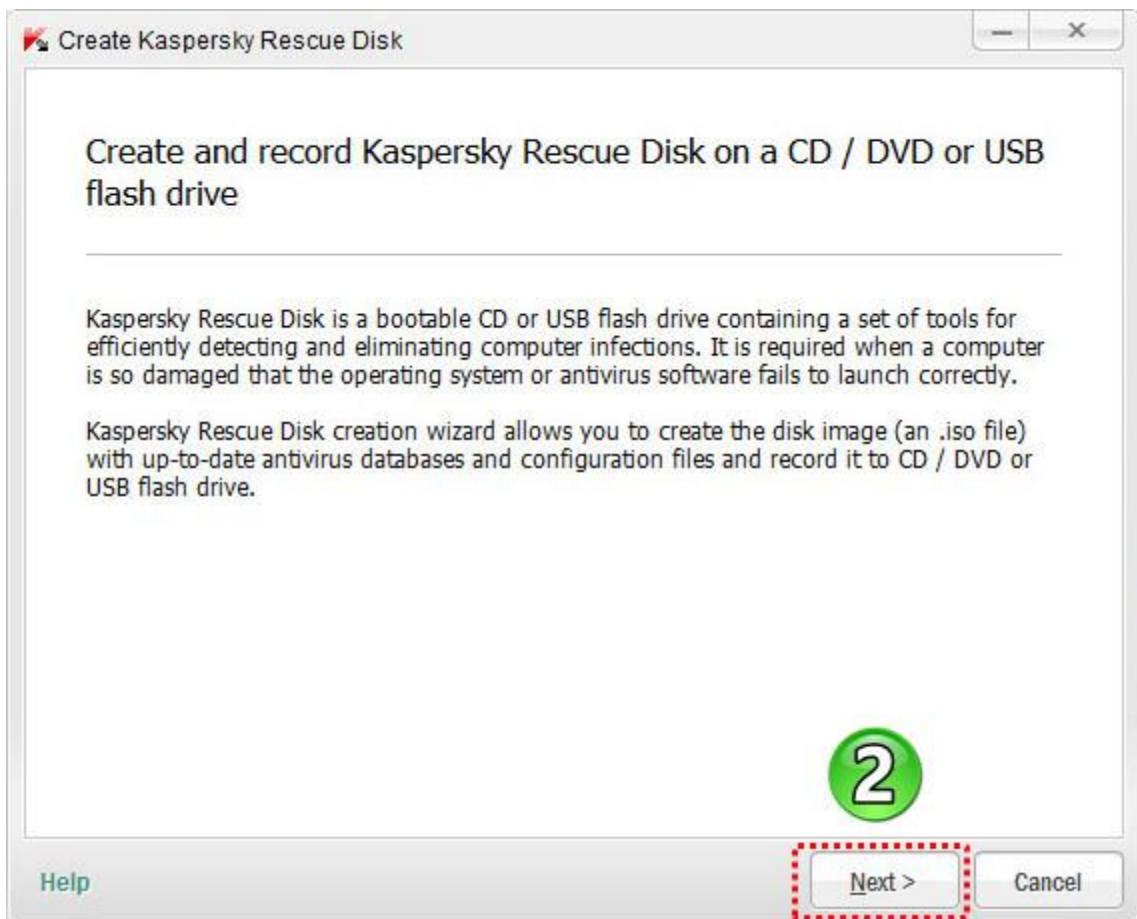
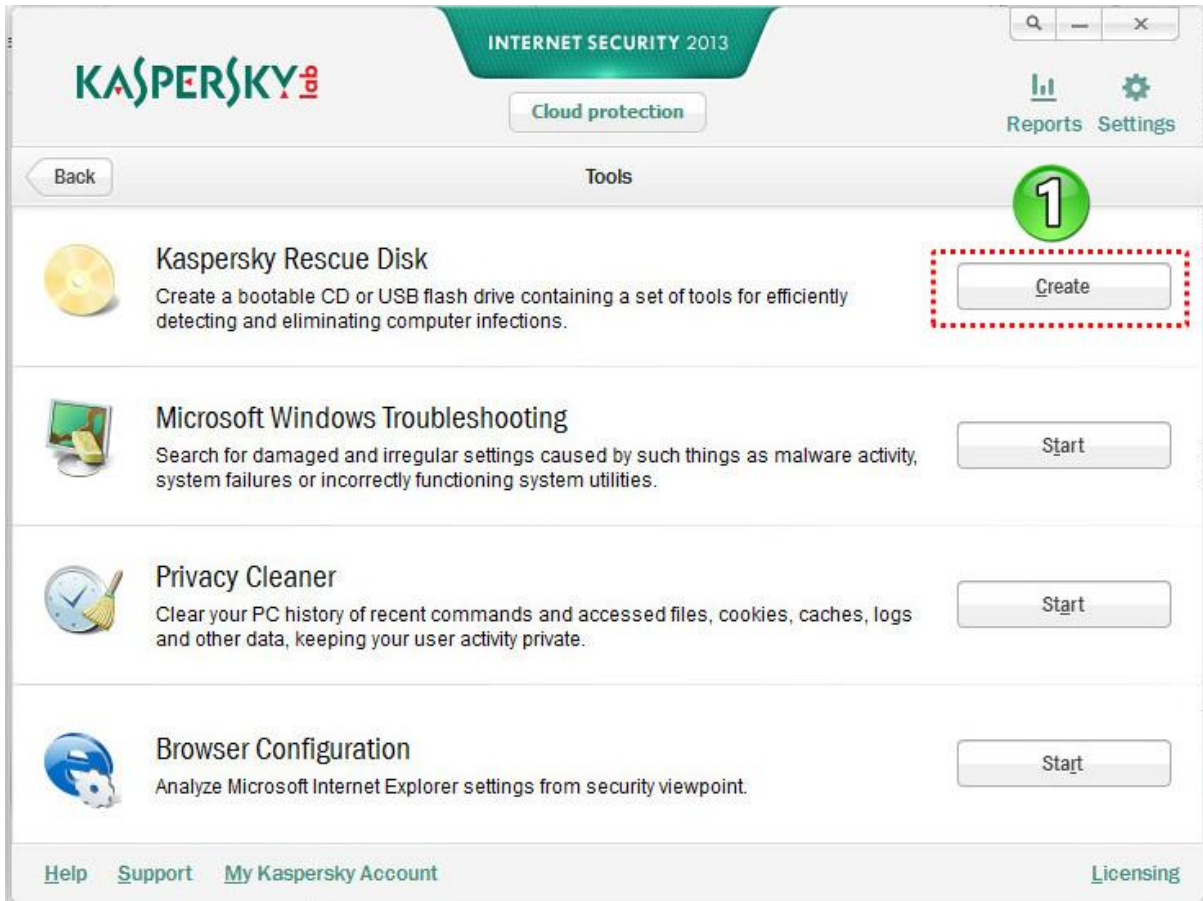
At the bottom of the interface, there are links for [Help](#), [Support](#), [My Kaspersky Account](#), and [Licensing](#).

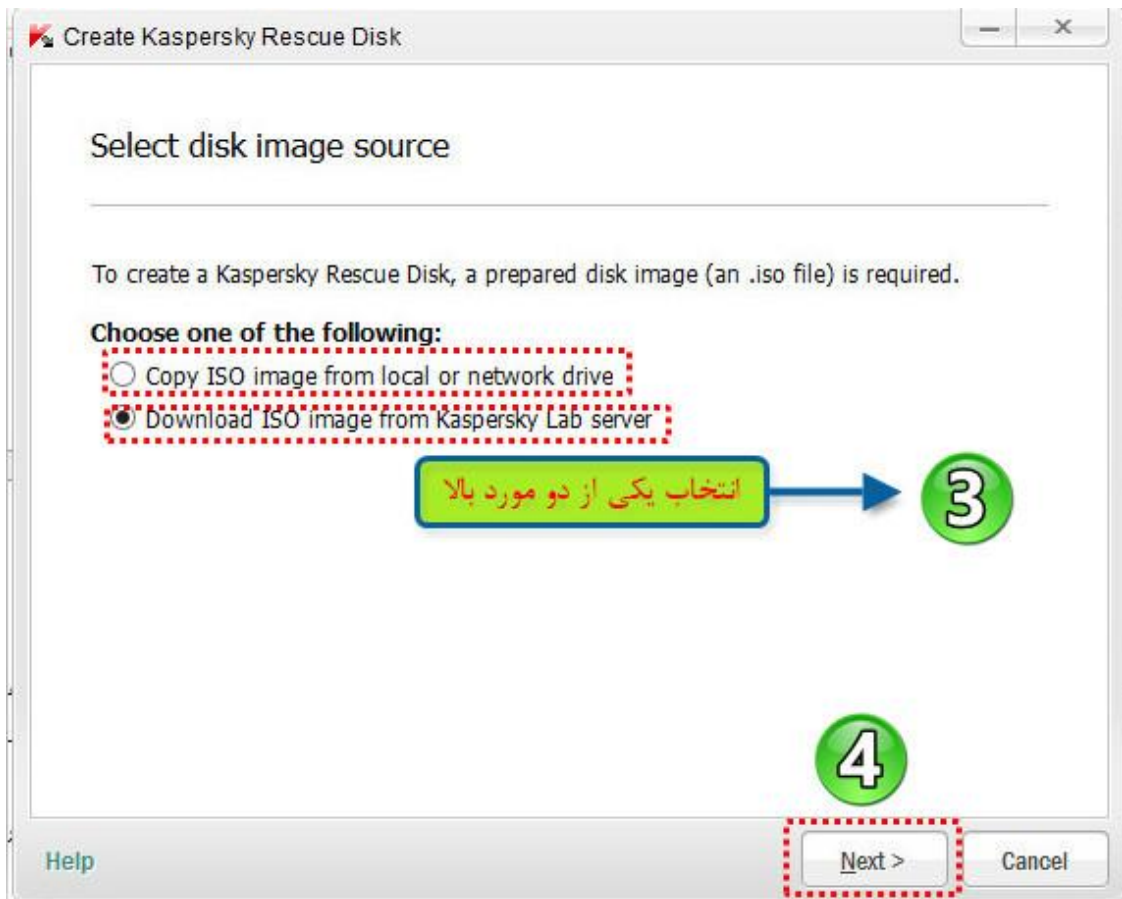
### ۱- دیسک نجات کسپرسکی (Kaspersky Rescue Disk)

با کلیک کردن این دکمه ساخت دیسک نجات کسپرسکی شروع میشود. دیسک نجات کسپرسکی معمولاً بعد از حمله ویروس یا ... که تأثیرات مخربی بر روی سیستم عامل میگذارند و بعضی از فایل‌های رجیستری یا استارت آپ رو از بین میبره و گاهی اوقات در محیط ویندوز قابل حذف نیستند کاربرد دارد. بعد از ایجاد دیسک نجات بر روی فلش یا CD /DVD و Boot able کردن آنها باید سیستم آلوده رو بوسیله فلش یا CD /DVD راه اندازی کرد. بعد از آن باید سیستم آلوده رو اسکن نموده و هرگونه ویروس و ... را از بین برد.

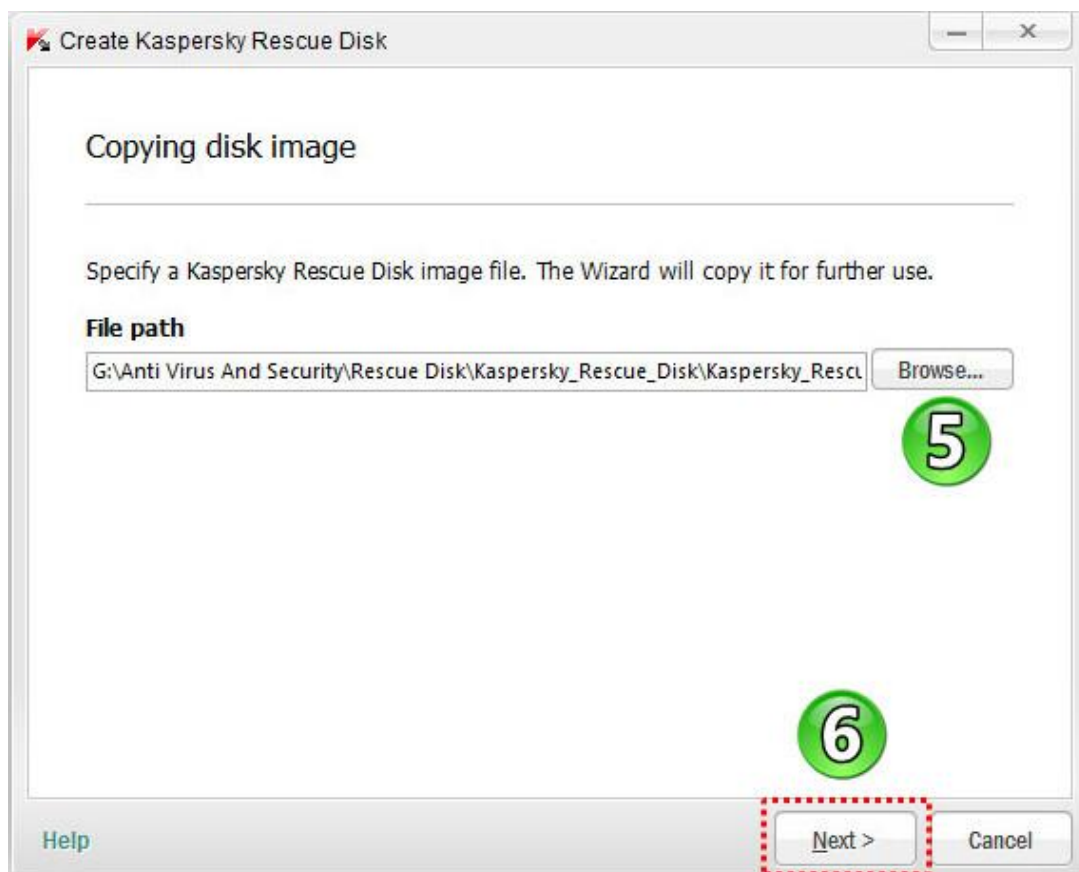
مراحل ایجاد دیسک نجات کسپرسکی :

مراحل طبق اسکرین شات توضیح داده میشود.

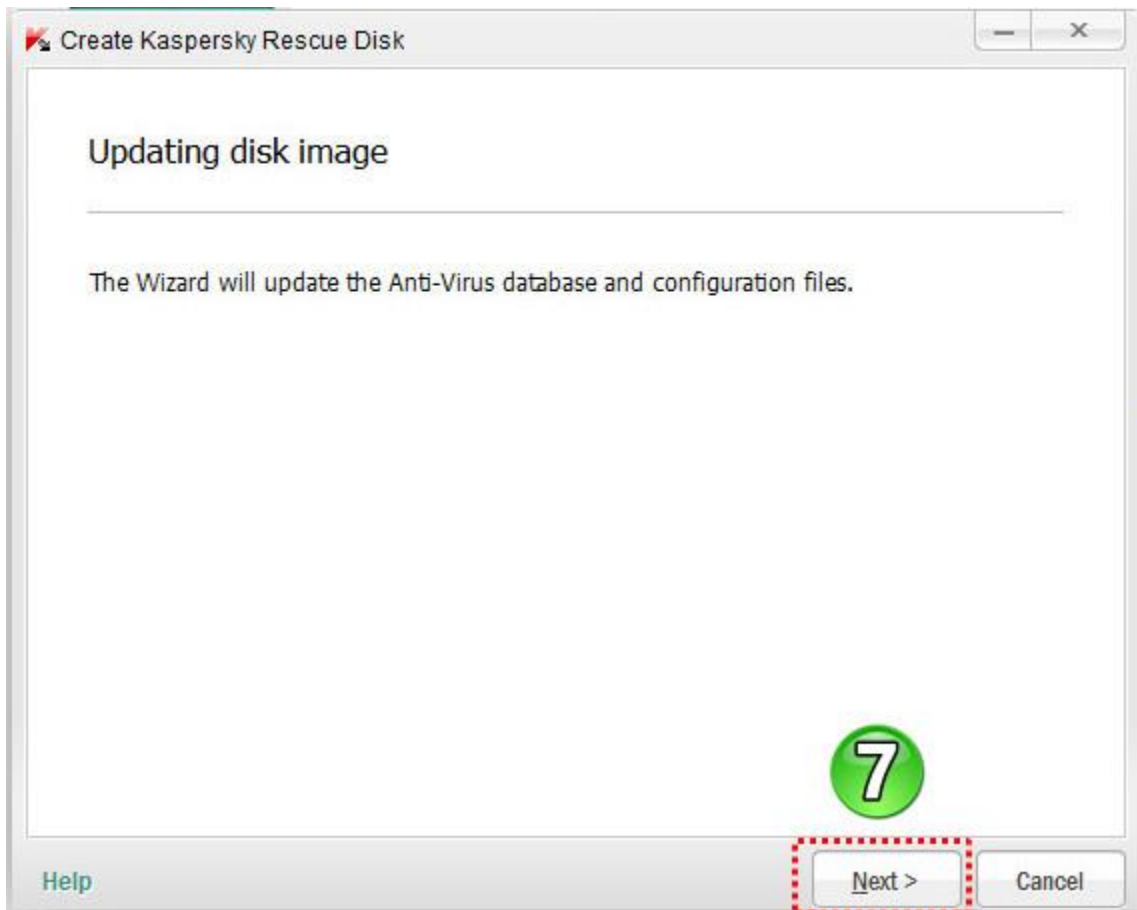
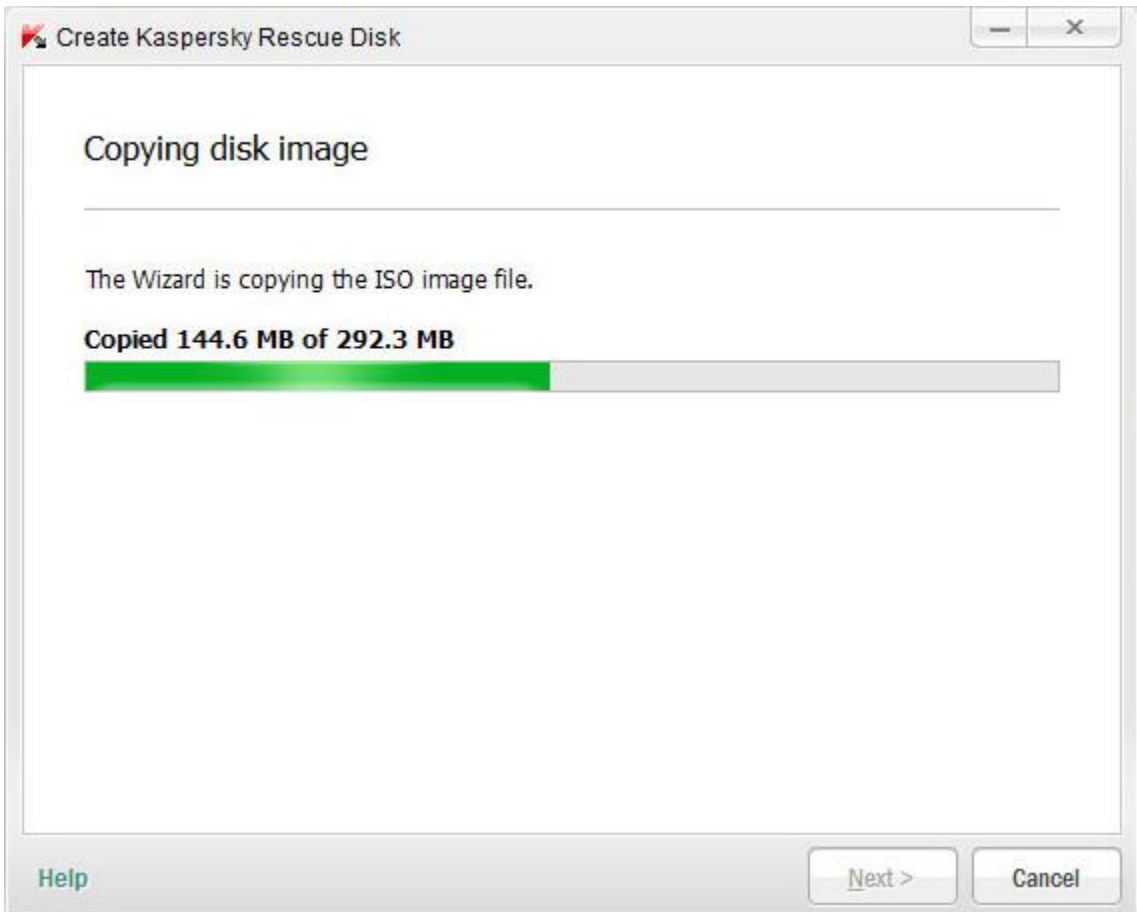




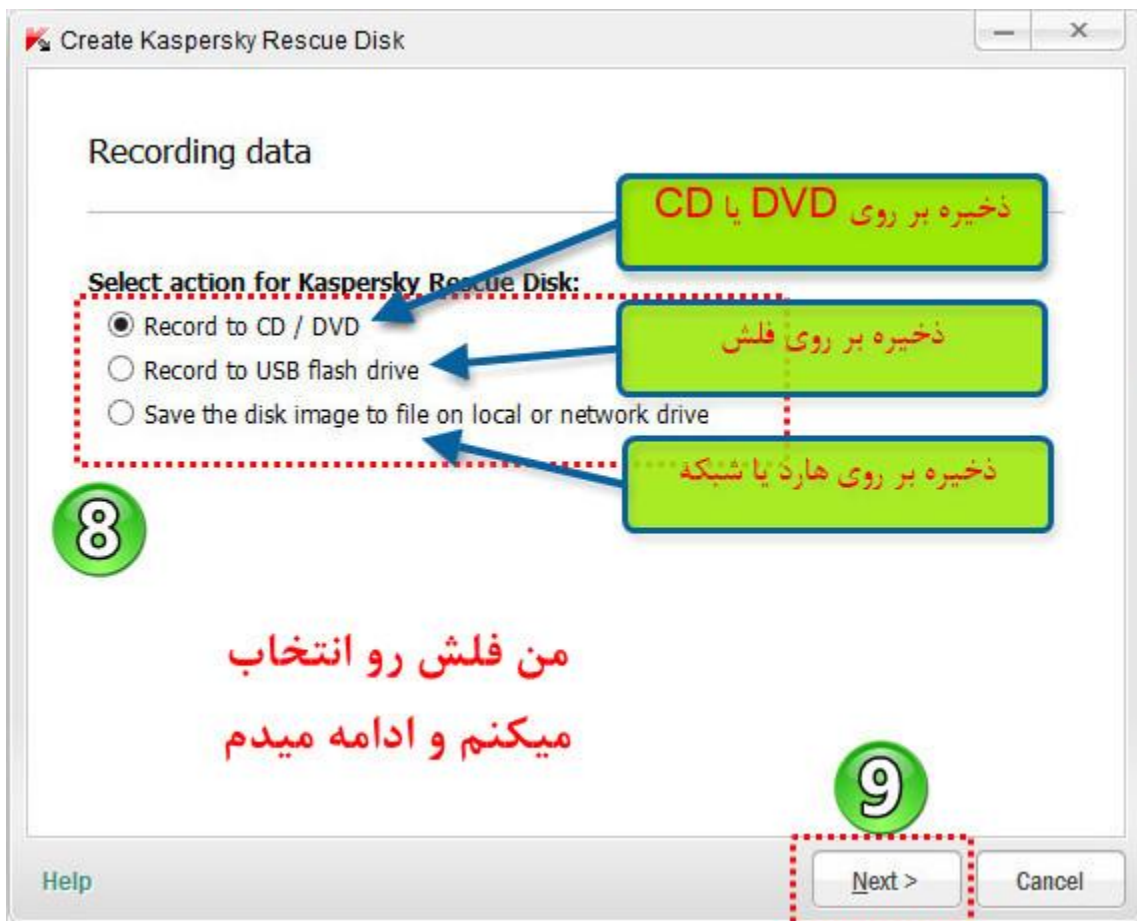
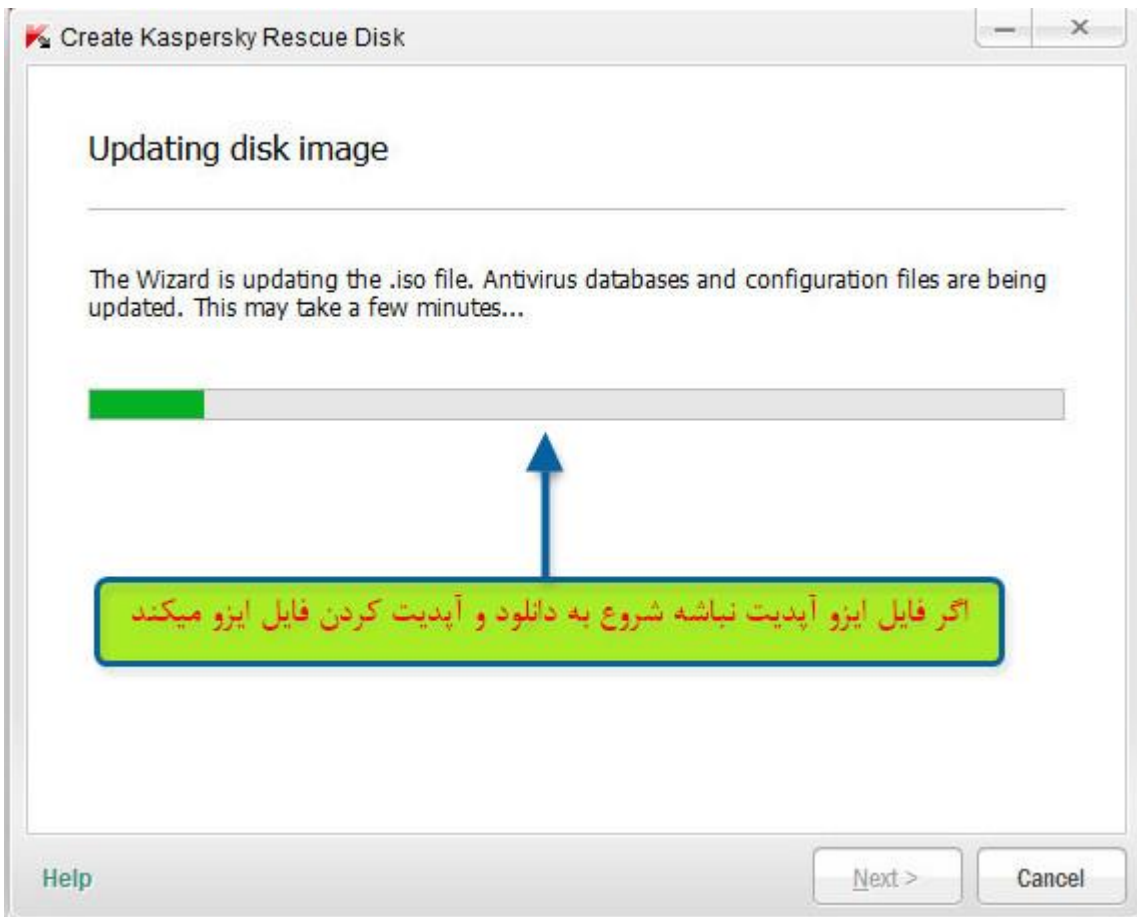
Copy ISO image from local or network drive : کپی ایمیج ISO از درایو هارد یا شبکه  
Download ISO image from Kaspersky Lab server : دانلود ایمیج ISO از سرور آزمایشگاه کسپرسکی  
اگر Copy ISO image from local or network drive انتخاب شود :

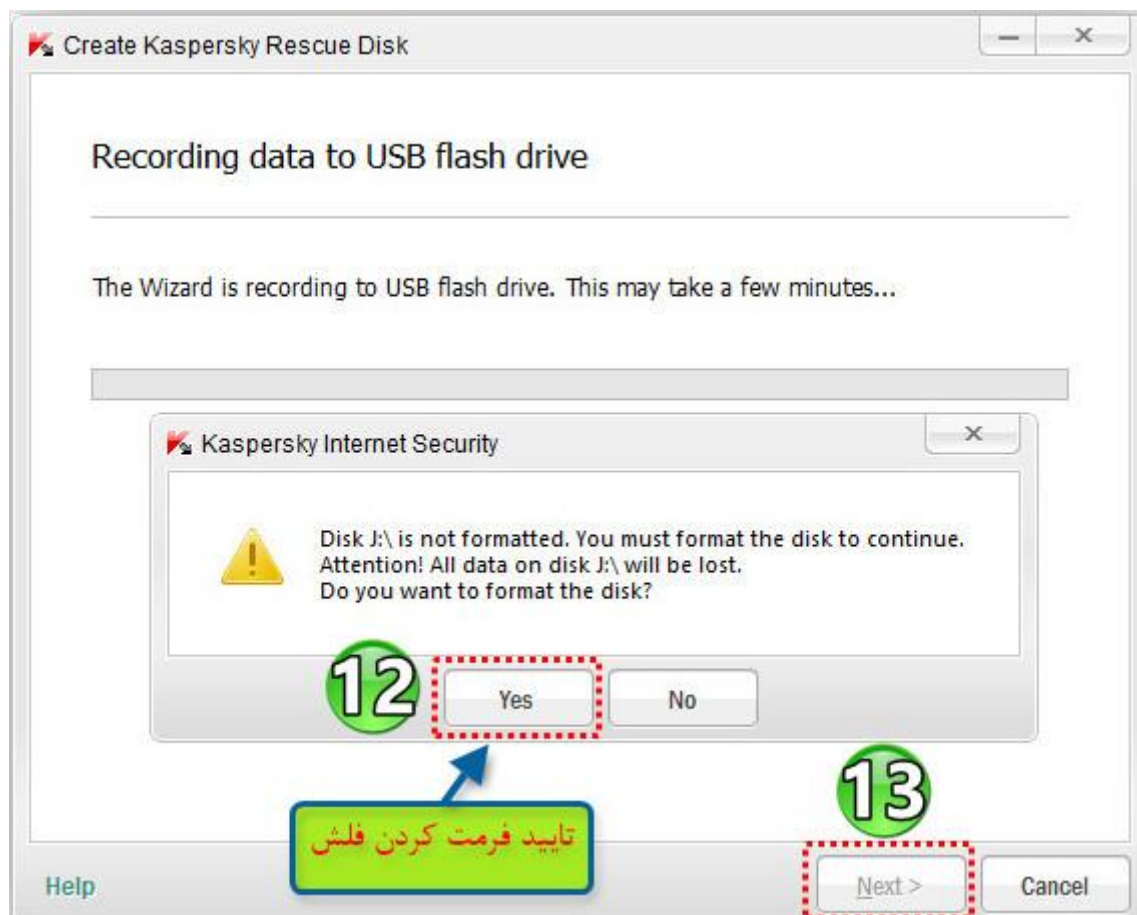
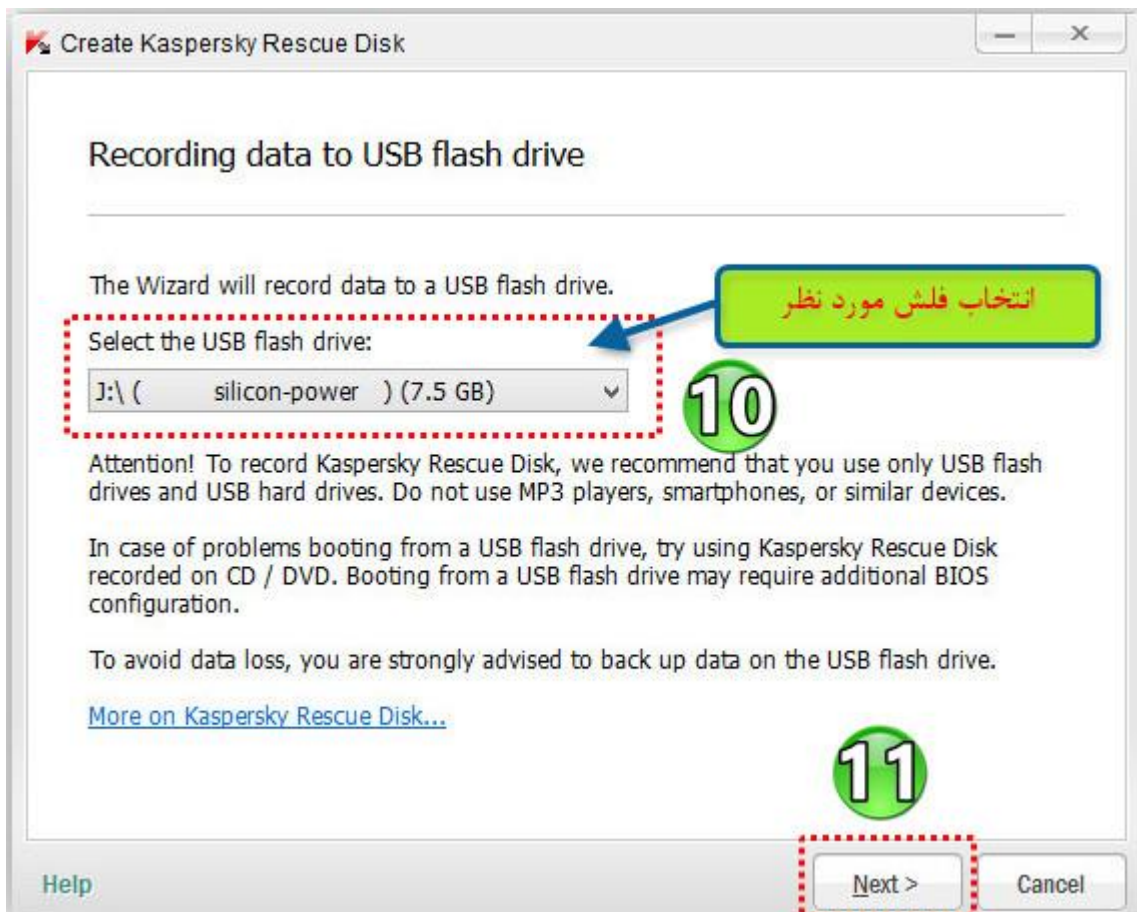


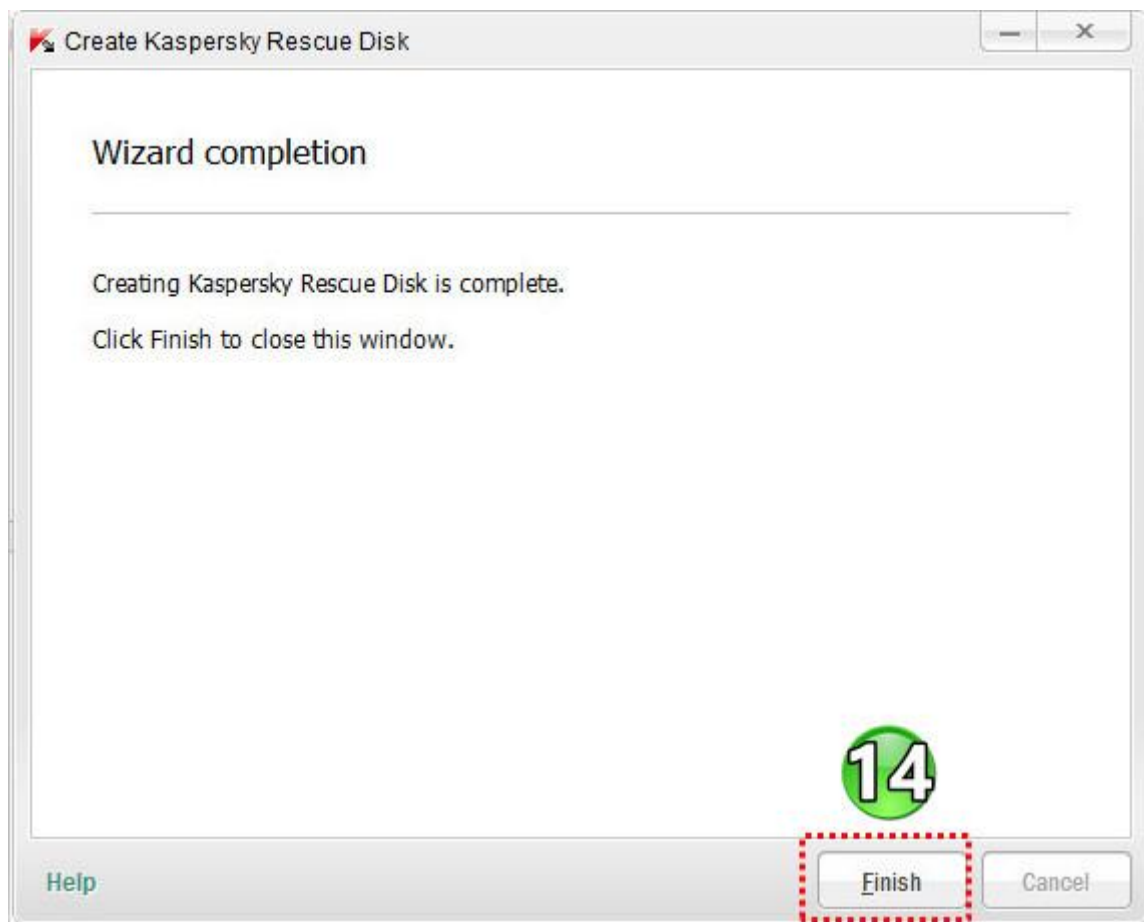
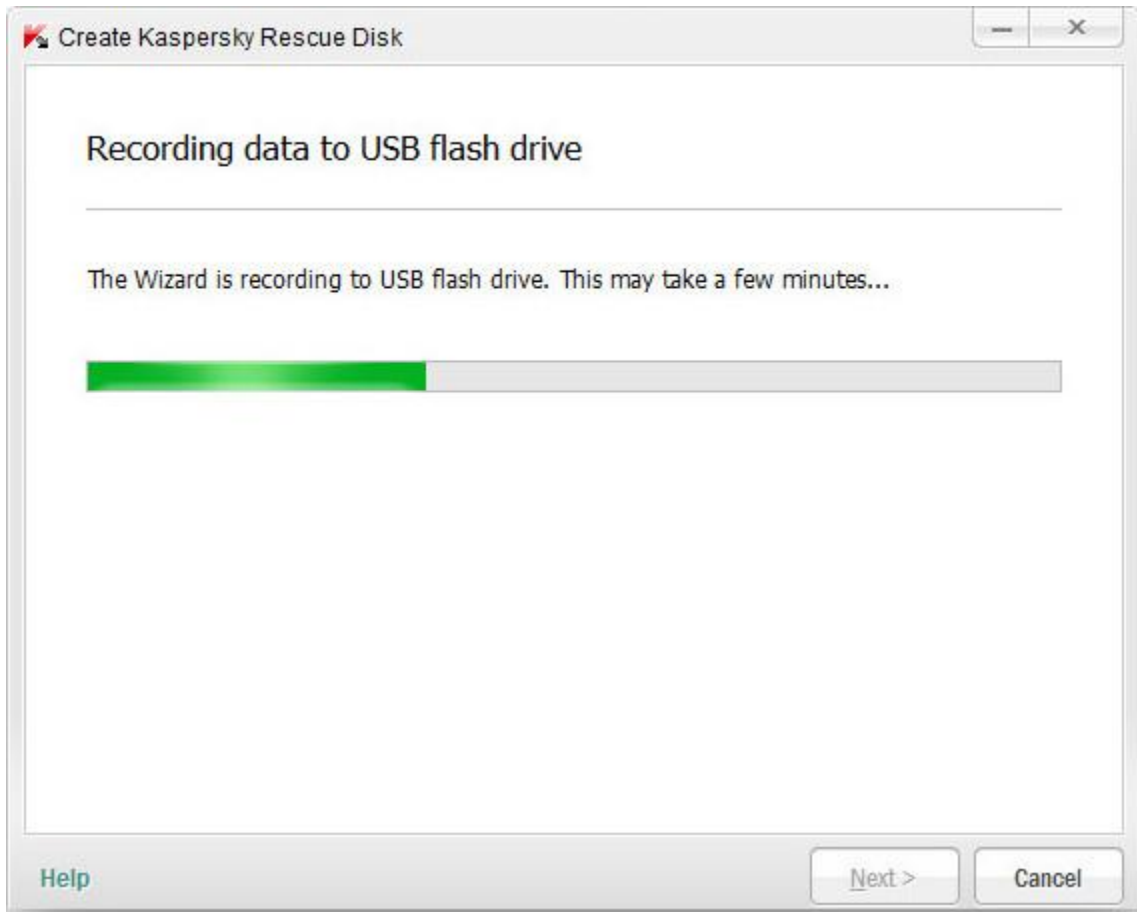




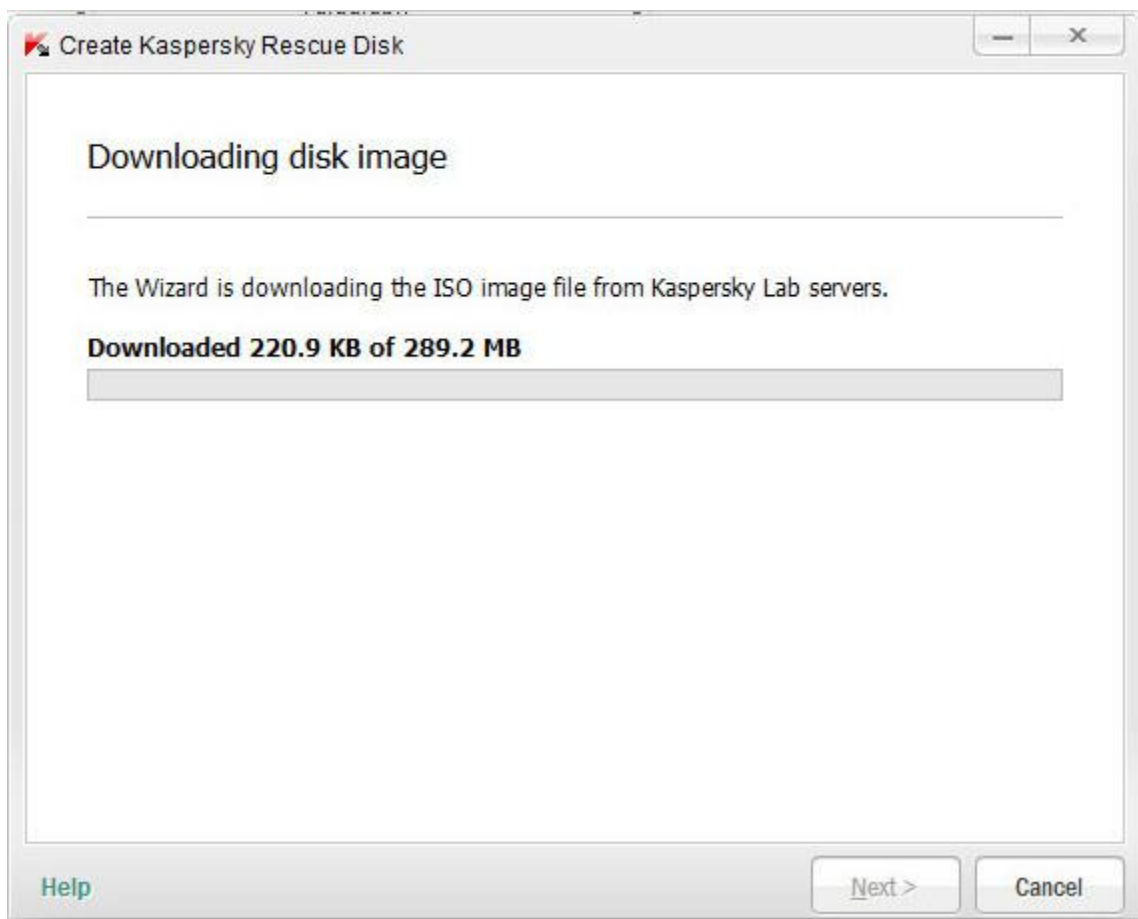








اگر **Download ISO image from Kaspersky Lab server** انتخاب شود : ایچ با فرمت ISO از سرور آزمایشگاه کسپرسکی با حجم تقریبی ۲۸۹ مگابایت دانلود میشود.

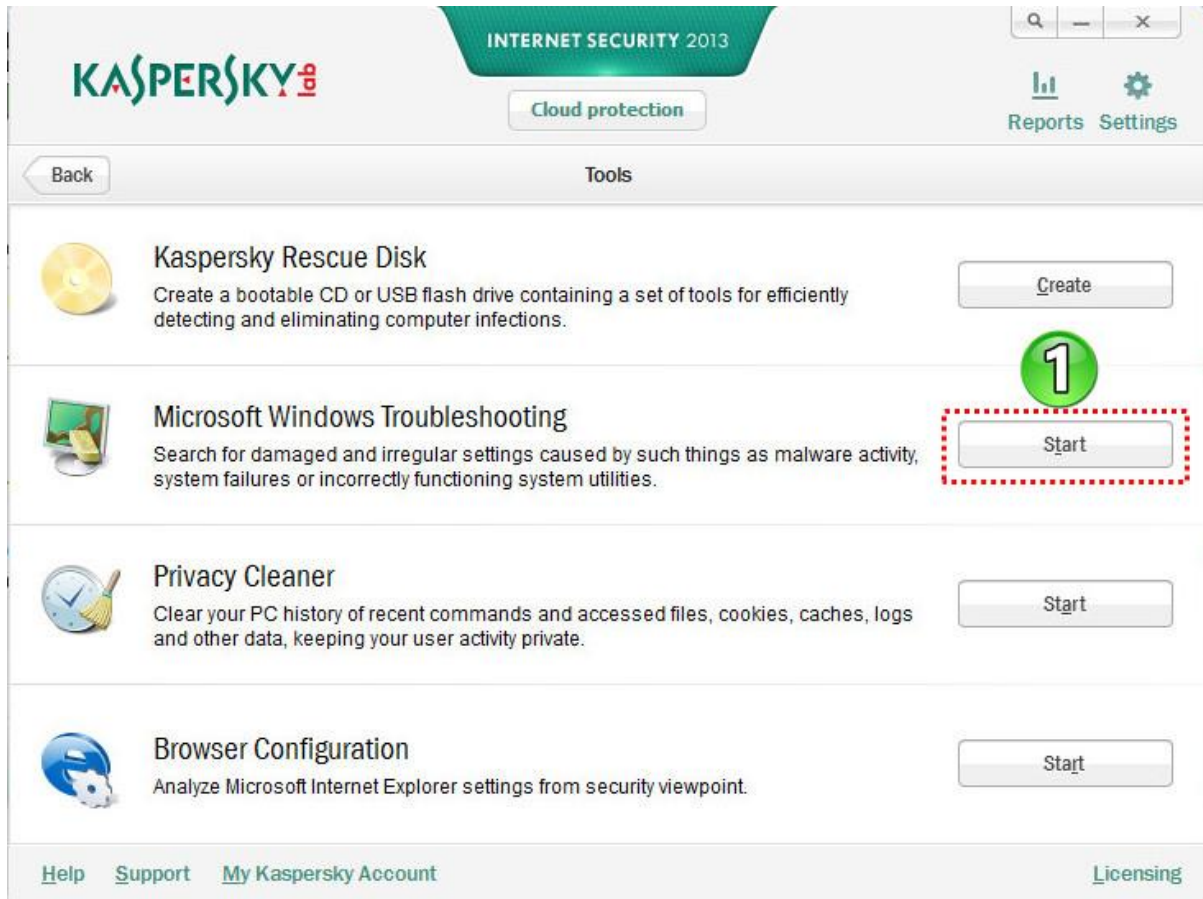


دیگه ادامه مراحل رو نمیگم چون تکراریه و مثل قبلیه

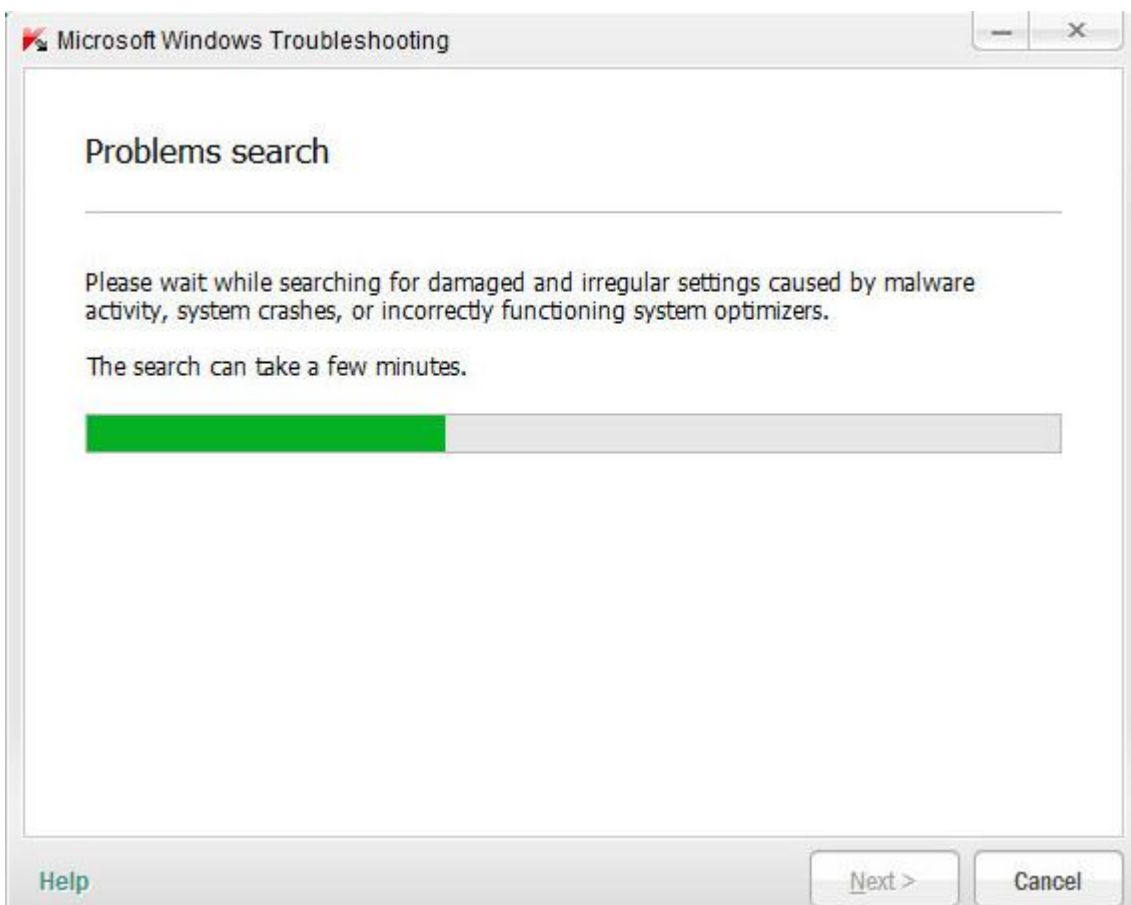
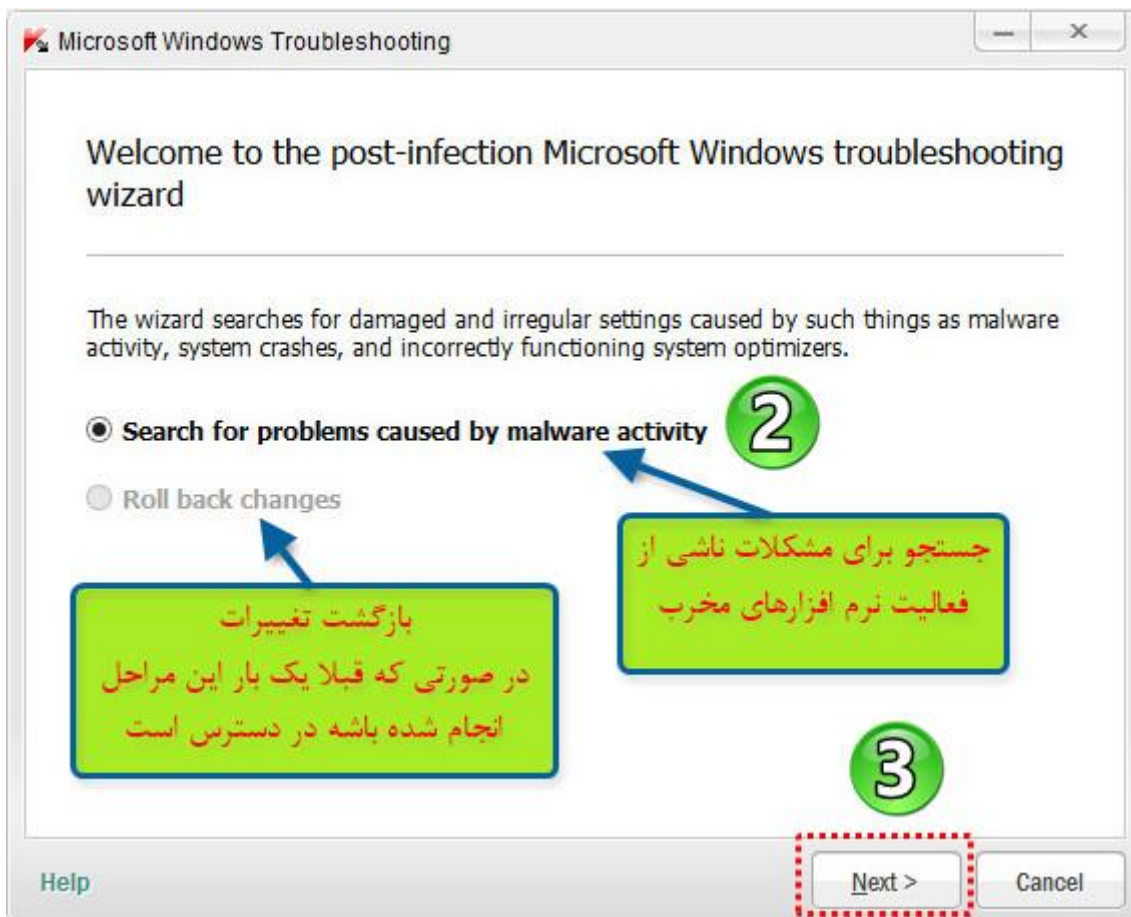
## ۲- عیب یابی ویندوز (Microsoft Windows Troubleshooting)

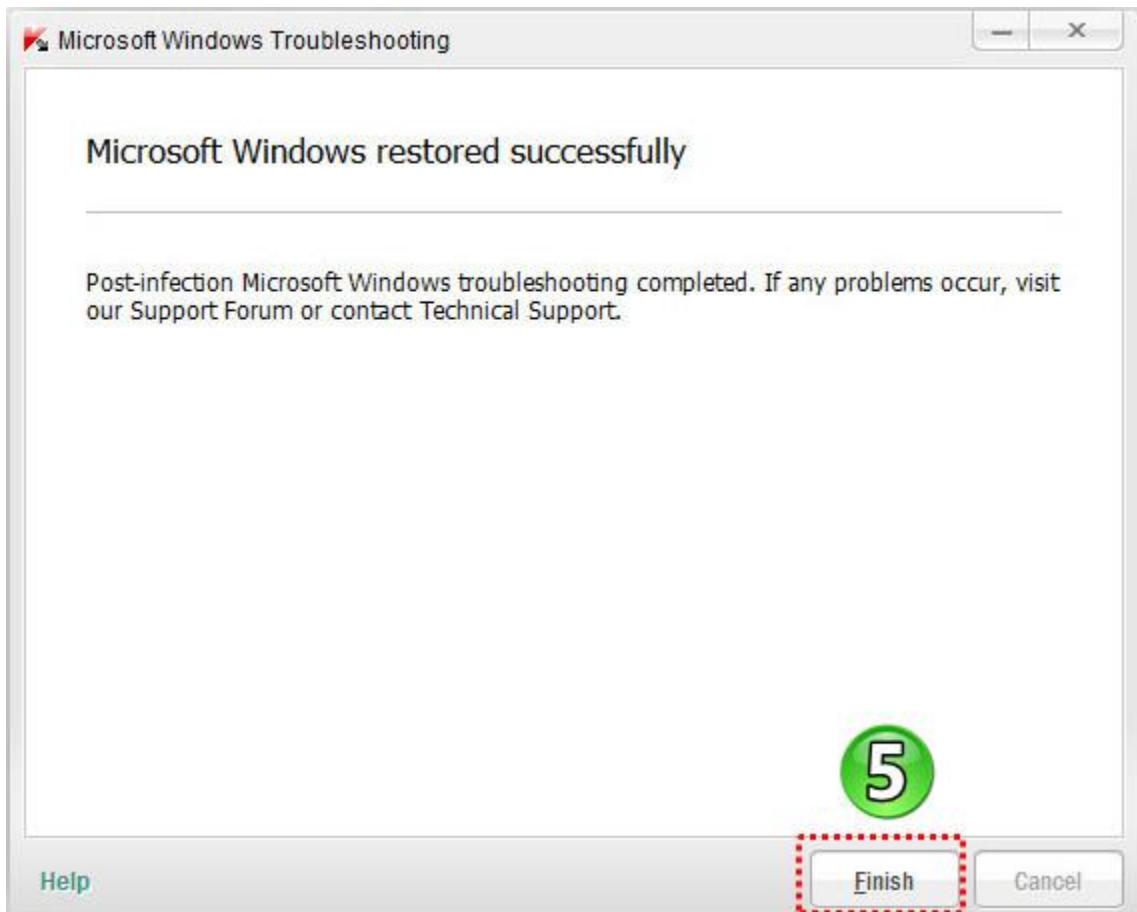
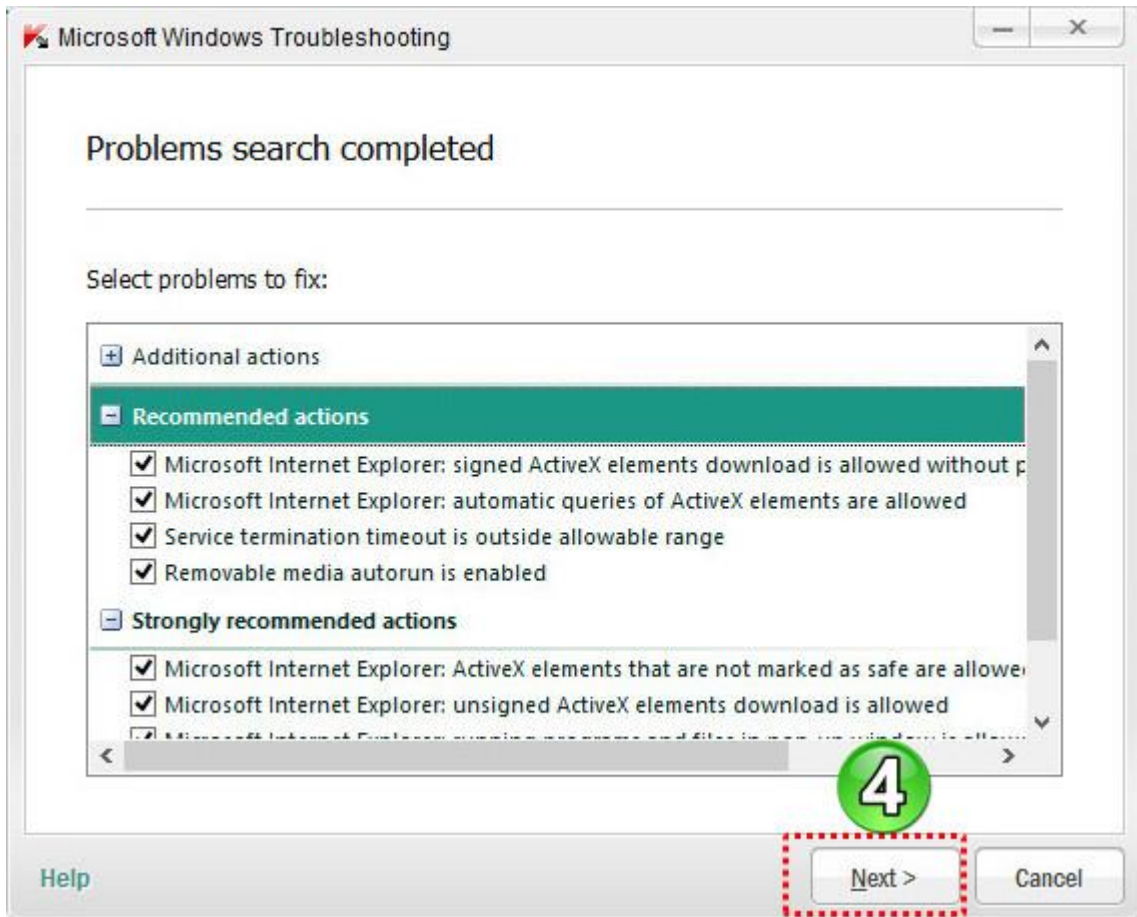
با کلیک کردن بر روی دکمه STSRT شروع به چک کردن تغییرات ویندوز، آنالیز اطلاعات جمع آوری شده و اقدامات لازم برای از بین بردن آثار مخرب میکنند.

مراحل کار طبق اسکرین شات ها









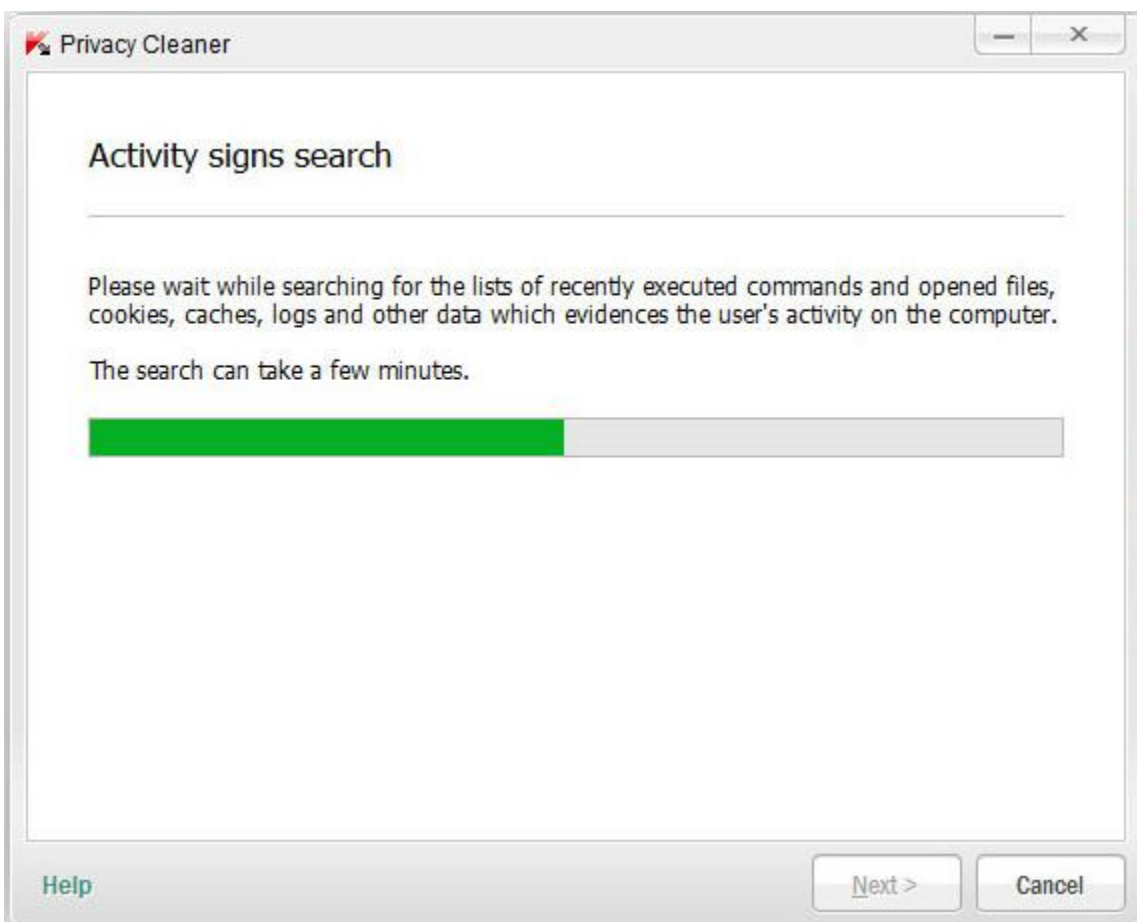
### ۳- پاکسازی حریم خصوصی (Microsoft Windows Troubleshooting)

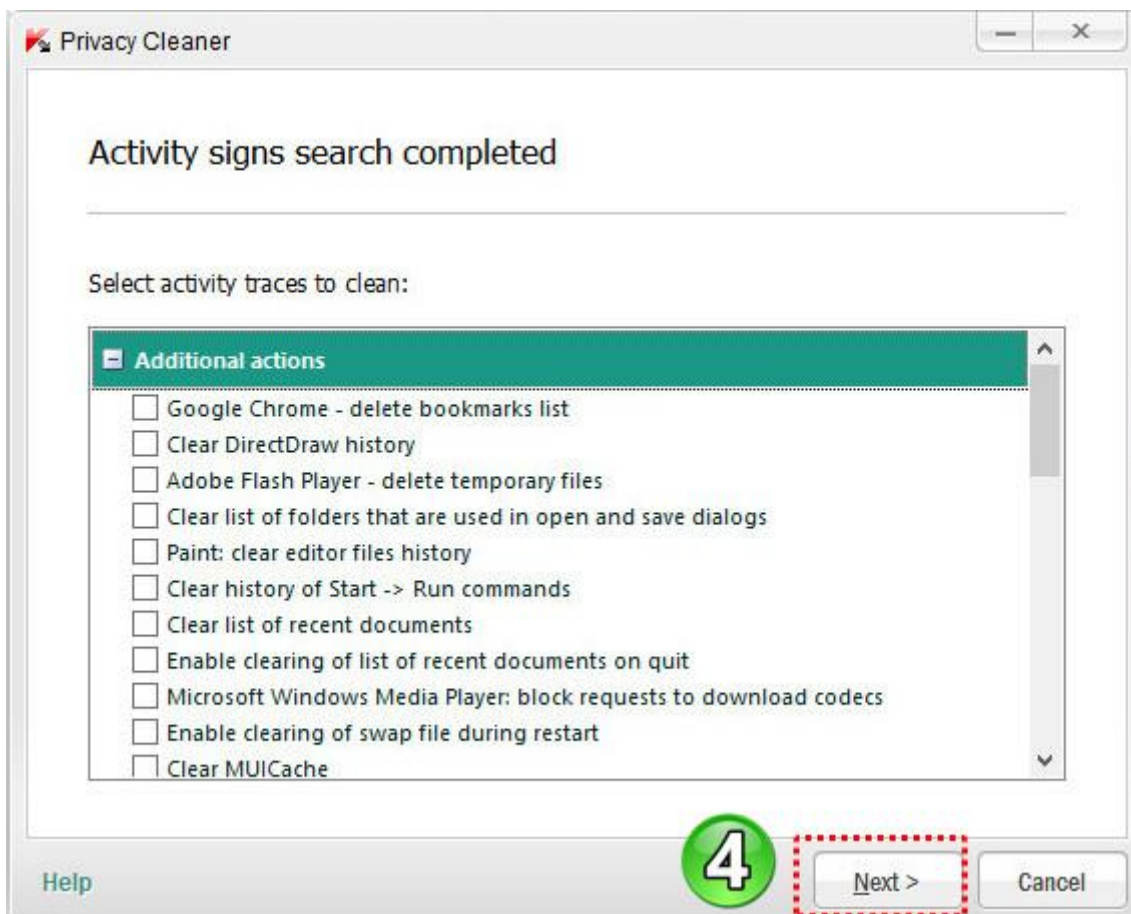
با کلیک کردن روی شروع به حذف آثار فعالیت کاربر در سیستم می‌کند. (برای مثال، تاریخ بازدید از وب سایت ها و یا شروع کار برنامه های کاربردی، فایل های موقت ایجاد شده (temporary files)، و غیره).

مراحل کار طبق اسکرین شات ها

The screenshot shows the 'Tools' section of the Kaspersky Internet Security 2013 interface. The 'Tools' menu is open, displaying four options: 'Kaspersky Rescue Disk', 'Microsoft Windows Troubleshooting', 'Privacy Cleaner', and 'Browser Configuration'. The 'Microsoft Windows Troubleshooting' option is highlighted with a green circle containing the number '1', and its 'Start' button is enclosed in a red dashed box. The interface includes a search bar, 'Cloud protection' button, 'Reports' and 'Settings' links, and a footer with 'Help', 'Support', 'My Kaspersky Account', and 'Licensing' links.

Tool Name	Description	Action
Kaspersky Rescue Disk	Create a bootable CD or USB flash drive containing a set of tools for efficiently detecting and eliminating computer infections.	Create
Microsoft Windows Troubleshooting	Search for damaged and irregular settings caused by such things as malware activity, system failures or incorrectly functioning system utilities.	Start
Privacy Cleaner	Clear your PC history of recent commands and accessed files, cookies, caches, logs and other data, keeping your user activity private.	Start
Browser Configuration	Analyze Microsoft Internet Explorer settings from security viewpoint.	Start





این لیست شامل آثار فعالیت ها و روش های برای از بین بردن آنها است. این لیست شامل سه گروه از اقدامات برای از بین بردن آثار فعالیت های اینترنتی میباشد:

**Additional actions** - اقدامات اضافی برای از بین بردن آثار فعالیت هایی که خطرناک نیستند.

**Recommended actions** - اقدامات توصیه شده برای حذف آثار فعالیت های که یک تهدید بالقوه محسوب میشوند.

**Strongly recommended actions** - اقداماتی که به شدت توصیه می شود و برای حذف آثار فعالیت هایی که به عنوان

یک تهدید امنیتی جدی محسوب میشوند.

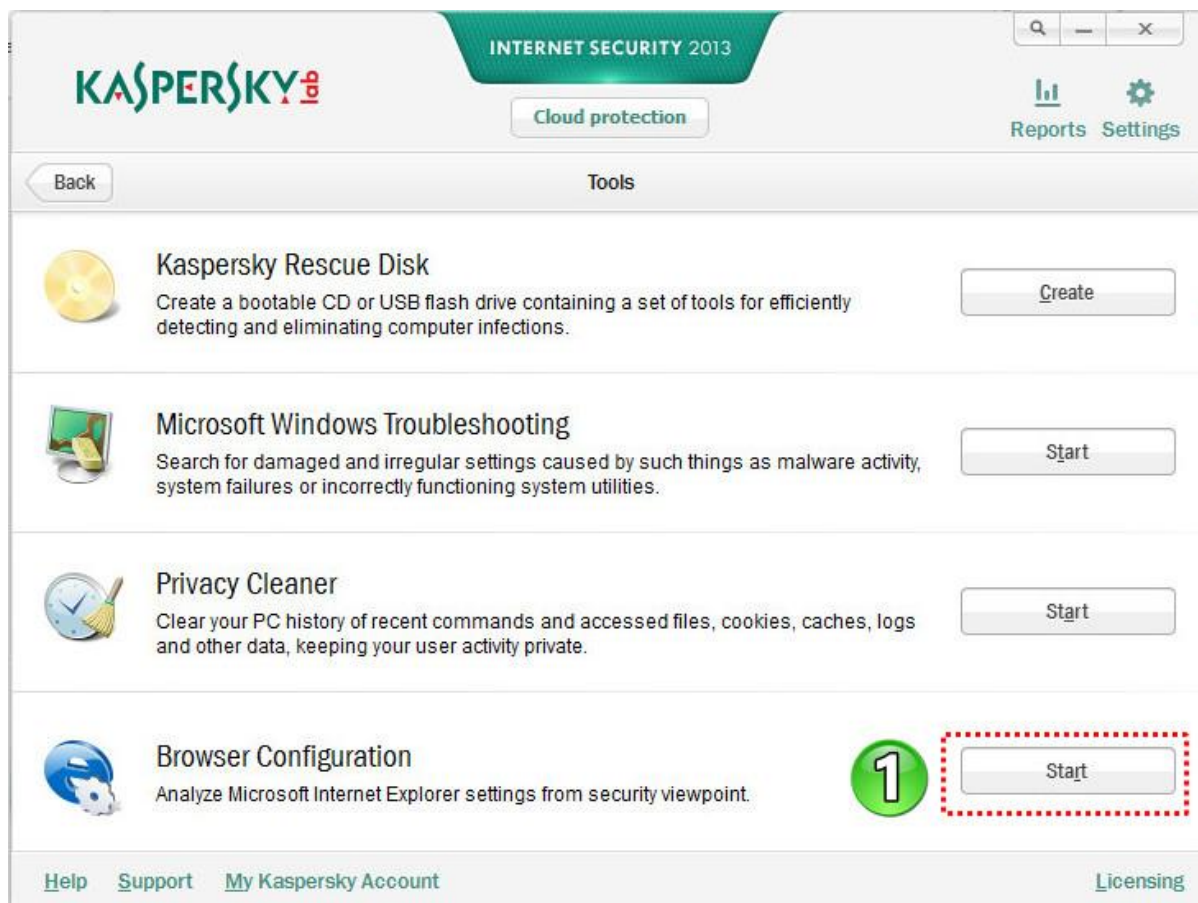
و در آخر روی **FINISH** کلیک میکنیم.

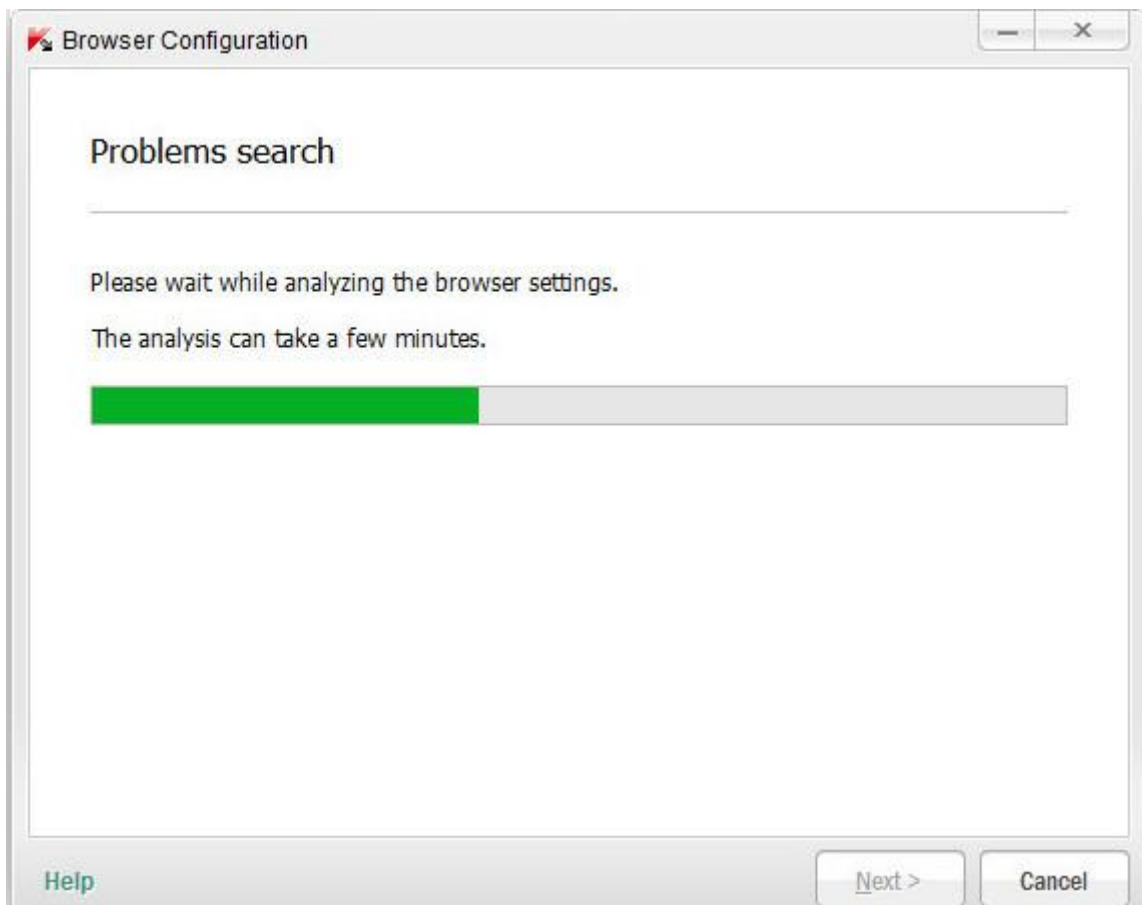
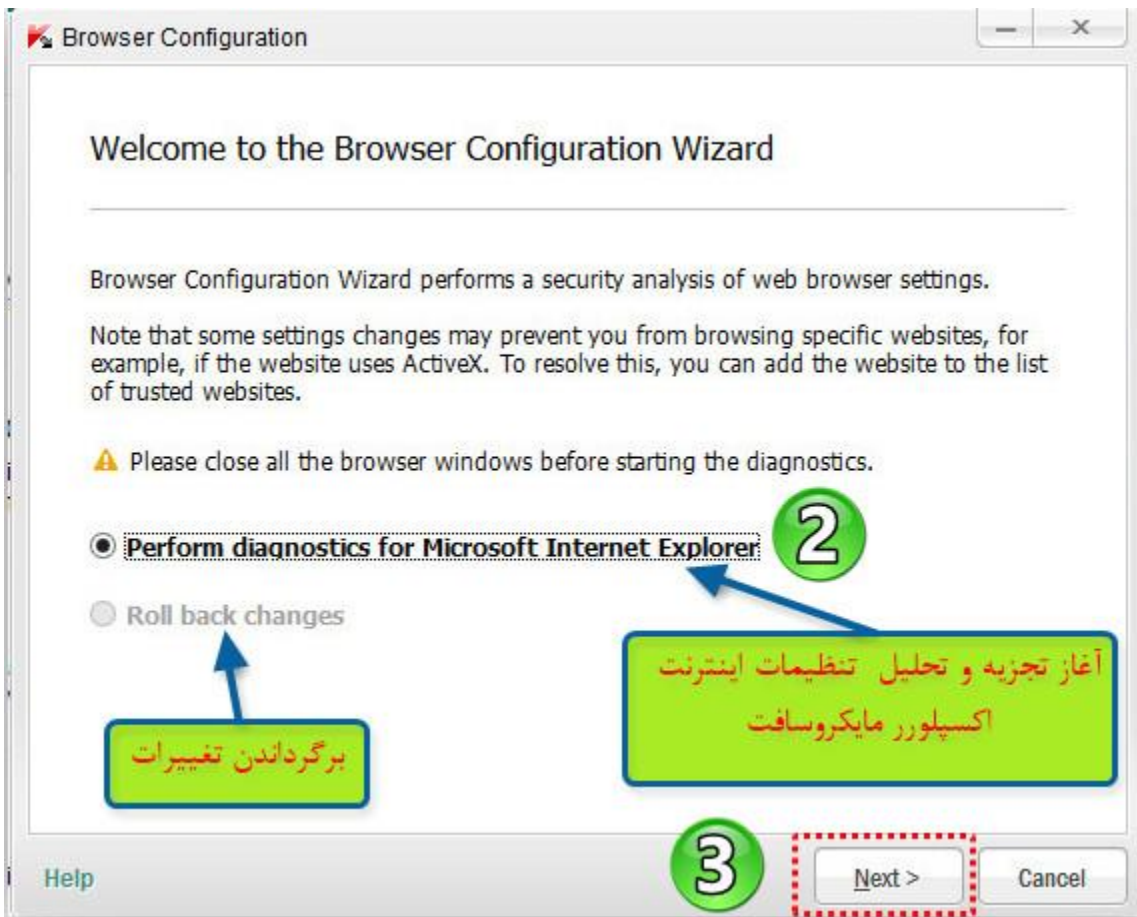


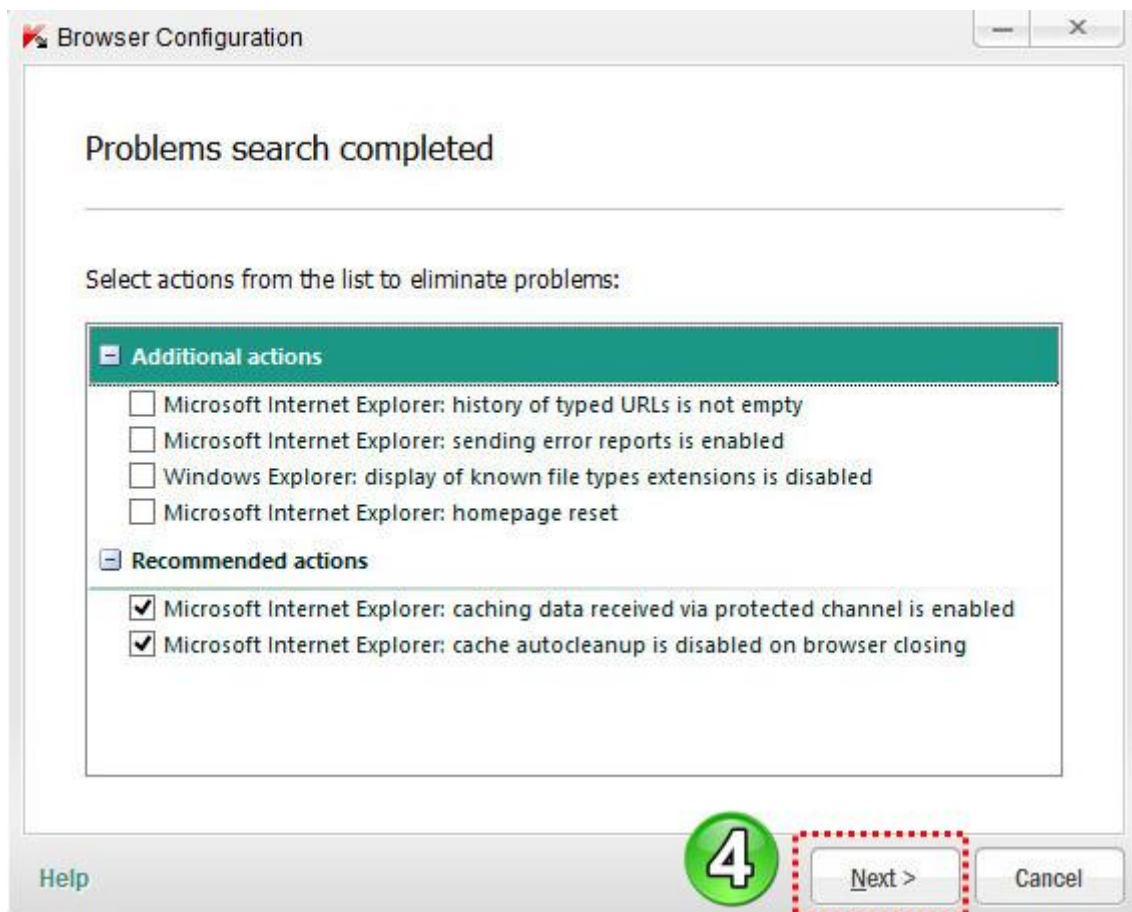
## ۴- پیکربندی مرورگر (Browser Configuration)

با کلیک کردن روی دکمه شروع به تجزیه و تحلیل تنظیمات امنیتی مایکروسافت اینترنت اکسپلورر می‌کند.

مراحل کار طبق اسکرین شات‌ها







لیست آسیب پذیری های شناسایی شده در مرحله قبلی نمایش داده میشود. آسیب پذیری یافت شده توسط کسپرسکی اینترنت سکیوریتی بر اساس نوع خطر آنها گروه بندی می شوند.

**Additional actions** - اقدامات اضافی طراحی شده برای رفع آسیب پذیری های مرورگر، که در حال حاضر بعنوان یک تهدید مطرح نیست اما می تواند امنیت کامپیوتر در آینده تهدید کند.

**Recommended actions** - کمک به از بین بردن مشکلاتی که به عنوان یک تهدید بالقوه محسوب میشوند.

**Strongly recommended actions** - به شدت این اقدامات توصیه می شود و به از بین بردن تهدیدات امنیتی جدی کمک میکند.

و در آخر روی **FINISH** کلیک میکنیم.

# تنظیمات Kaspersky Internet Security 2013

تنظیمات Kaspersky Internet Security 2013 شامل چهار سر برگ زیر میشود که هر کدام بصورت جداگانه

توضیح داده میشود:

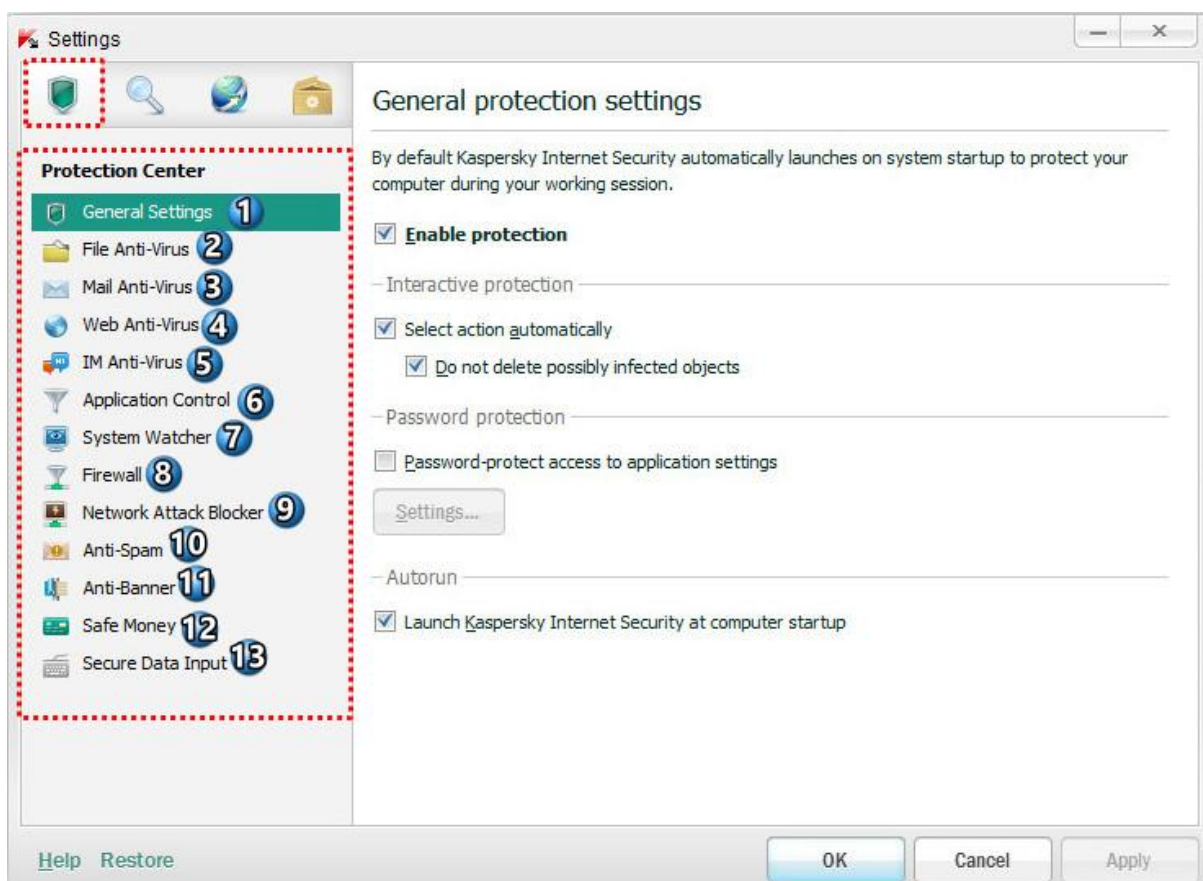
۱- سر برگ Protection Center

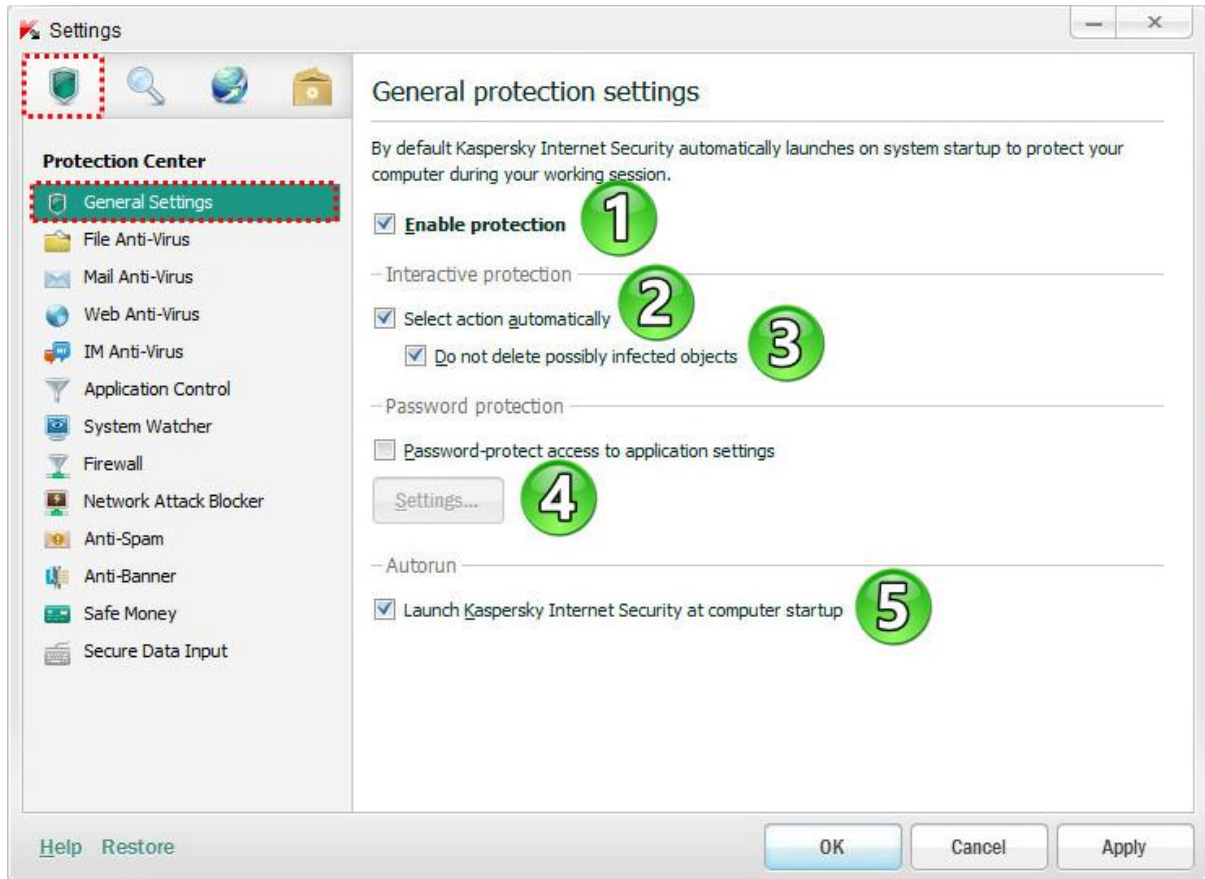
۲- سر برگ Scan

۳- سر برگ Update

۴- سر برگ Advanced Setting

## ۱- سر برگ Protection Center





### ۱- فعال سازی اجزاء حفاظتی

غیر فعال کردن این قسمت وظایف اسکن ویروس و بروز رسانی های امنیتی کسپرسکی را تحت تاثیر قرار نمی دهد.

### ۲- انتخاب عملکرد بصورت خودکار

**KIS** به دو صورت با کاربر ارتباط برقرار میکند :

**Interactive protection mode** (حالت حفاظت تعاملی) : **KIS** تمام رویدادهای خطرناک و مشکوک را به اطلاع کاربر

میرساند. در این حالت، کاربر به طور مستقل تصمیم می گیرد که به عملیات موجود اجازه دهد یا از آن جلوگیری کند.

**Automatic protection mode** (حالت حفاظت های اتوماتیک ) : اگر حتی یک رویداد خطرناک رخ دهد، **KIS** به

طور خودکار عمل میکند.

۳- **Do not delete probably infected objects** : با فعال کردن این گزینه زمانی که **KIS** در حالت اتوماتیک

است، مواردی که مشکوک به آلودگی هستند را حذف نمی کند.

۴- **Enable password protection** : با فعال کردن این قسمت دسترسی به تنظیمات **KIS** با پسوردی که خودمان

تعیین میکنیم را محدود میکنیم.

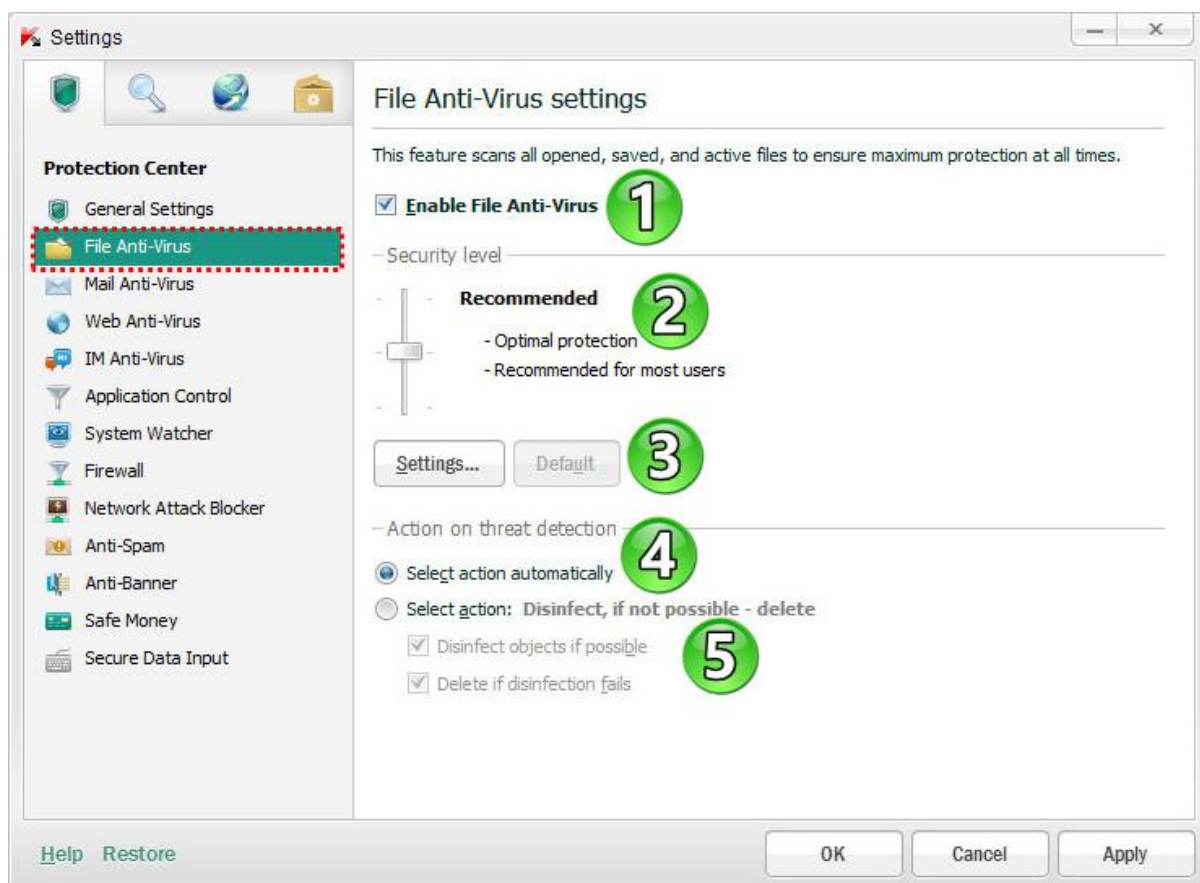
**Setting** : قسمت تنظیمات در اسکرین شات توضیح داده شده است.





۵- **Launch Kaspersky Internet Security at computer startup** : فعال سازی Kaspersky Internet Security

در Security Startup ( اجرای KIS در زمان راه اندازی ویندوز)



۱- **Enable File Anti-Virus (فعال کردن آنتی ویروس فایل):** با فعال شدن این قسمت ، **File Anti-Virus** در

سیستم عامل و بر روی حافظه (RAM) راه اندازی می شود و تمام فایل هایی که باز یا ذخیره و یا در حال اجرا هستند را اسکن می کند.

۲- **Security level (سطح امنیتی):** در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را برای فایل ها و حافظه انتخاب کرد.

**High (زیاد):**

در این سطح امنیتی، ضد ویروس فایل دقیق ترین کنترل را برای تمام فرمت های فایل باز، ذخیره شده و در حال اجرا، اعمال می کند. ضد ویروس فایل تمام فایل های روی هارد دیسک، درایوهای شبکه، USB، آرشوها و فایل های نصب (installer packages) را اسکن میکند.

**Recommended (توصیه شده):**

این سطح امنیتی، تعادل مطلوب بین عملکرد و امنیت سیستم را تضمین می نماید و برای بیشتر مواقع مناسب است. در این حالت ، ضد ویروس فایل فقط فرمت فایل های مشخص شده را در هارد دیسک ، درایوهای شبکه و USB اسکن میکند. همچنین **heuristic analysis** (تجزیه و تحلیل اکتشافی) را نیز انجام میدهد. **در این حالت (installer packages) فایل های نصب و آرشو اسکن نمی شود.**

**heuristic analysis:** یک تکنولوژی برای تشخیص اطلاعات موارد تهدیدکننده ای که هنوز در دیتابیس لابراتوار کسپرسکی

موجود نیست. **heuristic analysis** مواردی که ممکن است تهدیدی برای امنیت سیستم باشد را تشخیص میدهد. برای مثال، ممکن است یک فایل که شامل توالی از دستورات موارد مخرب باشد.

### Low (کم):

در این سطح امنیتی، فقط فایل های با پسوند مشخص شده در تمام هارد دیسک، USB، و درایوهای شبکه ای کامپیوتر اسکن میشود و **heuristic analysis** (تجزیه و تحلیل اکتشافی) سطحی است.

در این حالت اجزاء فایل ها اسکن نمی شود.

در این حالت میتوان حداکثر سرعت اسکن را داشت.

**۳-Setting (تنظیمات):** با کلیک بر روی این دکمه پنجره تنظیمات باز میشود.

### سربرگ General:



۱- **File types:** در قسمت نوع فایلی که آنتی ویروس باید اسکن را می توان انتخاب کرد. تنظیمات پیش فرض در این بخش به سطح امنیتی انتخاب شده (High ، Recommended ، Low) بستگی دارد و شامل ۳ قسمت زیر میشود:

**All files:** تمامی فایلها بدون استثناء (در سطح امنیتی High پیش فرض است)

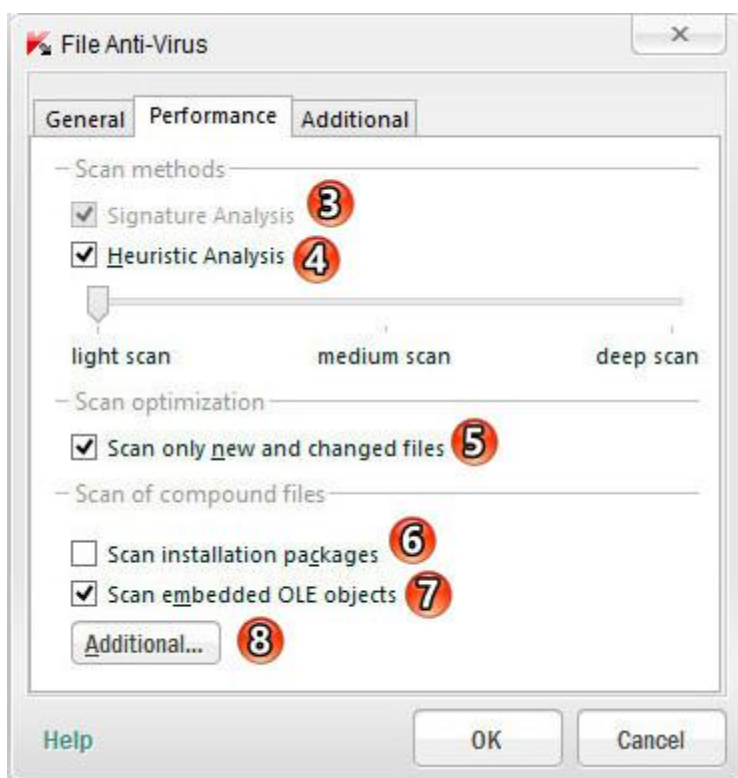
**Files scanned by format:** فقط فایلهایی که یک ویروس میتواند به آن نفوذ کند را اسکن میکند. (در سطح امنیتی Recommended پیش فرض است)

**Files scanned by extension:** فقط فایلهایی که بر اساس فرمتشان تعیین شده اند اسکن میشود. (در سطح امنیتی Low پیش فرض است)

۲- **Protection scope:** لیست محدوده حفاظت

در این لیست می توان مواردی که باید اسکن شود را تعیین کرد. ( تمام هارد دیسکها، تمام درایوهای شبکه، تمامی درایوهای ( removable

## سربرگ Performance :



**Scan methods :** روش های اسکن فایل برای آنتی ویروس

تنظیمات پیش فرض این بخش به سطح امنیتی انتخاب شده بستگی دارد.

**۳- Signature Analysis :** پایگاه داده کسپرسکی ، که شامل توضیحات تهدیدات شناخته شده و روش برای از بین بردن آنها میشود، حداقل سطح قابل قبول از امنیت را فراهم می کند.

بنا بر توصیه های کارشناسان لابراتوار کسپرسکی، این روش همیشه خود به خود فعال است.

**۴- Heuristic Analysis :** فعال کردن (تجزیه و تحلیل اکتشافی) حین اسکن برای ویروس

**Slider :** شامل سه سطح زیرمیشود :

**Light scan :** اسکن سبک

**Medium scan :** اسکن متوسط

**Deep scan :** اسکن عمیق

**۵- Scan only new and changed files :** فقط اسکن فایل های جدید و تغییر یافته

باتیکدار بودن این قسمت تنها فایل های جدید و فایل هایی که پس از آخرین باری که آنها اسکن شده اند ، تغییر کرده اند، اسکن میشوند.

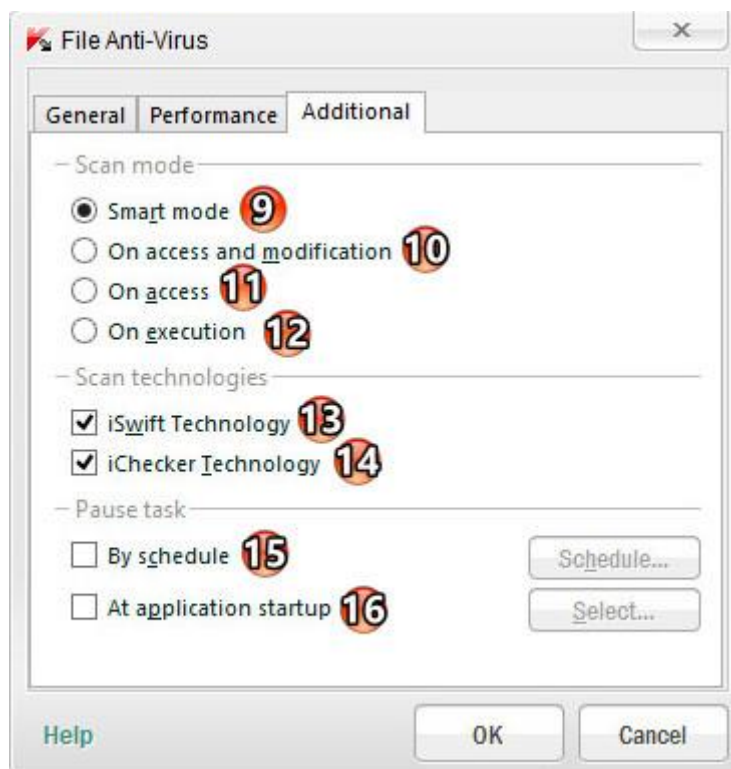
**۶- Scan installation packages :** اسکن بسته های نصب

با تیکدار بودن این قسمت، فایل های نصب اسکن میشود. اگر اسکن تیک بزنی فقط فایل های جدید و تغییر جعبه در بخش بهینه سازی اسکن پاک، شما می توانید هر یک از گزینه های اسکن را انتخاب کنید: همه اسکن تمام فایل های نصب و راه اندازی. جدید اسکن فایل ها فقط نصب جدید که از آخرین اسکن ظاهر شد.

**۷- Scan embedded OLE objects:** با تیکداربودن این قسمت اشیاء OLE تعبیه شده در فایل ها (مانند صفحات گسترده میکروسافت آفیس اکسل و یا ماکروها جاسازی شده در فایل های میکروسافت آفیس ورد، فایل پیوست ایمیل) توسط کسپرسکی اینترنت سکیوریتی اسکن میشود.

**۸- Additional:** با کلیک کردن روی این دکمه پنجره ای باز می شود که در آن می توانید اسکن فایل های ترکیبی را پیکربندی کنید.

**سربرگ Additional:**



**Scan mode:** حالت های اسکن که شامل ۴ قسمت میشود:

- ۹- Smart mode (حالت هوشمند):** در این حالت، آنتی ویروس یک مورد را بر اساس تجزیه و تحلیل اقدامات صورت گرفته روی فایل، اسکن میکند.
- به عنوان مثال، در هنگام کار با یک سند آفیس، آنتی ویروس فایل را زمانی که برای **اولین بار باز یا آخرین بار بسته** شده است، اسکن میکند.
- ۱۰- On access and modification (دسترسی و اصلاح):** در این حالت، آنتی ویروس مواردی که برای **باز شدن** تلاش میکنند و همچنین **تغییر آنها** را اسکن میکند.
- ۱۱- On access:** در این حالت، آنتی ویروس مواردی را که برای **باز شدن** تلاش میکنند، را اسکن میکند.
- ۱۲- On execution:** در این حالت، آنتی ویروس مواردی را که برای **اجرا** تلاش میکنند، را اسکن میکند.

**۱۳- iSwift Technology ( فناوری iSwift ):** این فن آوری حالت توسعه یافته فن آوری iChecker برای کامپیوترهایی که از یک فایل سیستم NTFS استفاده میکنند، کاربرد دارد.



**۱۴- iChecker Technology ( فناوری iChecker ) :** این فن آوری باعث افزایش سرعت اسکن توسط حذف فایل های خاصی از اسکن میشود.(منظور این است که یک سری از فایلها از چرخه اسکن خارج میشود و این باعث افزایش سرعت اسکن میشود.)

فایلی که از چرخه اسکن خارج میشود با استفاده از یک الگوریتم خاص مشخص میشود که به تاریخ انتشار دیتابیس KIS ، تاریخ فایلی که آخرین بار اسکن شده بود، و هر گونه تغییرات در تنظیمات اسکن بستگی دارد . محدودیتهایی که برای iChecker وجود دارد: iChecker با فایل های بزرگ کار نمی کند و تنها به فایل هایی با ساختاری که برنامه به رسمیت می شناسد، اعمال میشود.(به عنوان مثال: .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar)

**۱۵- By schedule :** این قسمت اجازه توقف آنتی ویروس را برای یک بازه زمانی مشخص میدهد. این قسمت برای کاهش حجم کار سیستم و فراهم آوردن امکان دسترسی سریعتر به object ها کاربرد دارد.

**۱۶- At application startup :** با فعال کردن این قسمت ، آنتی ویروس ، هنگام اجرای برنامه های مشخص شده ، متوقف میشود. (برای مثال، کسانی که نیاز به منابع سیستمی قابل توجهی دارند.) پس از اینکه برنامه بسته شود، آنتی ویروس به طور خودکار دوباره فعال میشود.

با کلیک بر روی این دکمه پنجره ای باز می شود که در آن می توانید یک لیست از برنامه های کاربردی را انتخاب کنید که زمانیکه در حال اجرا هستند ، آنتی ویروس متوقف شود.

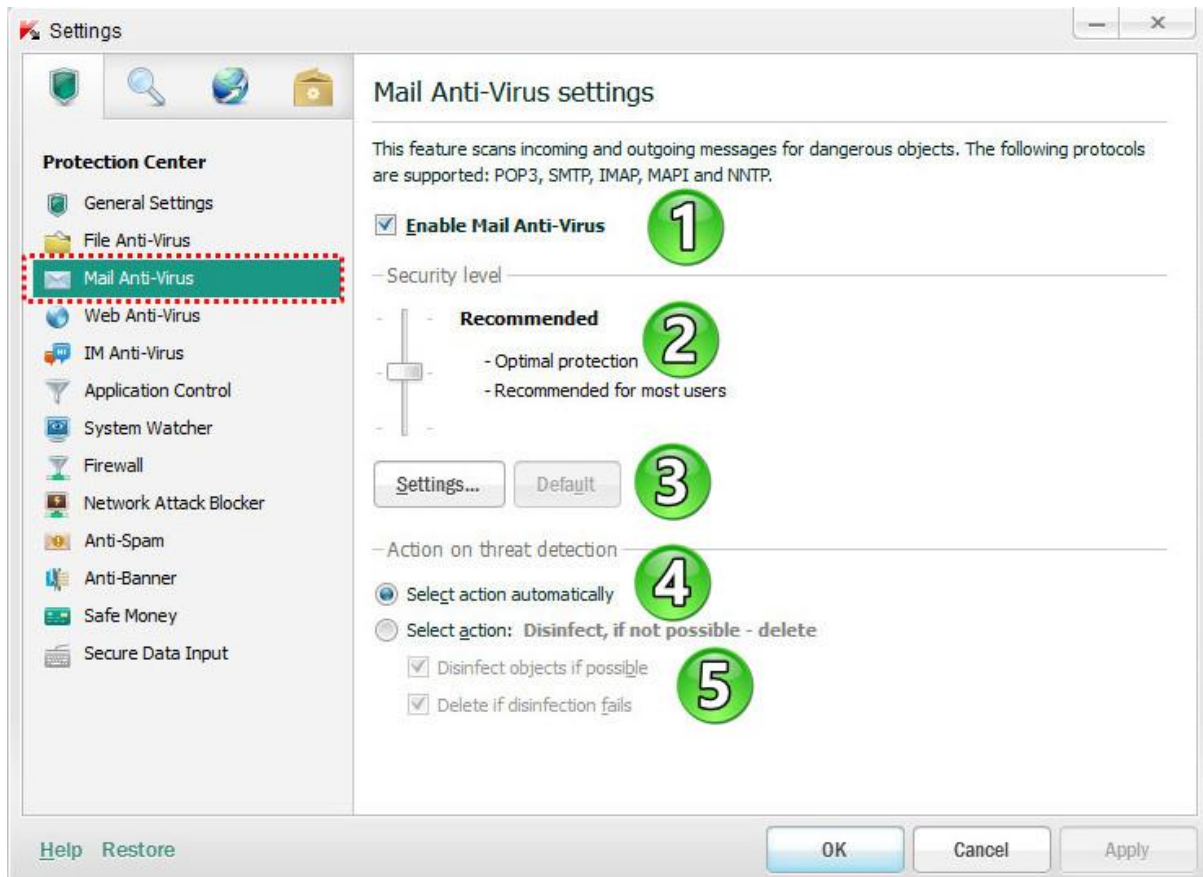
#### **بخش Action on threat detection :**

در این بخش اقداماتی که آنتی ویروس باید بر روی ، **تهدیدات تشخیص داده شده ، موارد آلوده یا احتمالا آلوده** انجام شود را انتخاب میکنیم که شامل دو عملکرد زیر میشود:

**۴- Select action automatically (انتخاب عملکرد اتوماتیک) :** پس از تشخیص موارد خطرناک، آنتی ویروس به طور خودکار اعمال توصیه شده توسط متخصصین آزمایشگاه کسپر斯基 را انجام می دهد. آنتی ویروس موارد مخرب را پاکسازی یا حذف میکند و اگر برای موارد احتمالا آلوده قادر به پاکسازی نباشد ، آنرا نادیده میگیرد. آنتی ویروس قبل از تلاش برای پاکسازی و یا حذف یک مورد آلوده، یک نسخه پشتیبان برای بازسازی پس از پاکسازی تهیه میکند.

#### **۵- Select action (انتخاب عملکرد) :**

**Disinfect objects if possible :** پاکسازی کردن فایل در صورت امکان  
**Delete if disinfection fails :** حذف کامل در صورت عدم امکان پاکسازی



۱- **Enable Mail Anti-Virus (فعال کردن آنتی ویروس ایمیل)**: با فعال بودن این قسمت، آنتی ویروس ایمیل بعد از راه اندازی سیستم عامل در آن اجرا می شود و به طور مداوم، ایمیل‌های با پروتکل POP3, SMTP, IMAP, MAPI و NNTP اسکن می‌کند. همچنین ارتباط امن (SSL) برای POP3، SMTP و IMAP نیز اسکن میشود.

۲- **Security level (سطح امنیتی)**: در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را انتخاب کرد:

**High (زیاد)**:

هنگامی که این سطح امنیتی انتخاب شود دقیقترین کنترل برای پیام های ایمیل اعمال میشود و اسکن پیام های ورودی و خروجی و انجام تجزیه و تحلیل اکتشافی عمیق انجام میشود.

**سطح امنیت بالا در هنگام کار در یک محیط خطرناک استفاده می شود .**

**Recommended (توصیه شده)**:

در این سطح امنیتی، آنتی ویروس ایمیل ، پیام های ورودی و خروجی و تجزیه و تحلیل اکتشافی را با شدت متوسط اسکن میکند.

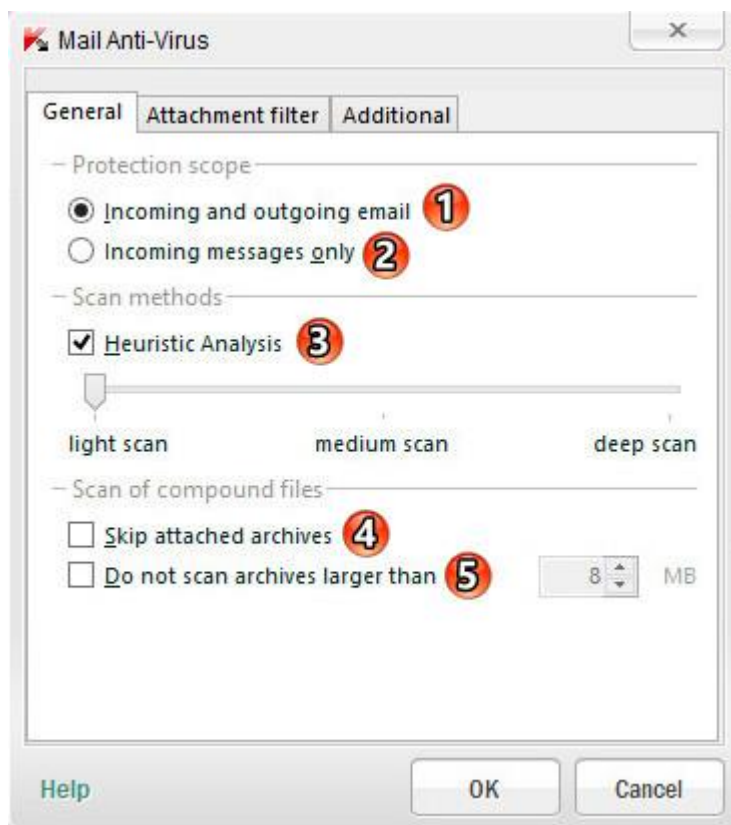
**Low (کم)**:

در این سطح امنیتی ، آنتی ویروس ایمیل ، فقط پیام های دریافتی را اسکن میکند.

**در این حالت فایل های ضمیمه اسکن نمی شود.**

**در این حالت میتوان حداکثر سرعت اسکن را با حداقل استفاده از منابع سیستم داشت.**

۳- **Setting (تنظیمات)**: با کلیک بر روی این دکمه پنجره تنظیمات باز میشود.



**Protection scope:** لیست محدوده حفاظت

۱- **Incoming and outgoing messages:** پیام های ورودی و خروجی

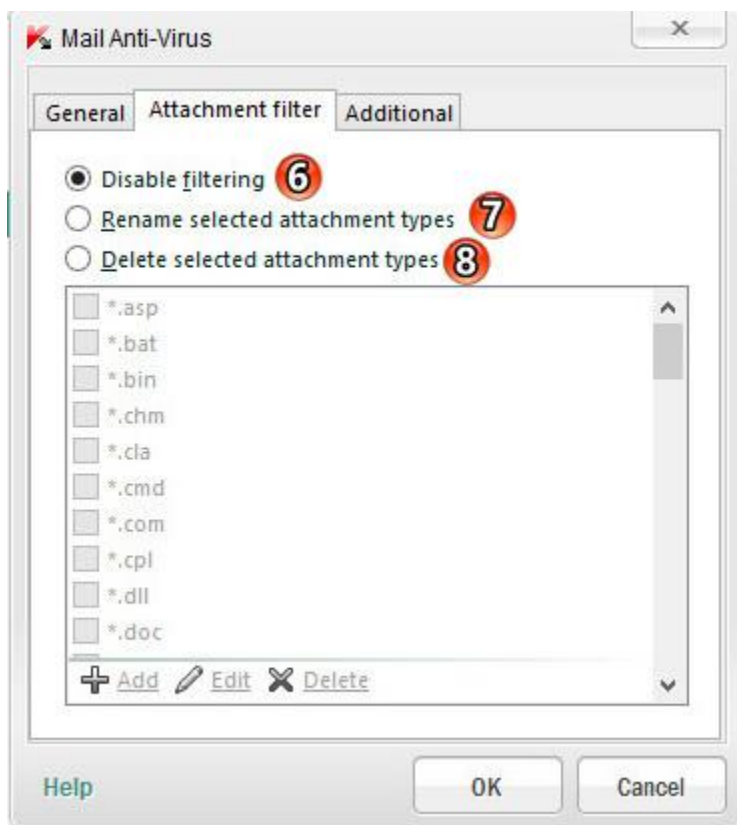
۲- **Incoming messages only:** فقط پیام های دریافتی

**Scan methods:** روشهای اسکن

۳- **heuristic analysis:** در قسمتهای قبلی توضیح داده شده است.

۴- **Skip attached archives:** با تیکدار کردن این قسمت فایل‌های پیوست شده در ایمیل اسکن نمیشود.

۵- **Do not scan archives larger than:** برای ایجاد کردن محدودیت حجم در اسکن

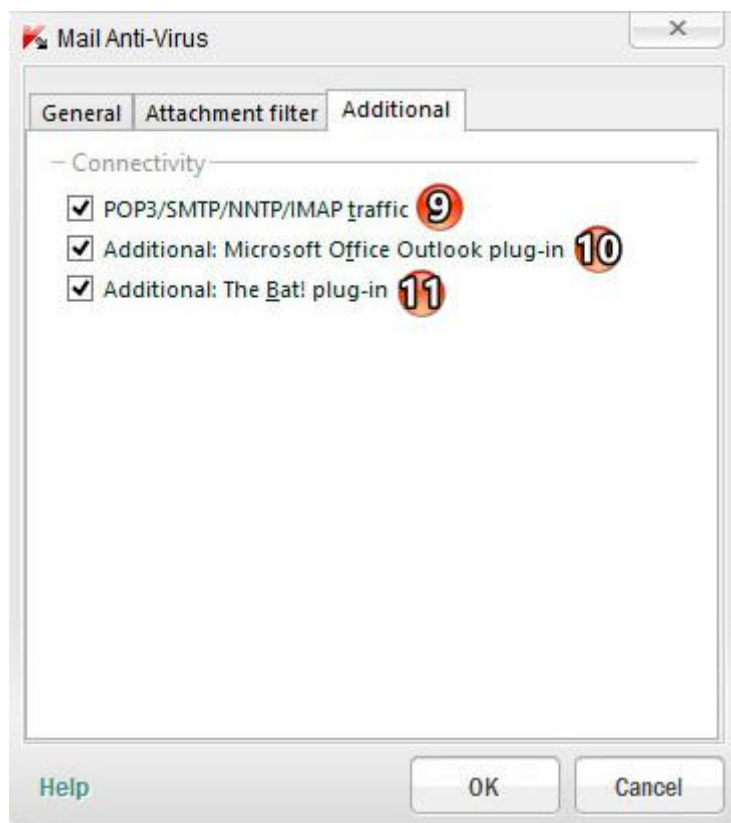


برنامه های مخرب امکان دارد در فایل پیوست در پیام های ایمیل گسترش بیابند . با فعال کردن فیلترینگ فایل پیوست در پیام های ایمیل ، به طور خودکار فایل های پیوست مشخص شده تغییر نام و یا حذف داده میشود.

۶- **Disable filtering** : غیرفعال کردن فیلترینگ

۷- **Rename selected attachment types** : تغییر نام فایل های ضمیمه انتخاب شده

۸- **Delete selected attachment types** : حذف فایل های ضمیمه انتخاب شده



### Connectivity : اتصال

۹- **POP3 / SMTP / NNTP / IMAP traffic** : با تیکدار بودن این قسمت ، ایمیل‌های که دارای پروتکل POP3 SMTP / NNTP / IMAP هستند، قبل از دانلود اسکن میشوند.

۱۰- **Additional: Microsoft Office Outlook plug-in** : این قابلیت می تواند برای دسترسی به تنظیمات ایمیل در داخل Microsoft Office Outlook و پیکربندی اسکن پیامها مورد استفاده قرار گیرد.

۱۱- **Additional: The Bat! plug-in** : تیکدار بودن این قسمت جهت فعال کردن یکپارچه سازی آنتی ویروس ایمیل با پلاگین Bat! است.

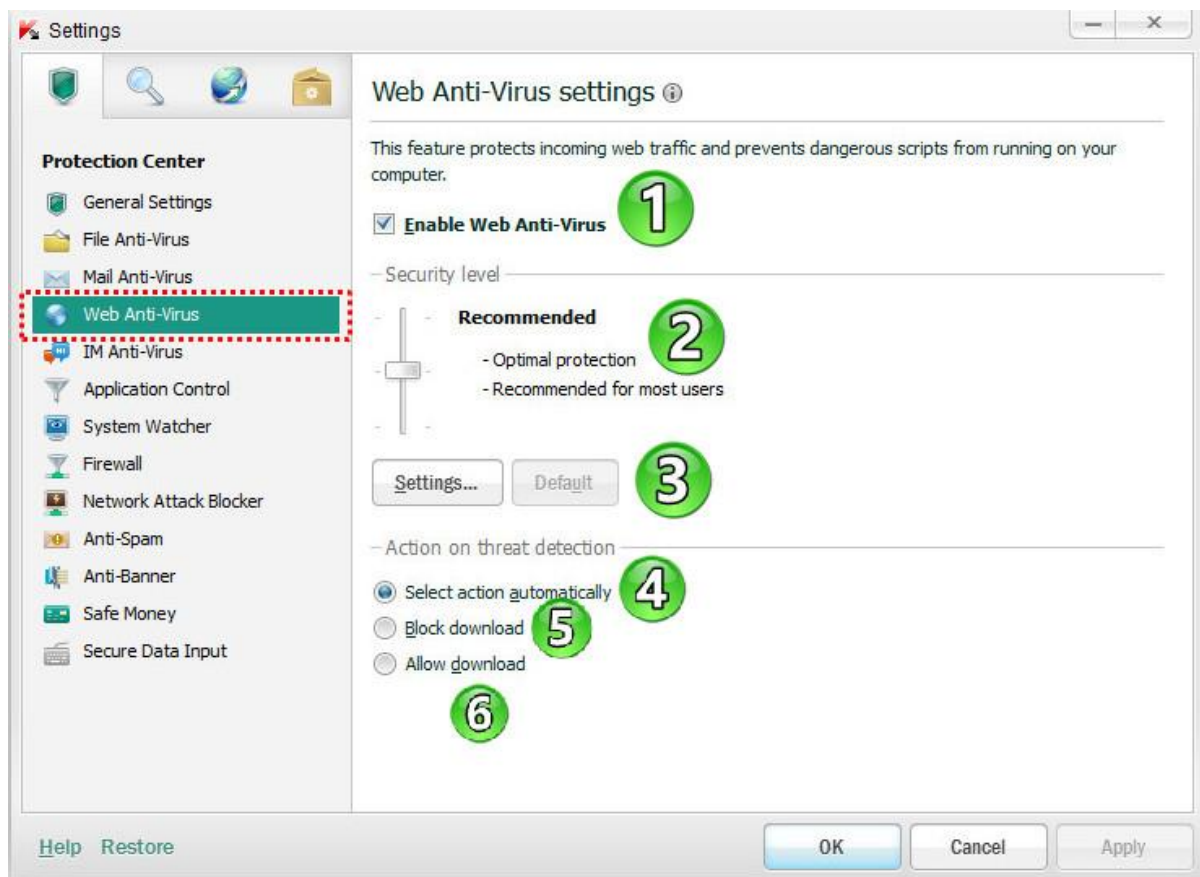
عملکرد آنتی ویروس با توجه به object های ایمیل آلوده در Bat! با استفاده از ابزار های خود نرم افزار تعریف شده است.

### Action on threat detection (اقدامات در تشخیص تهدید) :

۴- **Disinfect objects if possible** : پاکسازی کردن مورد در صورت امکان

۵- **Delete if disinfection fails** : حذف کامل در صورت عدم امکان پاکسازی





۱- **Enable Web Anti-Virus (فعال کردن آنتی ویروس وب):** با فعال شدن این قسمت، آنتی ویروس وب سایت از اطلاعات دریافت شده توسط کامپیوتر شما از طریق پروتکل های HTTP و FTP محافظت میکند. همچنین از اسکریپتهای خطرناک در حال اجرا بر روی کامپیوتر نیز جلوگیری میکند.

۲- **Security level (سطح امنیتی):** در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را انتخاب کرد:

**High (زیاد):**

در این سطح امنیتی ، دقیقترین کنترل بر روی اسکریپت ها و موارد ورودی از طریق HTTP و FTP اعمال میشود .

**در این سطح امنیتی تجزیه و تحلیل اکتشافی در سطح عمیق اسکن میشود.**

**Recommended (توصیه شده):**

در این سطح امنیتی، حفاظت مطلوب و سرعت متوسط در هنگام اسکن ترافیک وب و اسکریپت ها اعمال میشود. اسکن تجزیه و تحلیل اکتشافی در سطح متوسط انجام میشود.

**این سطح امنیتی پیش فرض است.**

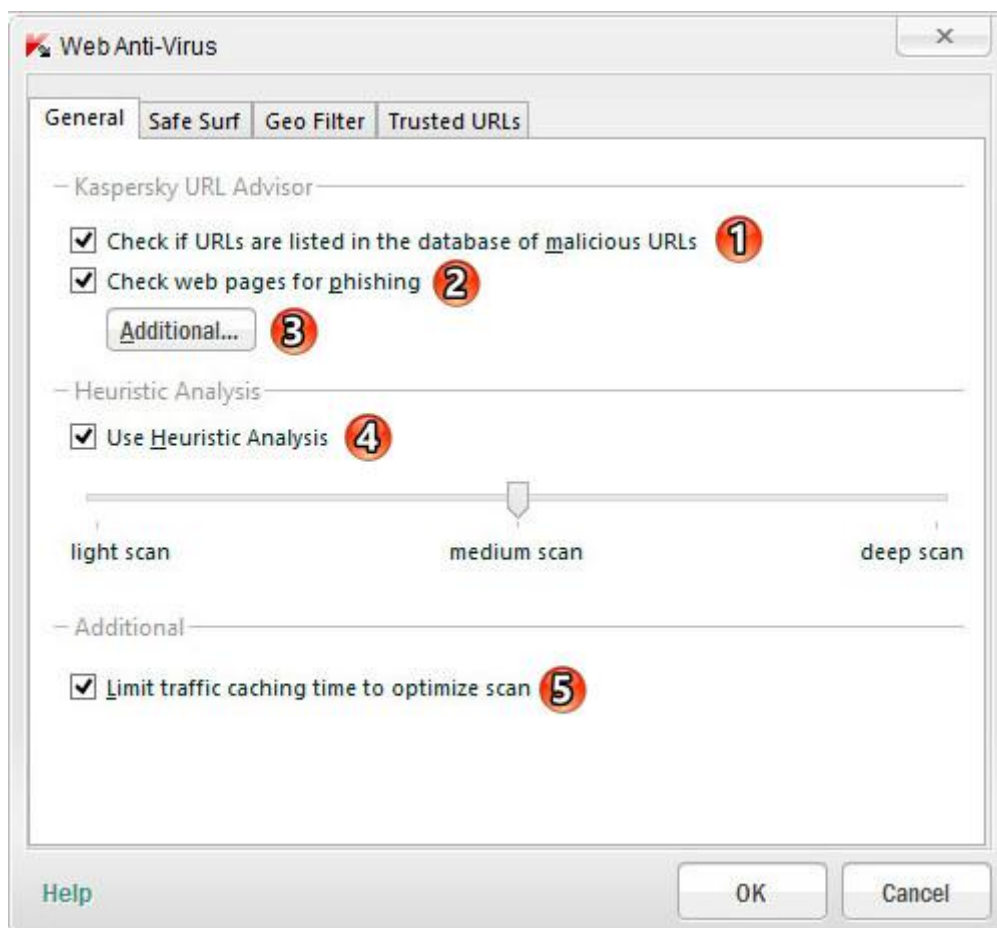
**Low (کم):**

در این سطح امنیتی آرشوها اسکن نمی شود و اسکن تجزیه و تحلیل اکتشافی سطحی است.

**در این حالت فایل های ضمیمه اسکن نمی شود.**

**در این حالت میتوان حداکثر سرعت اسکن را با حداقل استفاده از منابع سیستم داشت.**

۳- **Setting (تنظیمات):** با کلیک بر روی این دکمه پنجره تنظیمات باز میشود.



**Kaspersky URL Advisor** : در این بخش شما می توانید روش اسکن ترافیک وب سایت ها را انتخاب کنید.

۱- **Check if URLs are listed in the database of malicious URLs** : چک کردن URL ها یی که در پایگاه داده ی URL های مخرب ذکر شده است.

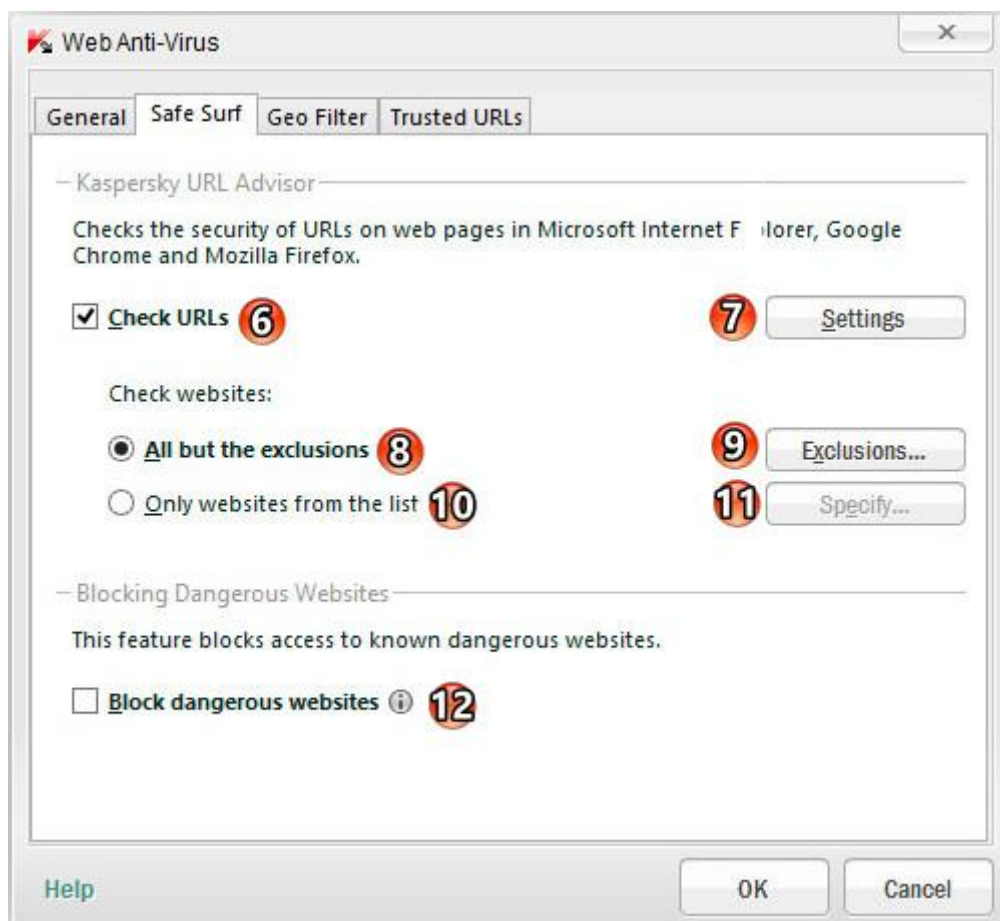
۲- **Check web pages for phishing** : چک کردن صفحات وب برای فیشینگ

۳- **Additional**: با کلیک کردن این دکمه، پنجره تنظیمات ضد فیشینگ باز می شود که در آن می توانید نوع اسکن صفحات وب فیشینگ ، با استفاده از تجزیه و تحلیل اکتشافی را پیکربندی کنید.

۴- **Use Heuristic Analysis** : در قسمتهای قبلی توضیح داده شده است.

۵- **Limit traffic caching time to optimize scan**: محدود کردن زمان ذخیره سازی ترافیک برای بهینه سازی

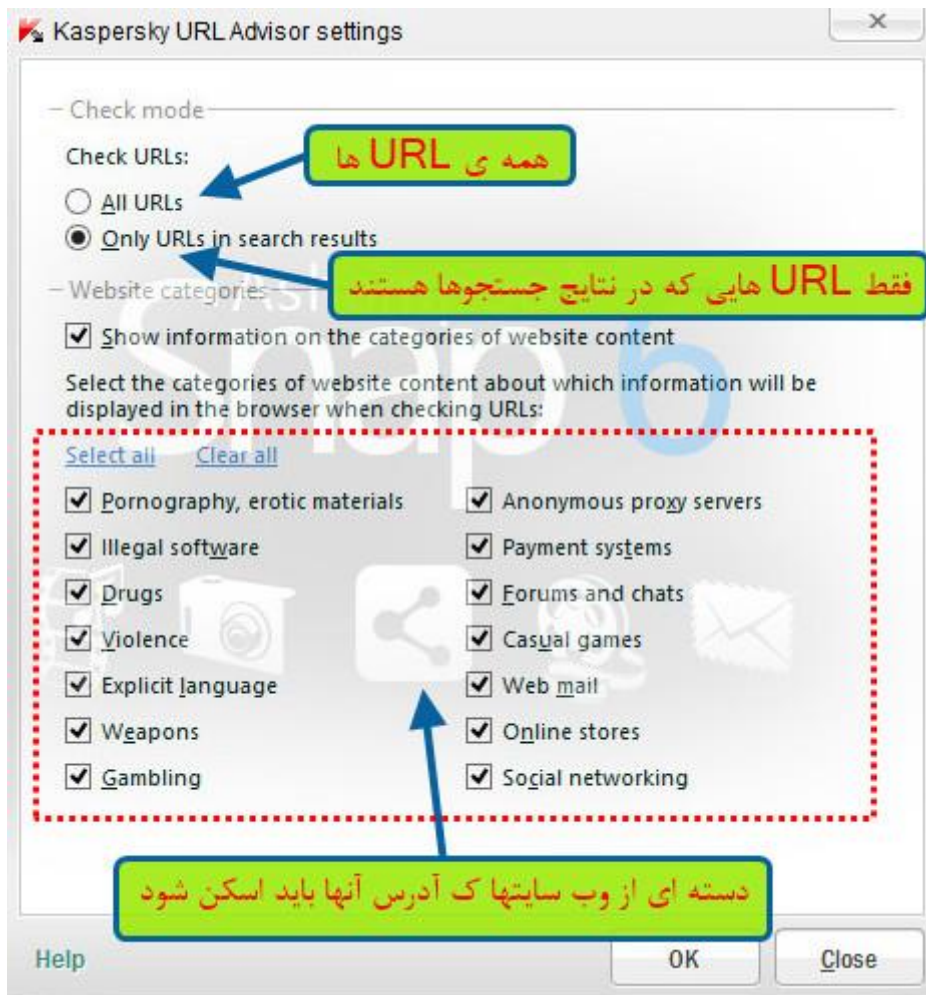
اسکن



۶- **Check URLs** : چک کردن URL های روی صفحات وب برای بررسی آدرس های مخرب یا فیشینگ

۷- **Settings** : ورود به پنجره تنظیمات URL

در این پنجره، می توان یک حالت از چک کردن آدرس وب سایتها و دسته بندی وب سایت ها که باید بررسی شود، را انتخاب کرد.



۸- **All but the exclusions**: در این حالت، تمام آدرس های روی یک صفحه وب و سطح خطر یک منبع وب قبل از تلاش شما برای دسترسی به آن، بررسی میشود.

البته محتوای وب سایت هایی که به لیست آدرس های مورد اعتماد (Exclusions) اضافه شده اند، اسکن نمیشود.

۹- **Exclusions**: با کلیک بر روی این دکمه پنجره استثنائات باز می شود که در آن می توان یک لیست از آدرس وب سایت های مورد اعتماد را اضافه کرد تا برای موارد خطرناک و فیشینگ اسکن نشود.



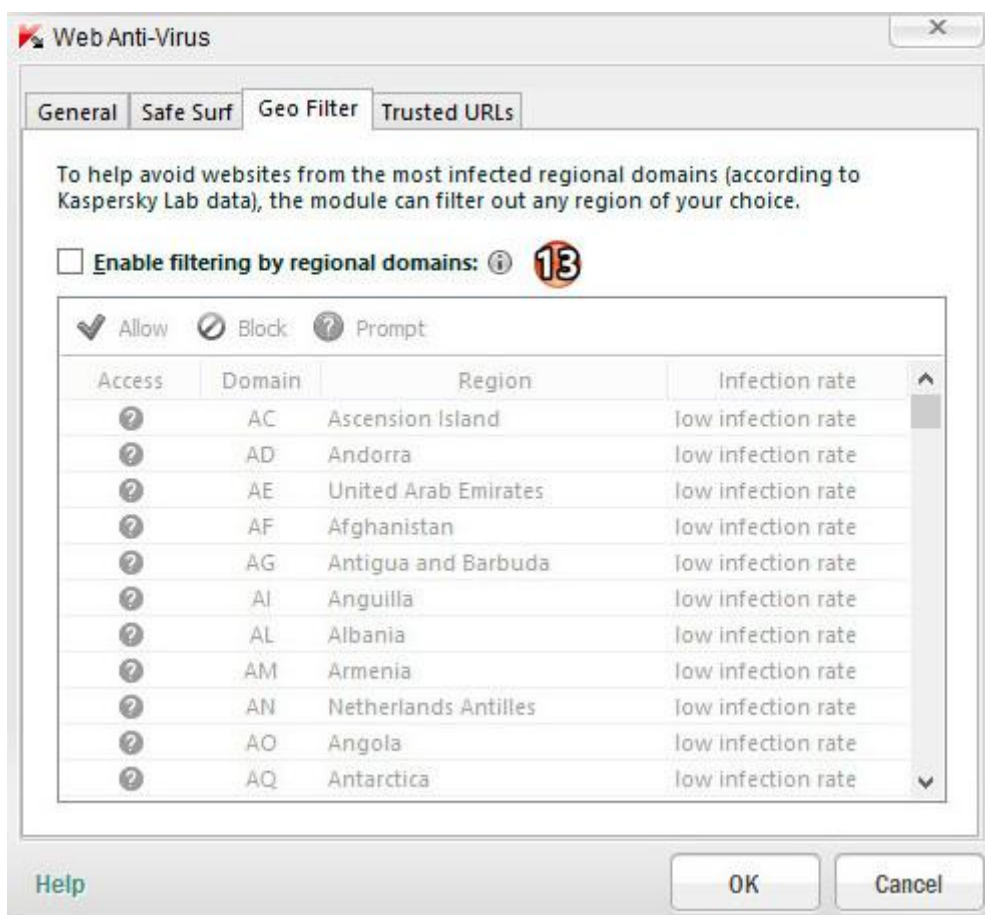
۱۰- **Only websites from the list**: در این حالت فقط، محتوای آدرس وب سایت هایی که در لیست Specify اضافه شده است، اسکن میشود.

۱۱- **Specify**: با کلیک بر روی این دکمه پنجره ای باز می شود که در آن می توان یک لیست از آدرس وب سایتهایی که باید توسط Web Anti-Virus اسکن شود را اضافه کرد.



۱۲- **Block dangerous websites**: مسدود کردن دسترسی به وب سایت های خطرناک

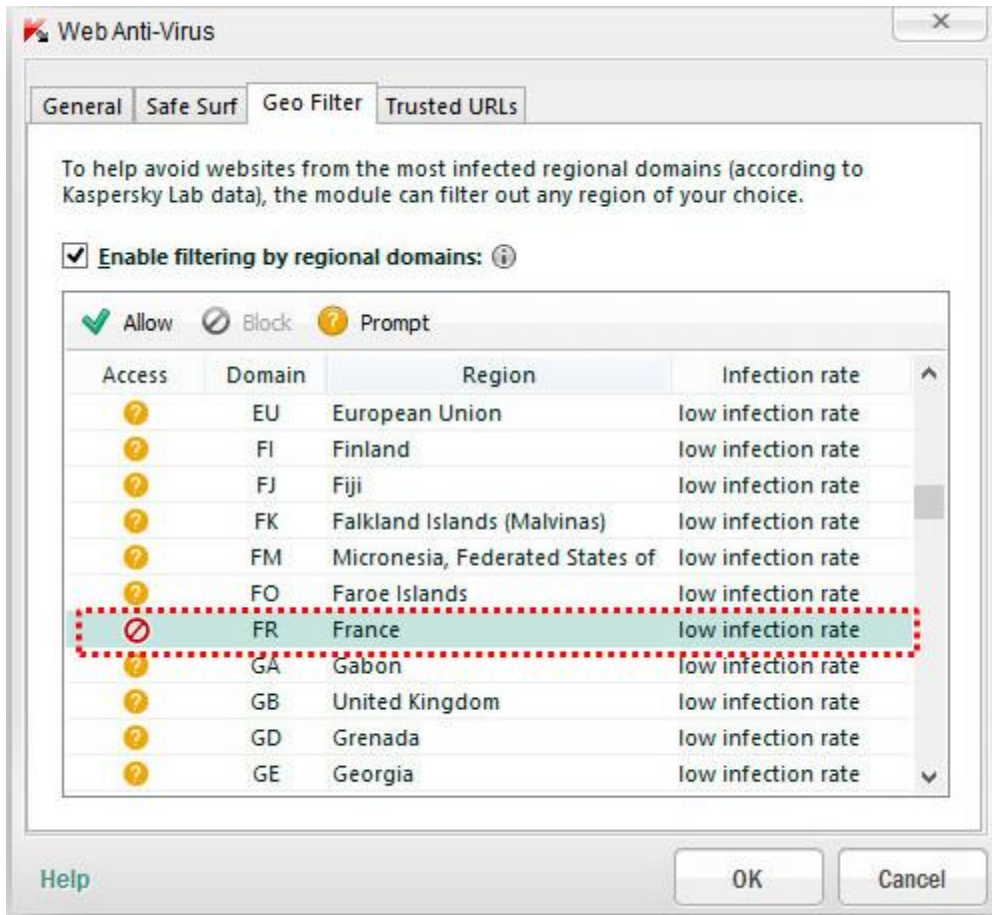
سربرگ **Geo Filter**:



۱۳- **Enable filtering by regional domains**: فعال کردن مدیریت دسترسی به دامنه های منطقه ای در این قسمت میتوان دامنه ی مربوط به یک کشور خاص را بلوکه کرد.(همچنین میتوان اجازه دسترسی داد)

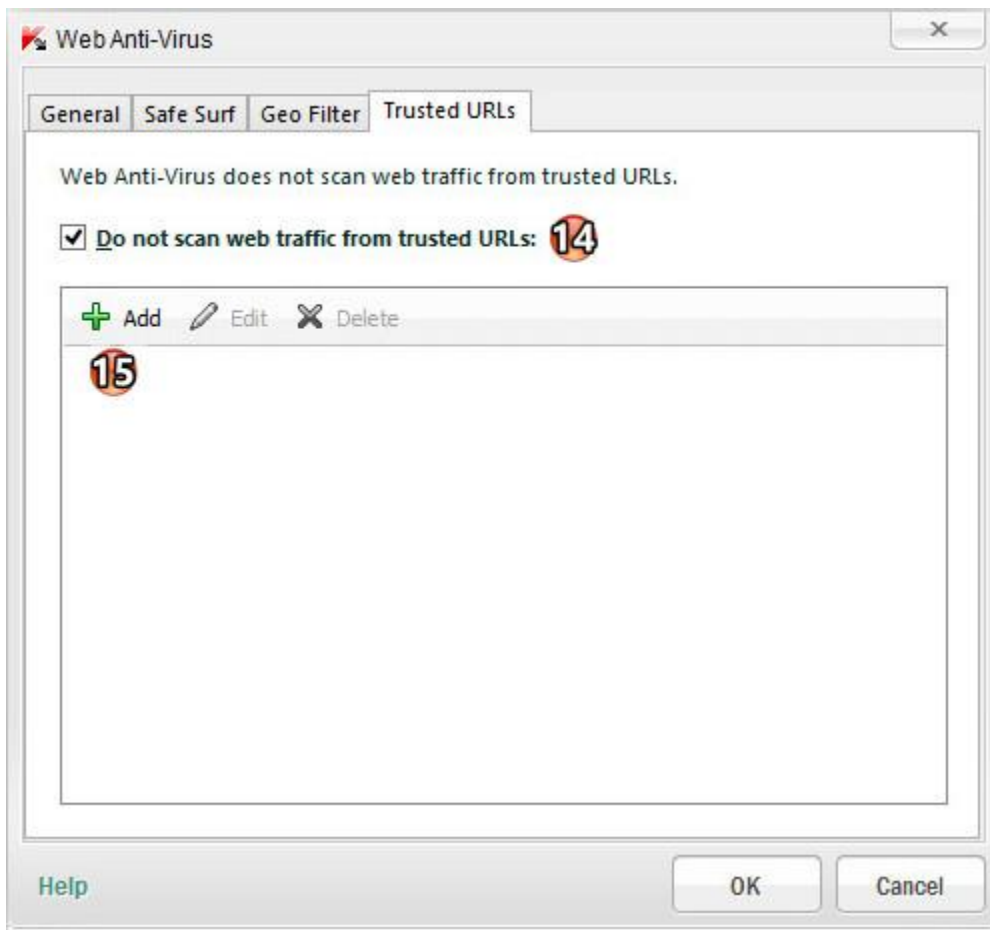
در اسکرین شات زیر من دامنه کشور فرانسه را بلوکه کردم.





پیغامی که بعد از باز کردن یک سایت با دامنه فرانسه میدهد.





**۱۴ - Do not scan web traffic from trusted URLs :** اسکن نکردن URL های (آدرسهای) مورد اعتماد بعضی اوقات خودمون از سالم بودن یک سایت مطمئنیم با این حال کسپرسکی بنا بدلایلی (مثلا : قرار دادن کلید) اقدام به بلوکه کردن سایت میکند. برای خارج کردن سایت از حالت بلوکه باید آدرس سایت را در این لیست وارد کرد. پیغامی که هنگام ورود به سایت مورد نظر داده میشود:



همانطور که در اسکرین شات بالا ملاحظه کردید سایت **iransetup** رو در حالت عادی بلوکه کرده که برای خارج کردن آن از حالت بلوکه باید این سایت را به لیست آدرسهای مورد اعتماد اضافه کرد. برای وارد کردن نام یک سایت باید اول یک ستاره، بعد نقطه، بعد نام سایت و در آخر هم ستاره وارد کرد. مانند: **\*.iransetup.com\***

البته این سایت دارای دامنه های دیگه مثل **ir** و **org**. نیز هست که باید به همین طریق به لیست اضافه کنید.

برای اضافه کردن بعضی از سایتها نباید نقطه ی بعد از ستاره را وارد کرد. مثال: **\*iransetup.com\***

بعد از اضافه کردن به لیست و رفرش مجدد مرورگر سایت از حالت بلوکه خارج میشود.

**۱۵- Add:** برای اضافه کردن سایت به لیست سایتهای مورد اعتماد (**لیست سفید**)



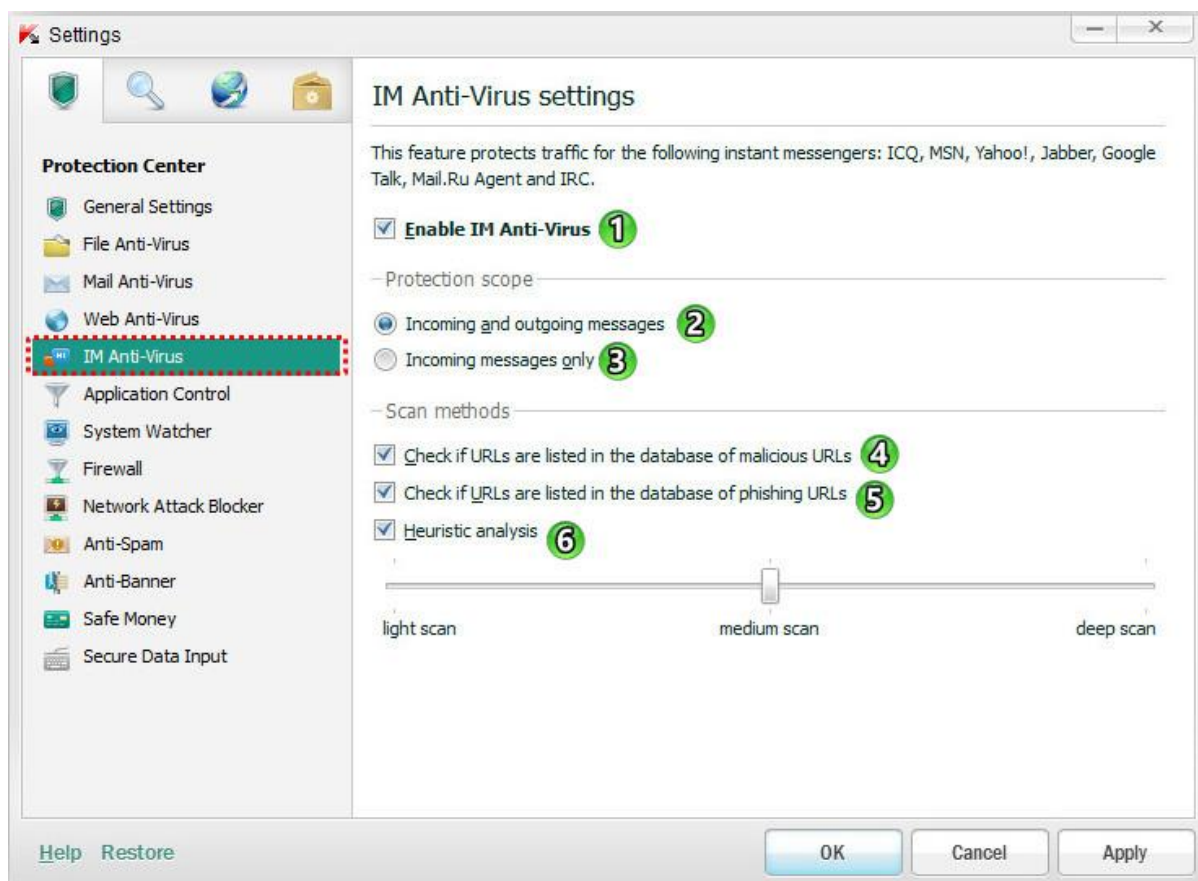
**Action on threat detection:** در این بخش، می توان یک عملکرد برای زمانی که کد مخرب در محتوای ترافیک یک

وب سایت تشخیص داده شد، را انتخاب کرد.

**۴- Select action automatically:** انتخاب عملکرد به صورت خودکار

**۵- Block download:** مسدود کردن دانلود

**۶- Allow download:** اجازه دادن برای دانلود



این ویژگی برای حفاظت از ترافیک مسنجرهای زیر است :

IRC و Mail.ru agent، Google Talk، Jabber، Yahoo، MSN، ICQ

۱- **Enable IM Anti-Virus** : با تیکدار بودن این قسمت، در هنگام راه اندازی سیستم عامل اجرا میشود و تمام پیام های ورودی و خروجی منتقل شده از طریق مسنجرهای ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent, or IRC اسکن میشود.

۲- **Incoming and outgoing messages** : پیام های ورودی و خروجی

۳- **Incoming messages only**: فقط پیامهای ورودی

۴- **Check if URLs are listed in the database of malicious URLs** : چک کردن URL های موجود در

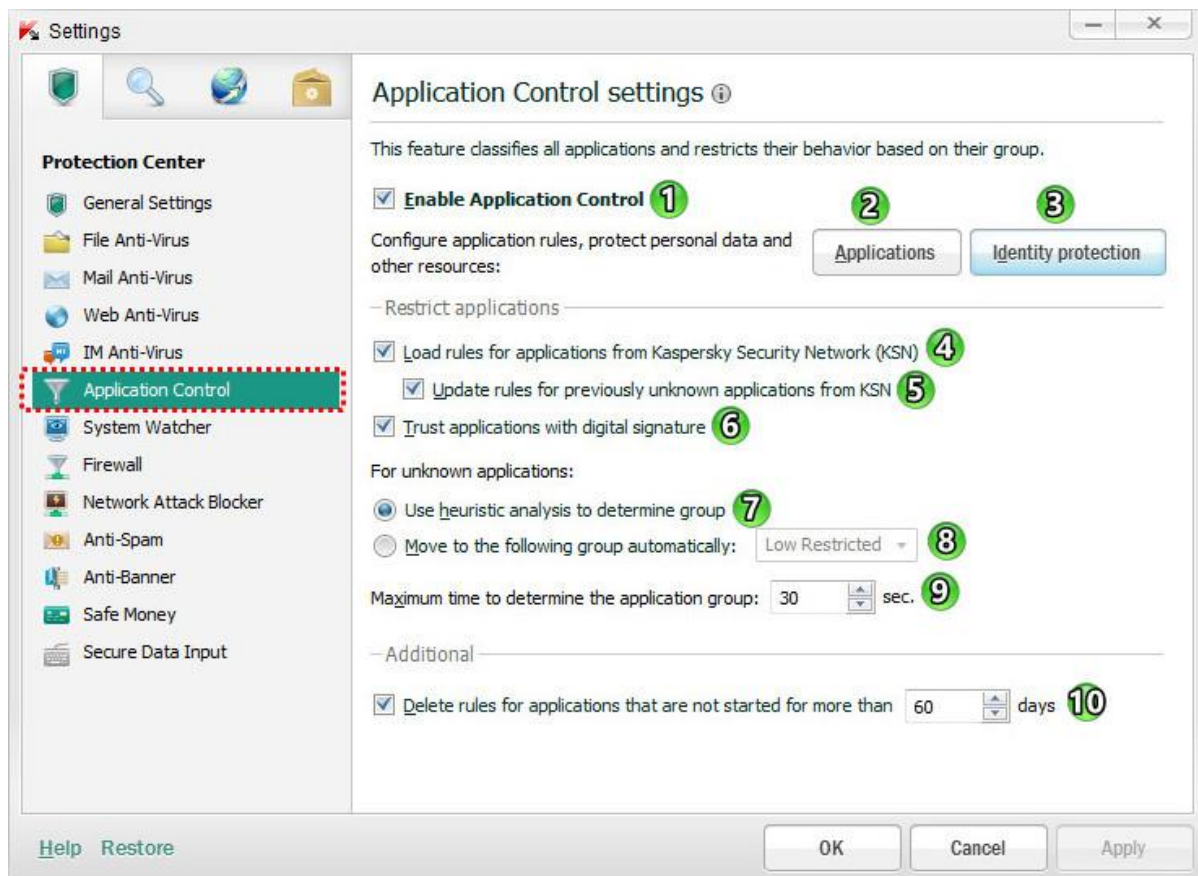
پیامها، از جهت وجود یا عدم وجود در دیتابیس URL های مخرب

۵- **Check if URLs are listed in the database of phishing URLs**: چک کردن URL های موجود در

پیامها، از جهت وجود یا عدم وجود در دیتابیس URL های فیشینگ

۶- **Heuristic Analysis** : این قسمت قبلا توضیح داده شده است.

## ۶- تنظیمات کنترل برنامه (Application Control Setting)

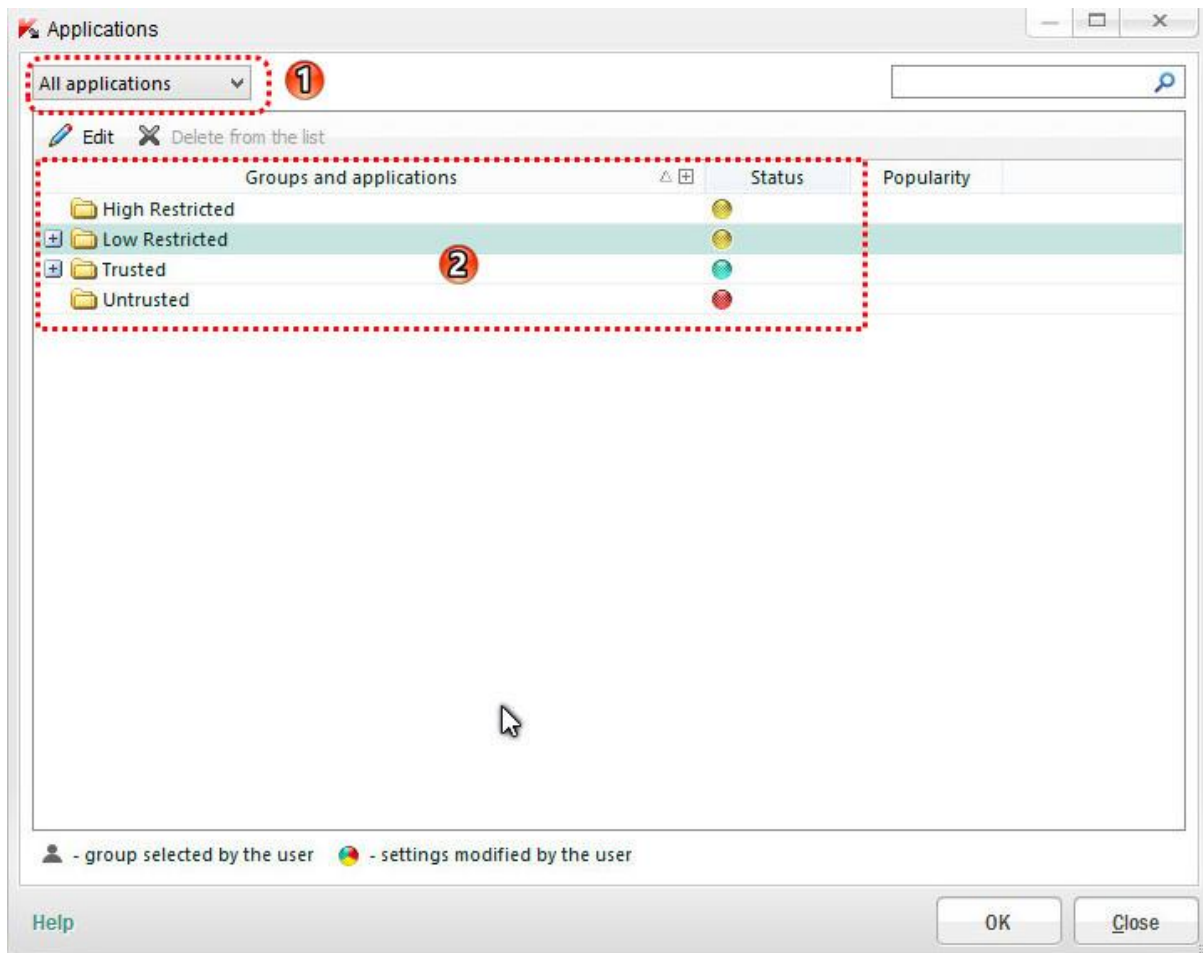


۱- **Enable Application Control** : فعال کردن کنترل برنامه

۲- **Applications** : برنامه های کاربردی

با کلیک بر روی این دکمه پنجره نرم افزارهای کاربردی باز می شود که در آن میتوان قوانین را برای برنامه ها ویرایش کنید.





۱- لیست کشویی جهت اعمال فیلتر نمایش برنامه ها : شامل دو فیلتر زیر میشود:

**All applications** (همه برنامه های کاربردی)

**Running on start-up** (در حال اجرا در راه اندازی)

۲- **Groups and applications** : در اینجا نام گروه و برنامه های کاربردی در آنها نمایش داده میشود. این قسمت

دارای چهار گروه زیر می باشد.

**High Restricted** : با محدودیت بالا

**Low Restricted** : با محدودیت پایین

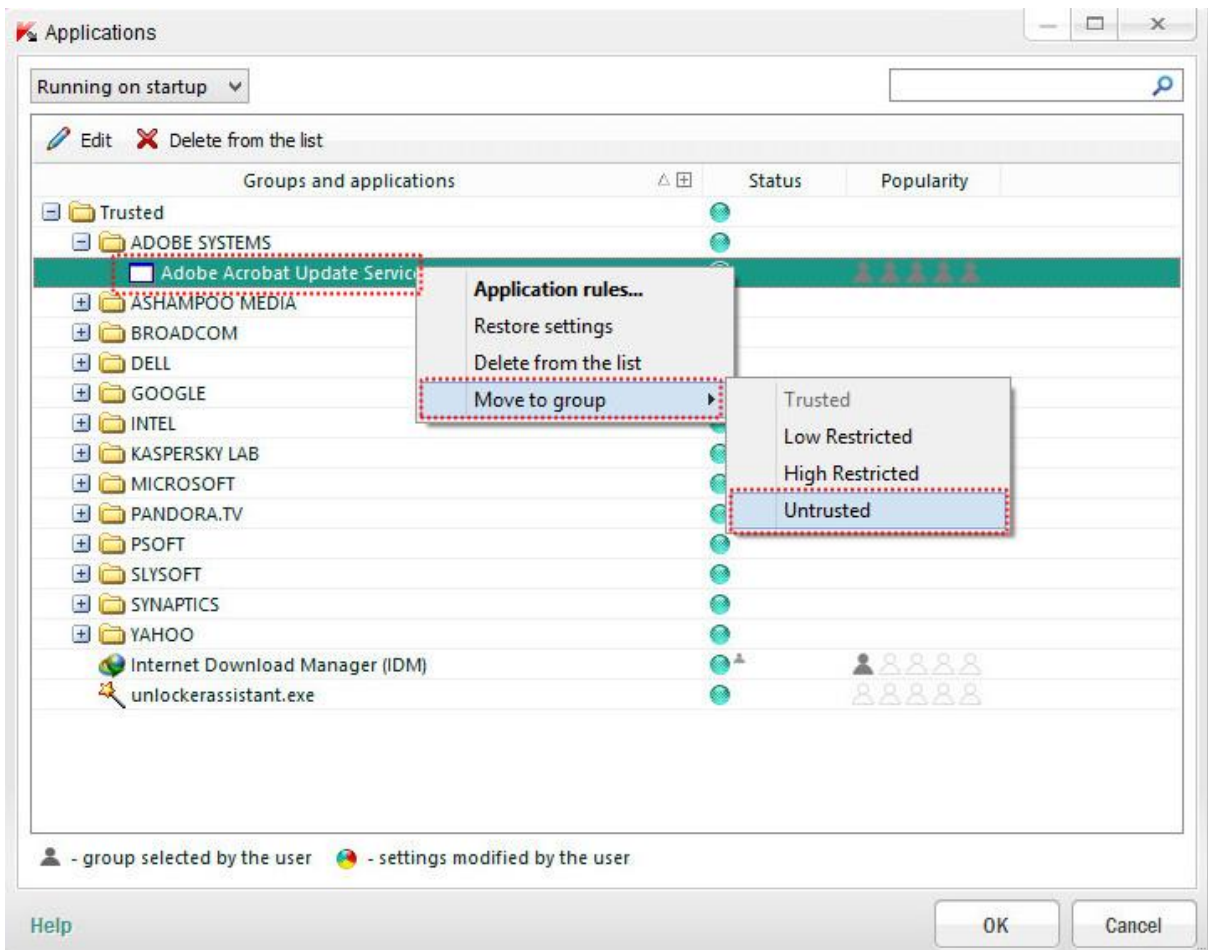
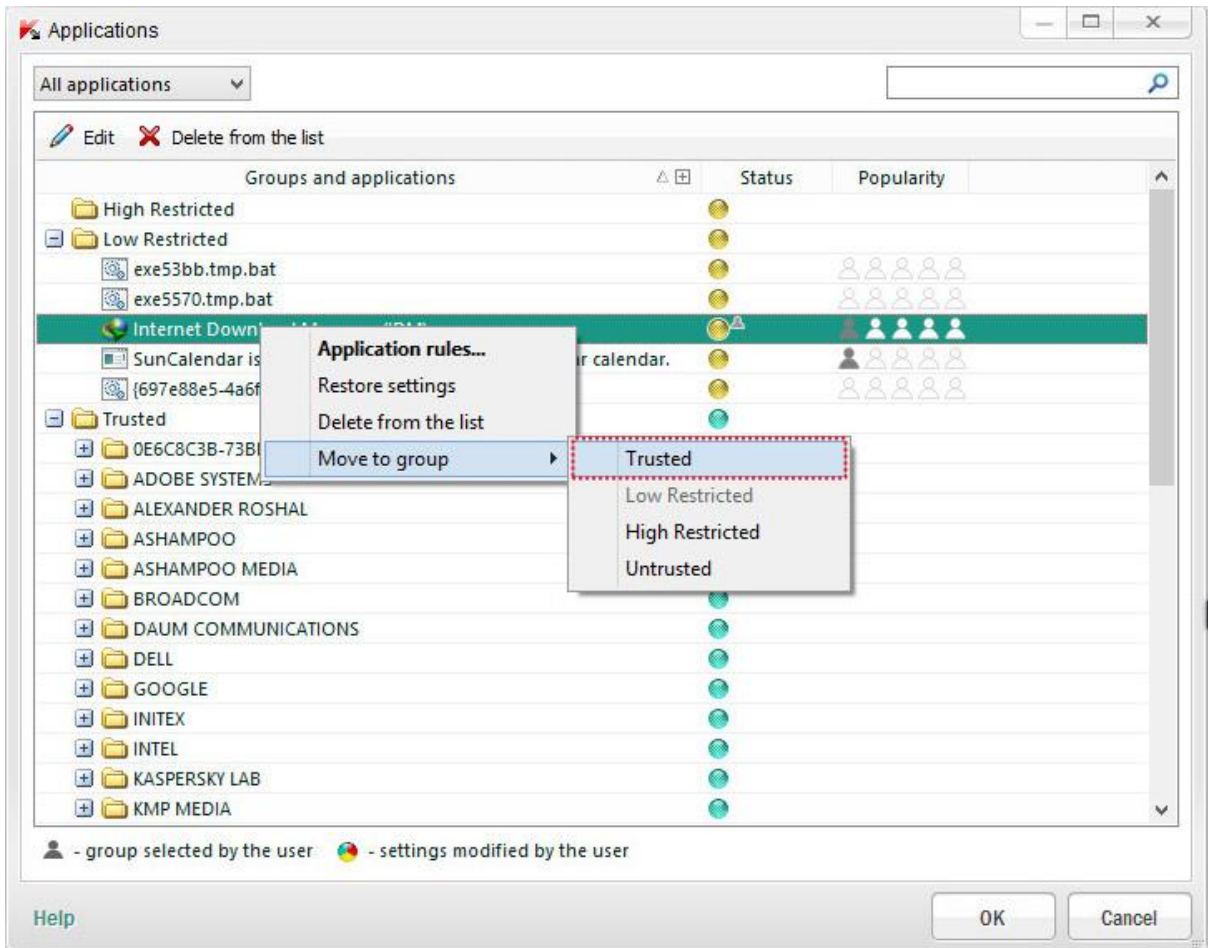
**Trusted** : مورد اطمینان

**Untrusted** : غیرقابل اطمینان

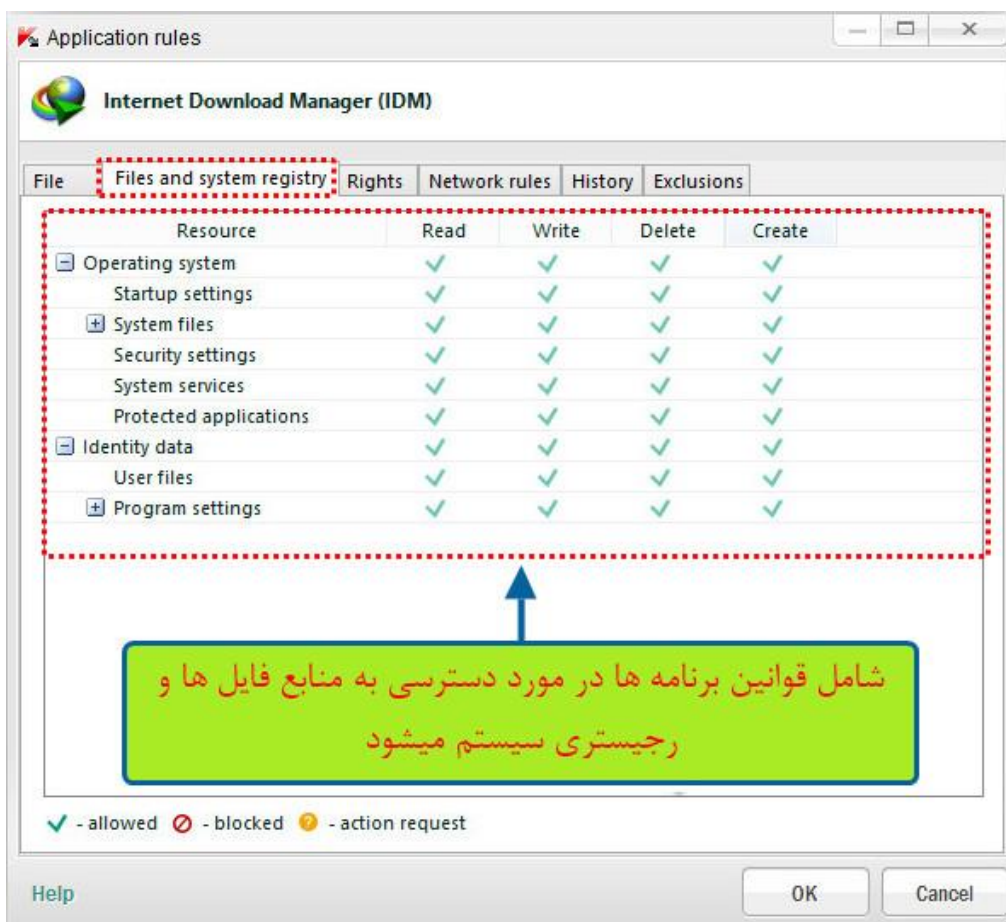
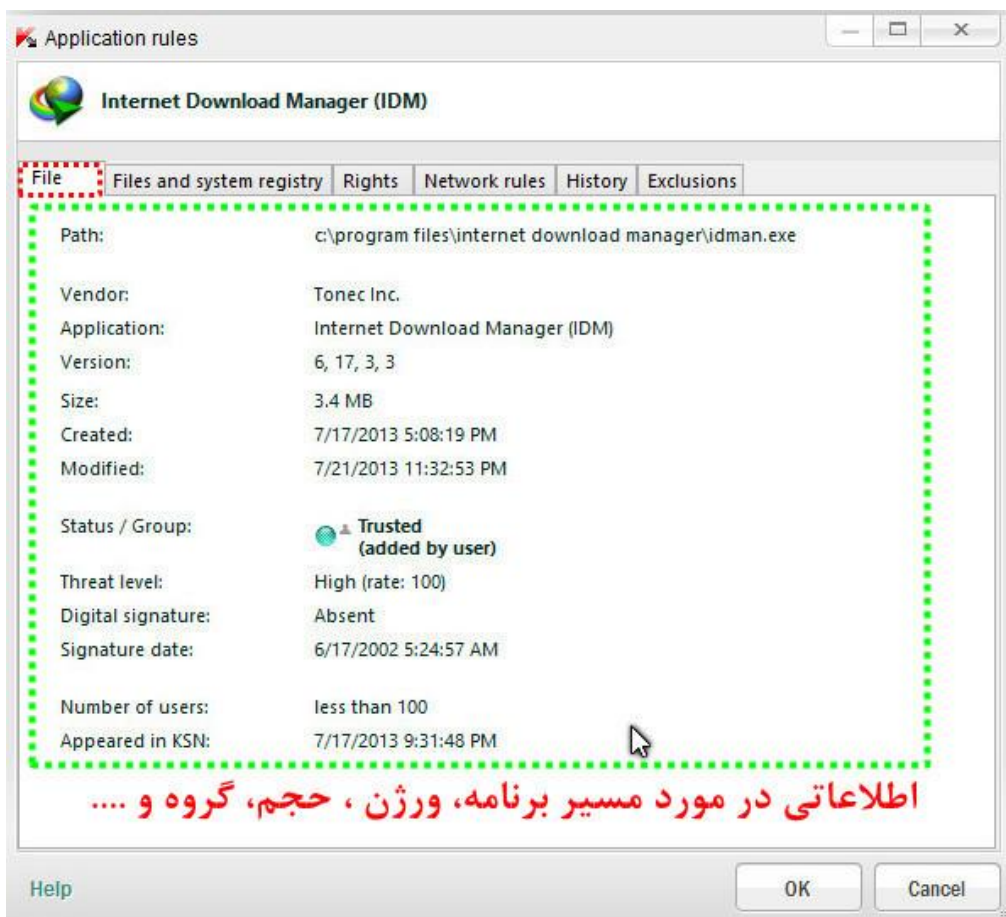
در هر گروه میتوان برنامه های قرار داد تا محدودیت های گروه به آن اعمال شود. در صورتی که یک برنامه را بخواهیم به گروهی دیگر منتقل کنیم به روش زیر عمل میکنیم.

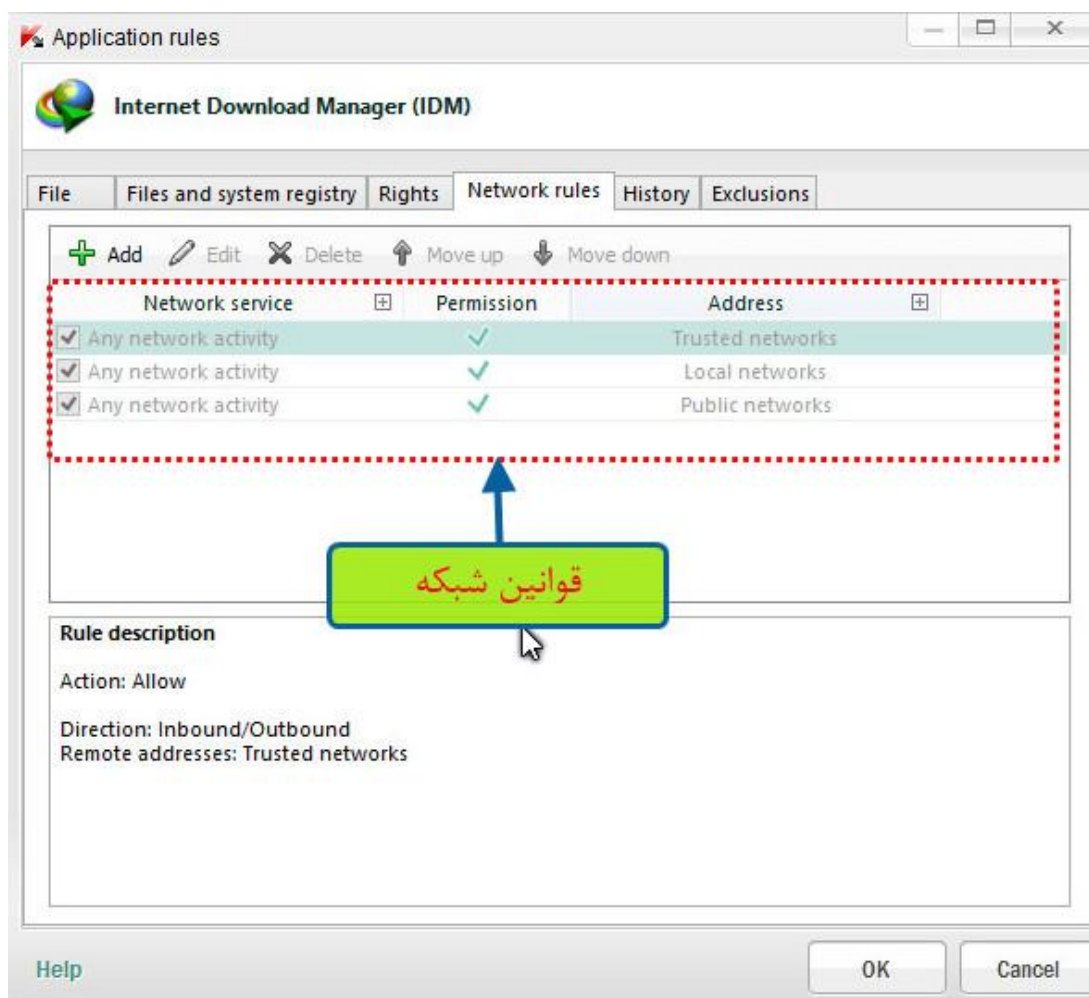
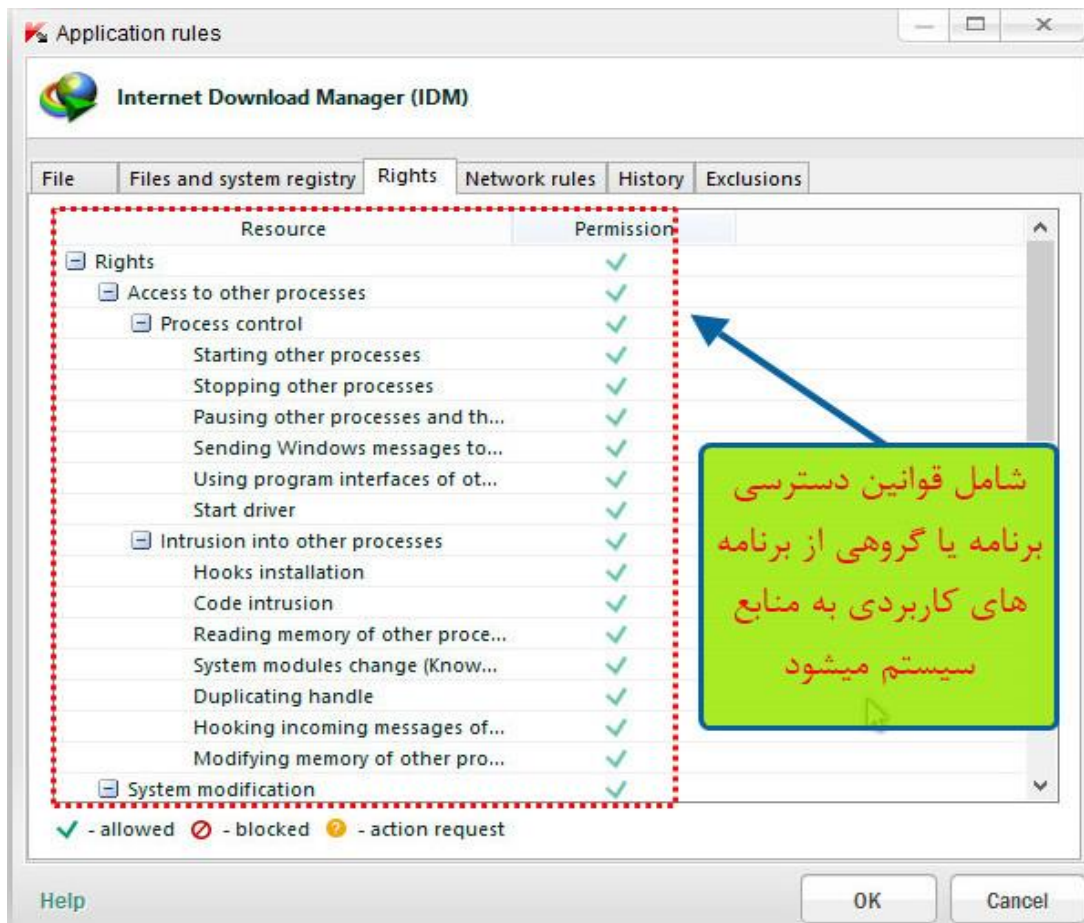
در اسکرین شات اول برای مثال برنامه IDM را که بطور پیش فرض در گروه Low Restricted قرار میگیرد به گروه Trusted انتقال میدهم.

در اسکرین شات دوم یک برنامه را که قصد جلوگیری از اجرای آن را دارم در گروه Untrusted قرار میدهم.



با راست کلیک بر روی هر کدام از برنامه ها و انتخاب گزینه **Application rules...** میتوان قوانینی برای آن برنامه اعمال کرد. ( در اینجا من IDM را انتخاب کردم).





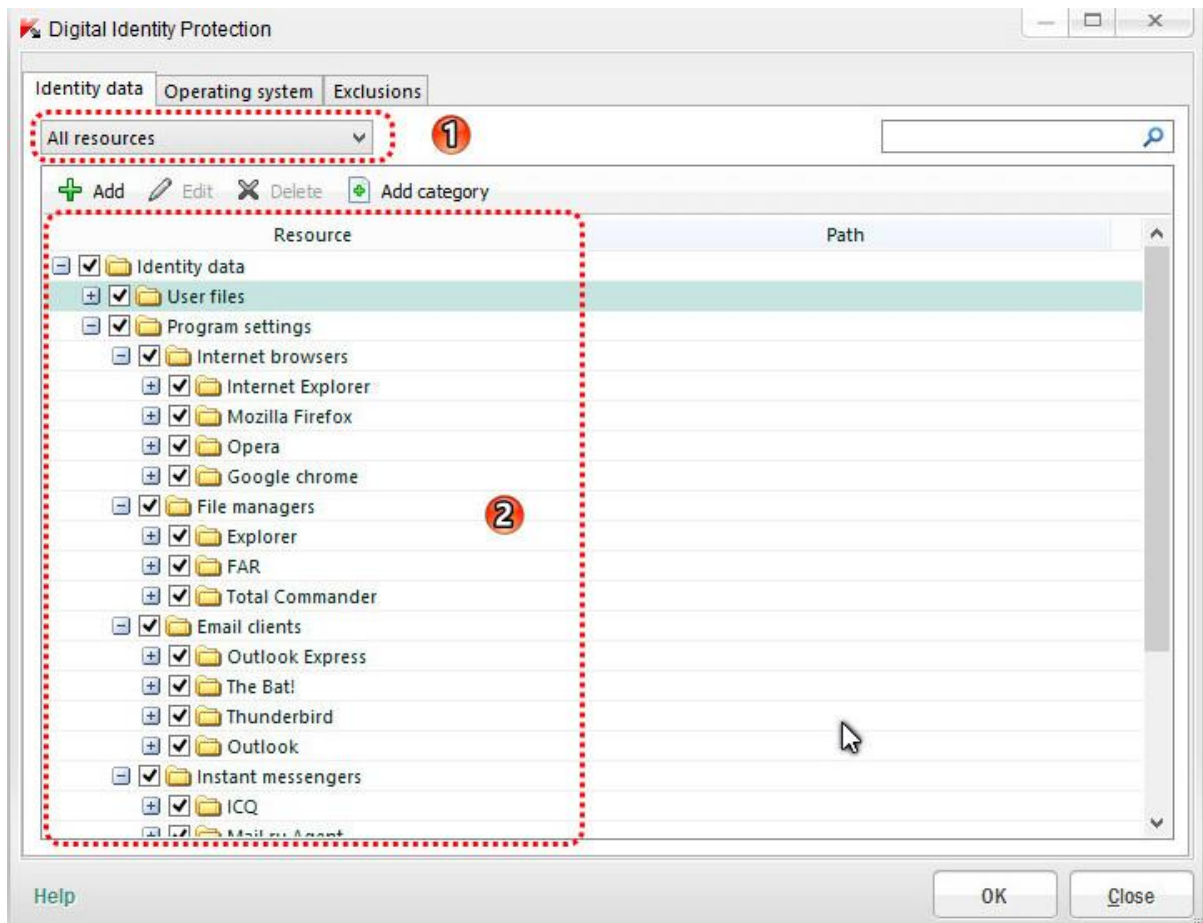






### ۳- Identity protection: حفاظت از هویت

با کلیک بر روی این دکمه پنجره حفاظت از هویت دیجیتال باز می شود که در آن میتوان یک لیست ایجاد کرد که در آن دسترسی به اطلاعات شخصی، تنظیمات سیستم عامل و منابع، توسط کنترل برنامه نظارت بشود.



۱- لیست کشویی جهت اعمال فیلتر نمایش: شامل هفت فیلتر زیر میشود:

**User files**: فایل‌های کاربر (پوشه My Documents، فایل‌های کوکی، اطلاعاتی در مورد فعالیت‌های کاربر)

**Internet browsers**: مرورگر اینترنت (مانند Explorer, Internet, Chrome, Opera, Firefox)

**File managers**: مدیریت فایل (مانند Explorer)

**Email clients**: برنامه‌های مدیریت ایمیل (مانند Outlook)

**Instant messengers**: پیام‌رسانها (مسنجرها مانند Skype)

**Electronic purses**: کیف پول الکترونیکی

**Antiviruses**: آنتی ویروس‌ها

**All resources**: همه منابع

۲- **Resource**: نمایش نام طبقه بندی و برنامه‌های موجود در آن

#### ۴- **Load rules for applications from Kaspersky Security Network (KSN)** : بارگذاری قوانین

برنامه های کاربردی از شبکه امنیت کسپرسکی (KSN) با تیکدار بودن این قسمت ، کنترل برنامه ها (Application Control) یک درخواست به پایگاه داده های (KSN) به منظور تعریف گروه نرم افزار می فرستد.

#### ۵- **Update rules for previously unknown applications from KSN** : بروزرسانی قوانین برای برنامه های

کاربردی ناشناخته از KSN

#### ۶- **Trust applications with digital signature** : برنامه های کاربردی مورد اعتماد با امضای دیجیتال

با تیکدار بودن این قسمت، کنترل برنامه (Application Control) ، برنامه های کاربردی با امضای دیجیتالی را قابل اعتماد (trusted) در نظر می گیرد [کنترل برنامه (Application Control) ، این برنامه را به گروه قابل اعتماد منتقل میکند].

#### ۷- **Use heuristic analysis to determine group** : تعیین گروه با استفاده از تجزیه و تحلیل اکتشافی ( heuristic analysis)

(analysis) برنامه های ناشناخته

#### ۸- **Move to the following group automatically** : انتقال برنامه های ناشناخته به صورت خودکار به گروه های

زیر :

۱- Low Restricted ۲- High Restricted ۳- Untrusted

#### ۹- **Maximum time to define the application group** : حداکثر زمان برای تعریف گروه نرم افزار

مدت زمانی که کنترل برنامه (Application Control) برنامه های کاربردی در حال اجرا را با استفاده از تجزیه و تحلیل اکتشافی اسکن میکند.

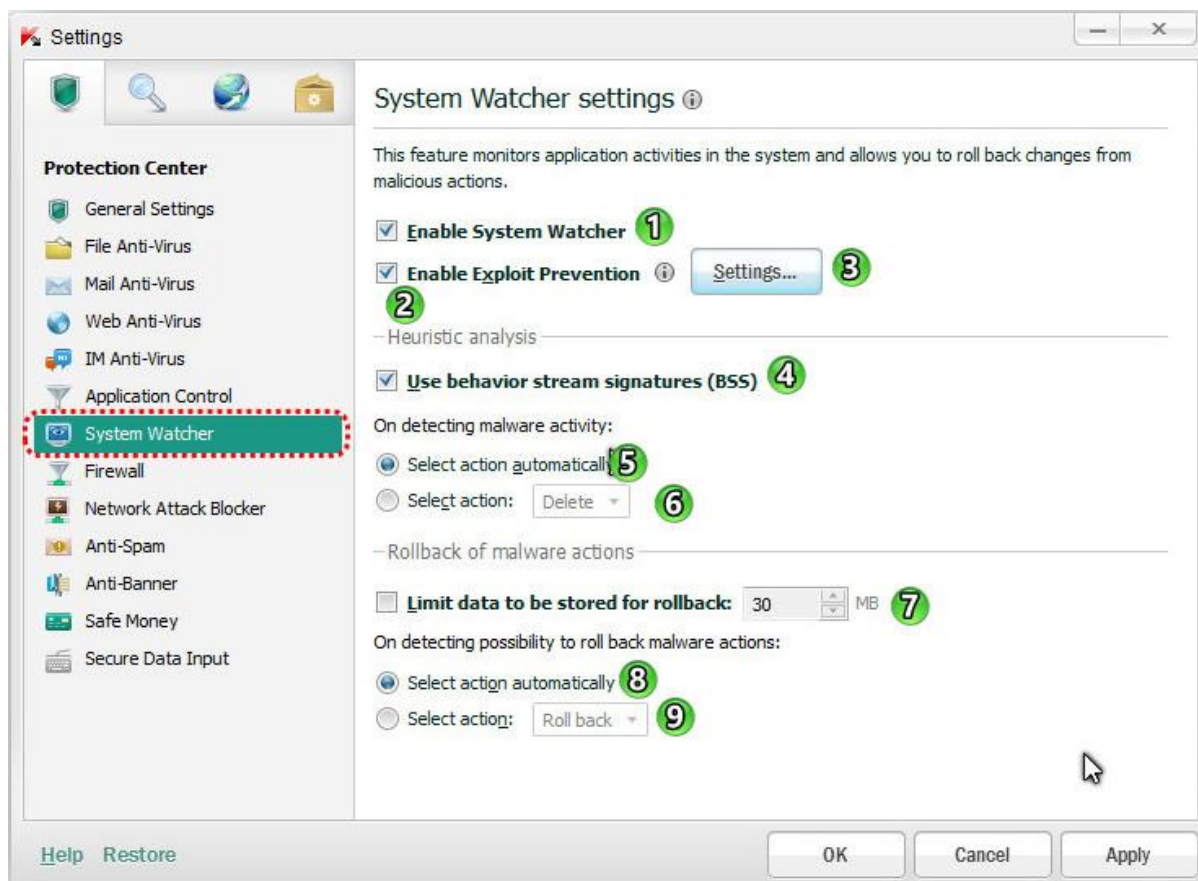
به طور پیش فرض، تجزیه و تحلیل یک برنامه به مدت ۳۰ ثانیه است. اگر این مدت زمان تمام شود، کنترل برنامه (Application Control) به وضوح نمی تواند سطح تهدید برنامه را تعیین کند در نتیجه آن را به گروه **Low Restricted** منتقل می کند. کنترل برنامه (Application Control) اسکن برنامه را پس از قرار گیری در گروه مورد اعتماد (Trusted) در حالت پس زمینه ادامه میدهد .

#### ۱۰- **Delete rules for applications that are not started for more than** : حذف اتوماتیک قوانین برنامه

های کاربردی که در یک دوره زمانی مشخص اجرا نمیشود. مدت زمان در روز مشخص شده است.

## ۷- نگهدارنده (مراقب ، نظاره گر) سیستم (System Watcher)

این ویژگی بر فعالیت برنامه ها در سیستم نظارت دارد و به شما اجازه برگرداندن به حالت قبل از تغییرات ایجاد شده توسط عوامل مخرب را میدهد. ( تنظیمات مربوط به Malware )

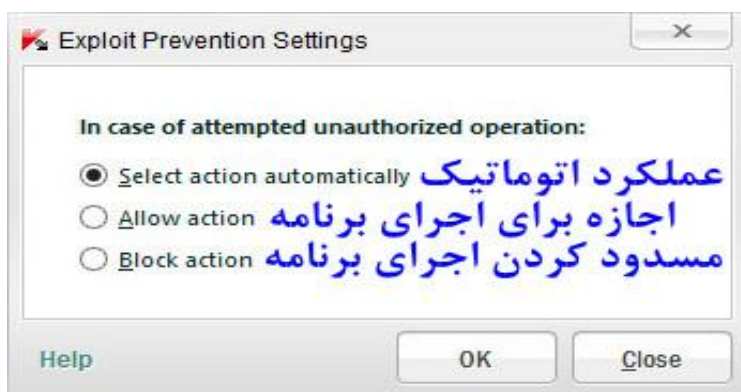


۱- **Enable System Watcher** : با تیکدار بودن این قسمت ، تمام اتفاقاتی که در اطلاعات سیستم رخ میدهد (مانند تغییر فایلها ، تغییر کلید های رجیستری، شروع درایورها ، تلاش برای خاموش کردن کامپیوتر) جمع آوری و ذخیره سازی میشود. این داده ها برای پیگیری فعالیت های مخرب برنامه های کاربردی و بازگرداندن شرایط سیستم به قبل از ظاهر شدن برنامه مخرب ، مورد استفاده قرار میگیرد.

۲- **Enable Exploit Prevention** : فعال کردن قسمت پیشگیری

با تیکدار بودن این قسمت ، **فایل های اجرایی**، اجرا شده توسط برنامه های آسیب پذیر، پیگیری میشود. اگر KIS تلاش برای اجرای **فایل های اجرایی** ، یک برنامه آسیب پذیر که توسط کاربر آغاز نشده است را تشخیص دهد ، درخواستهای اجرای فایل را **مسدود** میکند.

۳- **Settings** : تنظیمات



۴- **Use behavior stream signatures (BSS)** : استفاده از الگوهای قابل آپدیتِ فعالیت های خطرناک بر اساس رفتار (BSS)

با تیکدار بودن این قسمت ، فعالیت های نرم افزارها را بر اساس اطلاعات جمع آوری شده و BSS تجزیه و تحلیل میشود. همچنین فعالیتهای برنامه های مشابه برنامه های مخرب، نیز بررسی میشود.

**On detecting malware activity** : برای تشخیص فعالیت **Malware**

۵- **Select action automatically** : انتخاب عملکرد بصورت اتوماتیک

۶- **Select action** : انتخاب عملکرد دستیکه شامل :

۱- **Delete** (حذف) ۲- **Terminate the malicious application** (خاتمه دادن به برنامه های مخرب) ۳- **Ignore** (نادیده گرفتن)

۷- **Limit data to be stored for rollback** : محدود کردن اطلاعات ذخیره شده برای بازگردانی (بر حسب مگابایت)

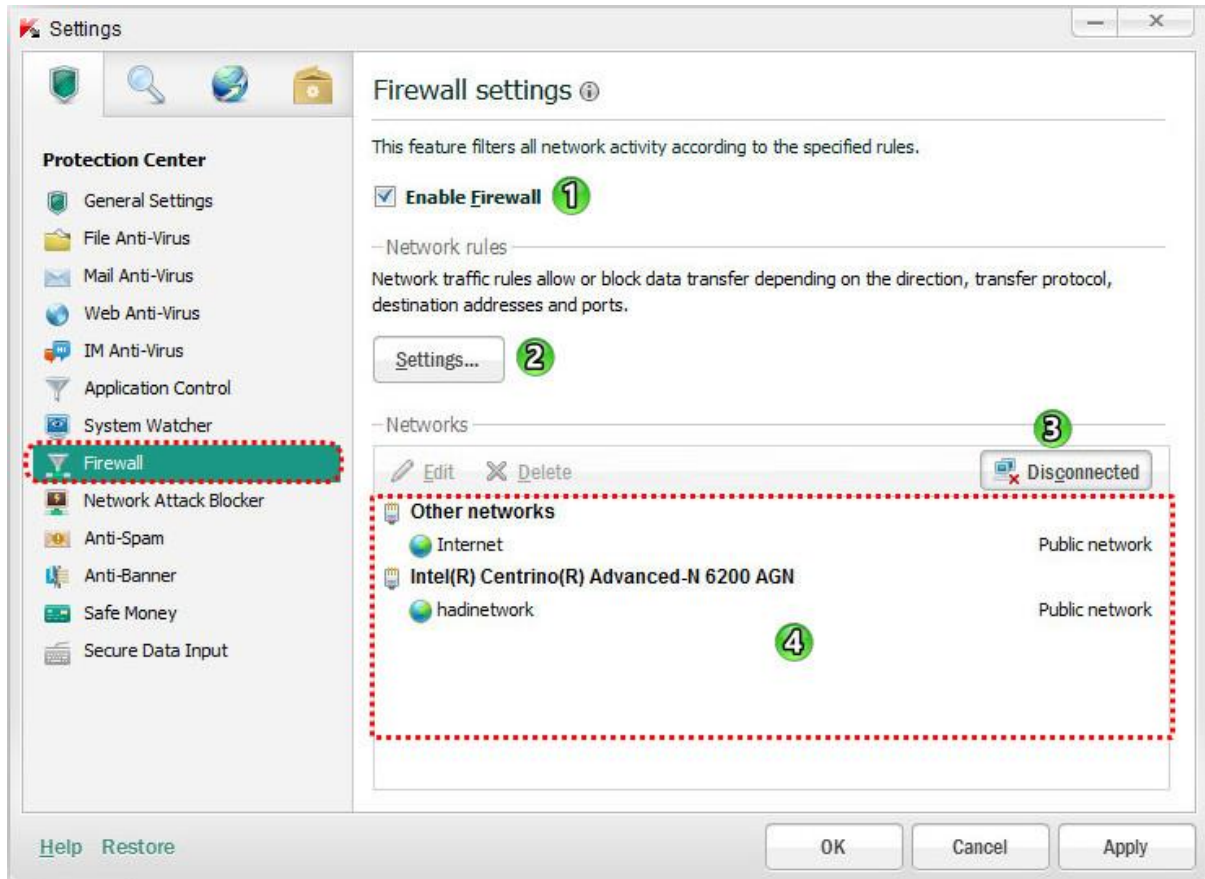
**On detecting possibility to roll back malware actions** : در صورت احتمال تشخیص عملکرد **Malware**

برای بازگردانی دو حالت زیر را میتوان انتخاب کرد: (قسمت ۸ و ۹)

۸- **Select action automatically** : انتخاب عملکرد بصورت اتوماتیک

۹- **Select action** : انتخاب عملکرد دستی که شامل :

۱- **Roll back** (بازگردانی) ۲- **Do not roll back** (عدم بازگردانی)



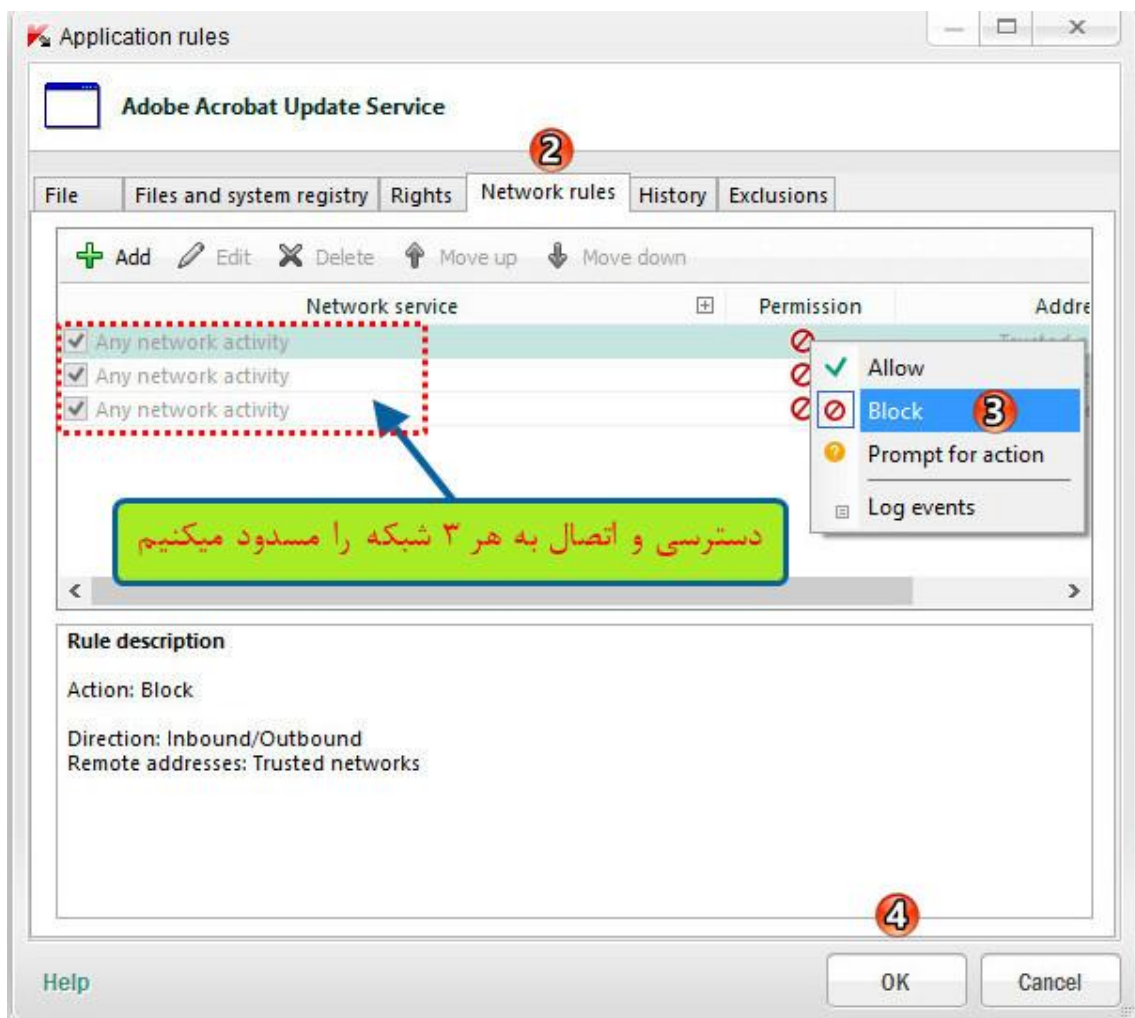
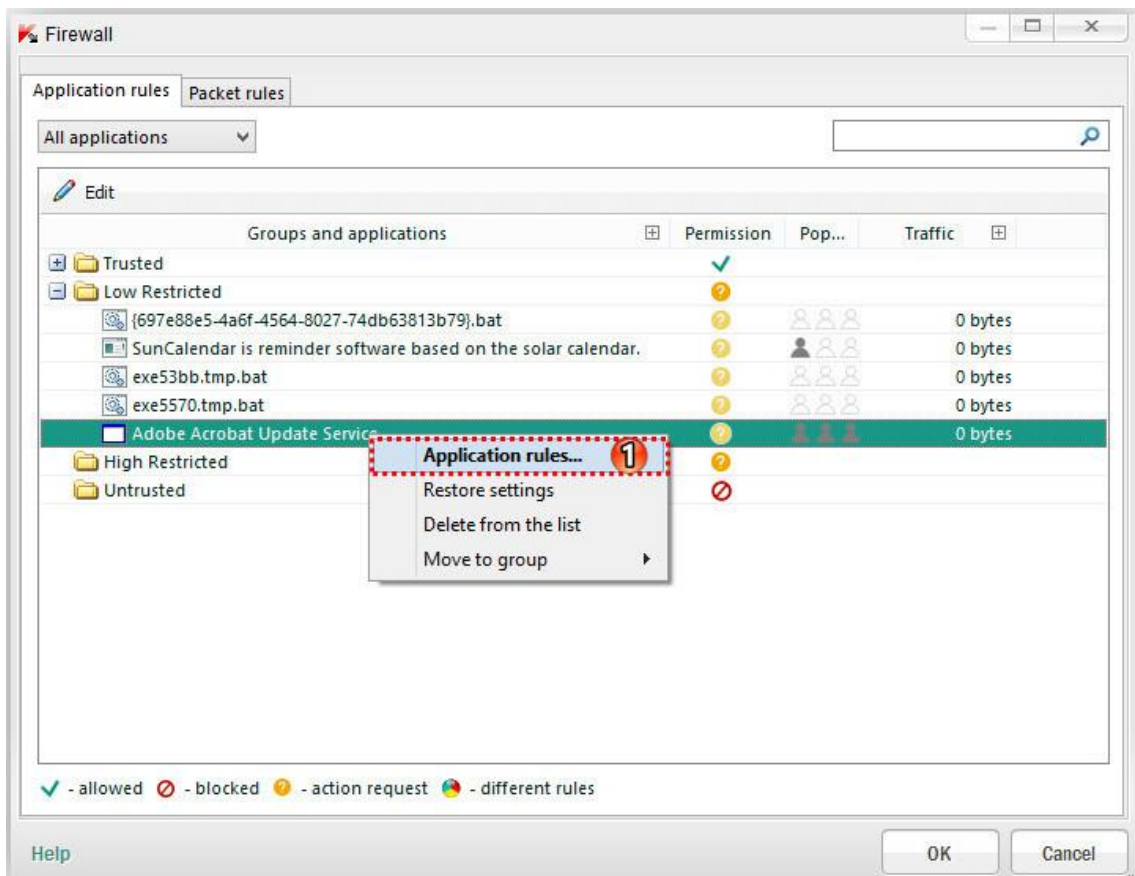
۱- Enable Firewall : فعال کردن فایروال

۲- Settings (تنظیمات) : تنظیمات این قسمت بصورت کامل در بخش Application control توضیح داده شده است. در این قسمت فقط یک مثال که کاربرد زیادی هم داره براتون میزنم.

**قرار دادن برنامه ها داخل فایروال برای جلوگیری از اتصال به اینترنت :**

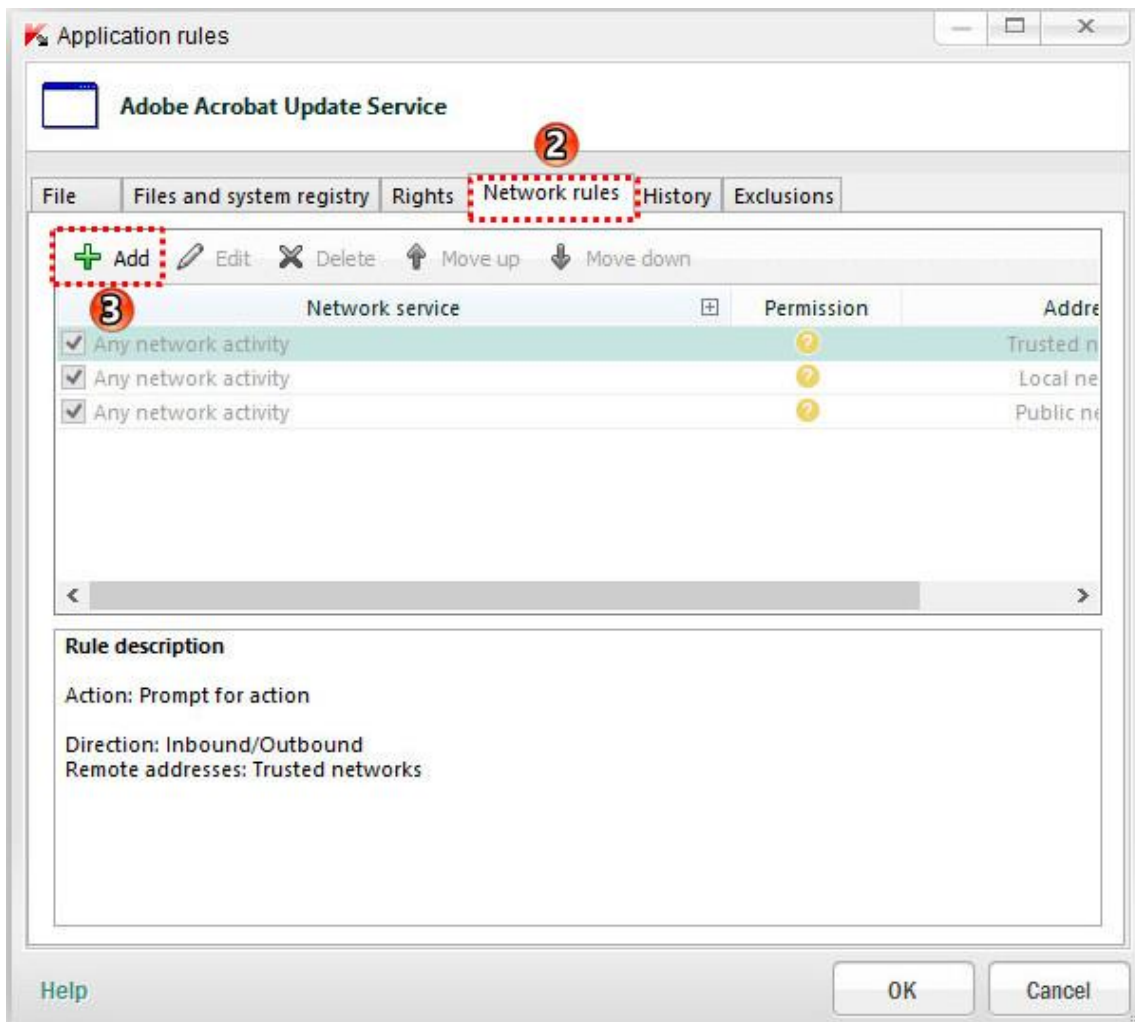
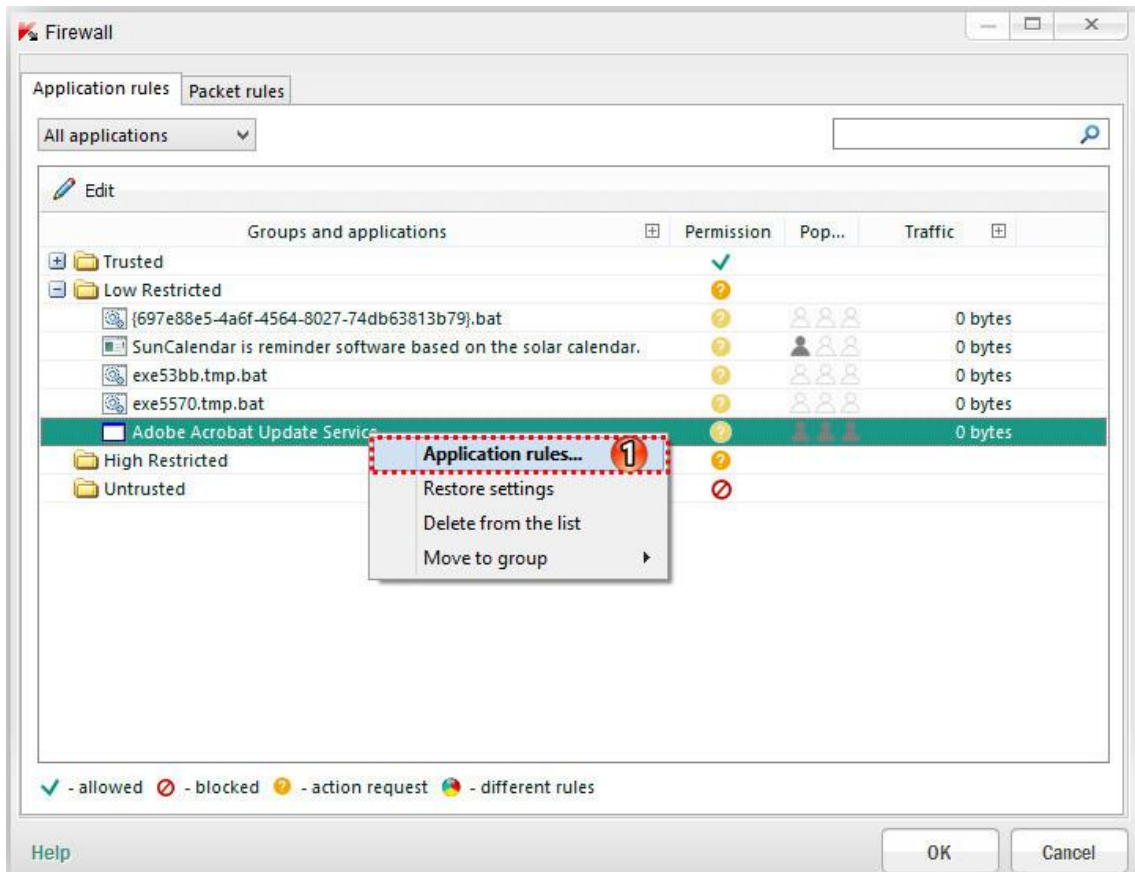
برای همه ی ما پیش میاد که قصد داریم از اتصال یکسری از برنامه ها به اینترنت (جهت جلوگیری از باطل شدن کرک و ... ) جلوگیری کنیم. برای اینکار در قسمت فایروال بر روی دکمه Setting کلیک کرده و طبق اسکرین شاتهای زیر عمل میکنیم.

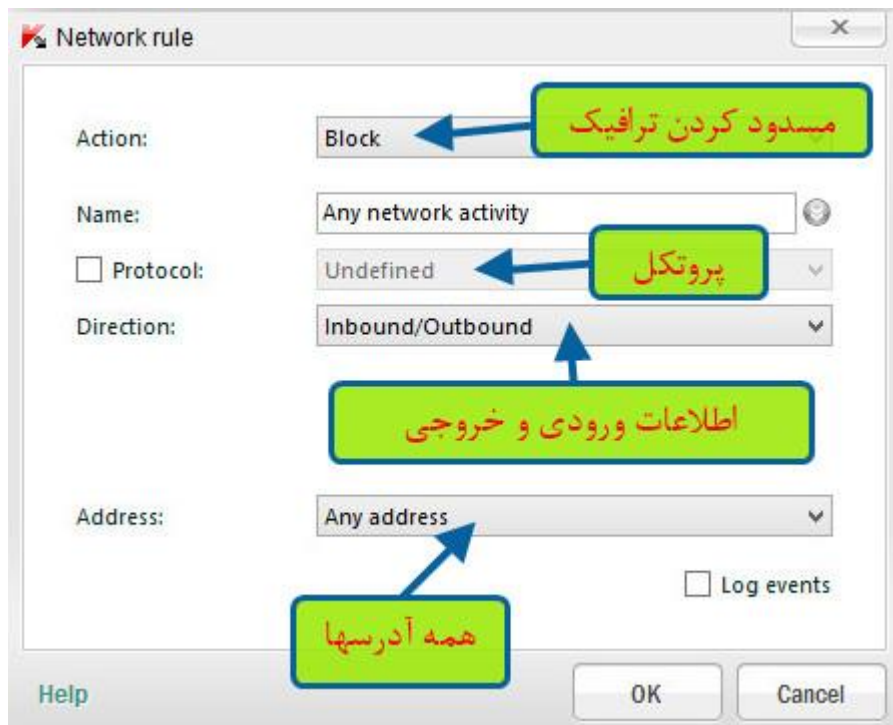




بعد از مرحله ۴ باید مراحل بعدی را **ok** و **apply** کرد. در اینجا کار جلوگیری از اتصال برنامه به اینترنت تمام است.

همچنین برای جلوگیری از اتصال برنامه ها به اینترنت میتوانیم بصورت دستی یک قانون جدید را ایجاد کنیم.

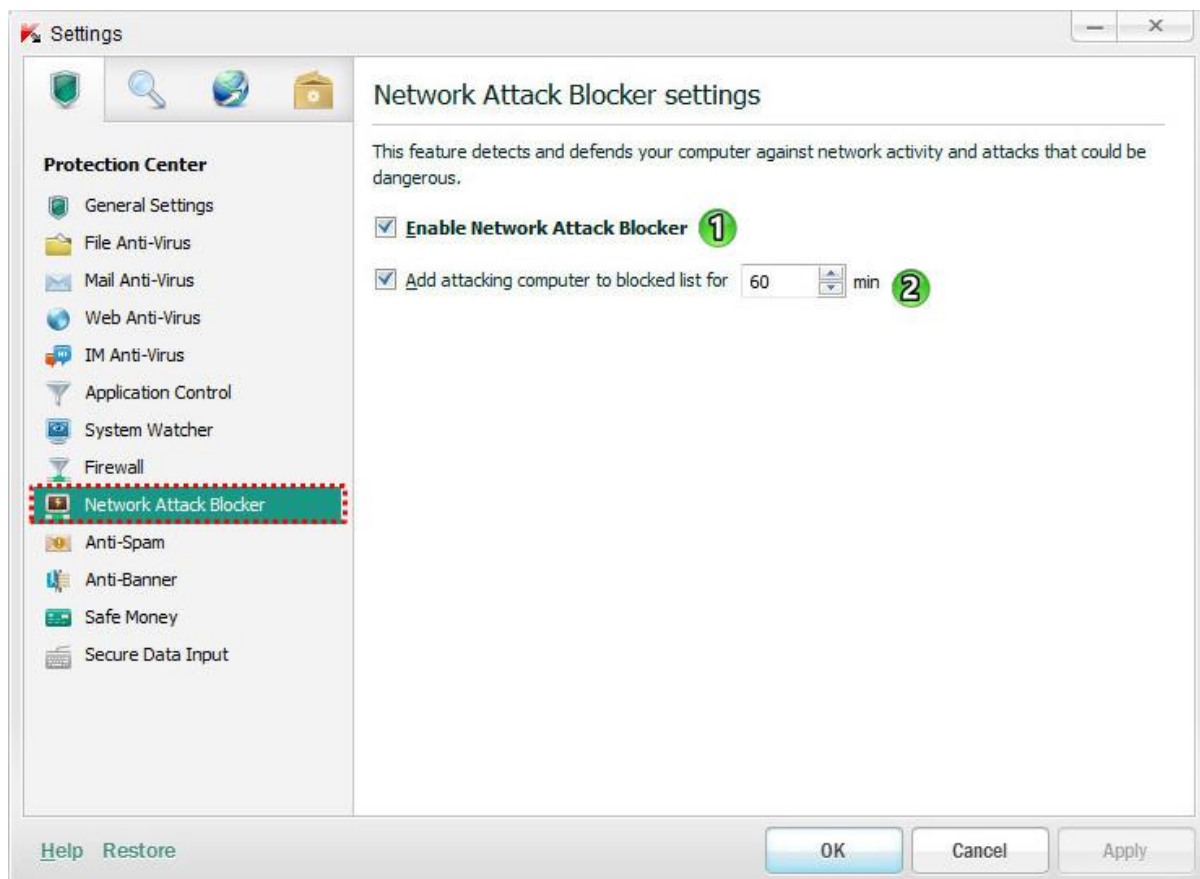




بعد از این مرحله باید مراحل بعدی را **ok** و **apply** کرد. در اینجا کار جلوگیری از اتصال برنامه به اینترنت تمام است.

۳- **Disconnected**: با کلیک کردن روی این دکمه اتصالات فعال و غیر فعال در لیست شبکه نمایش داده میشود.

۴- **Networks**: شامل اتصالات شبکه که فایروال بر روی کامپیوتر شما شناسایی میکند.



۱- **Enable Network Attack Blocker**: فعال کردن این قسمت (مسدود سازی حملات شبکه ای)

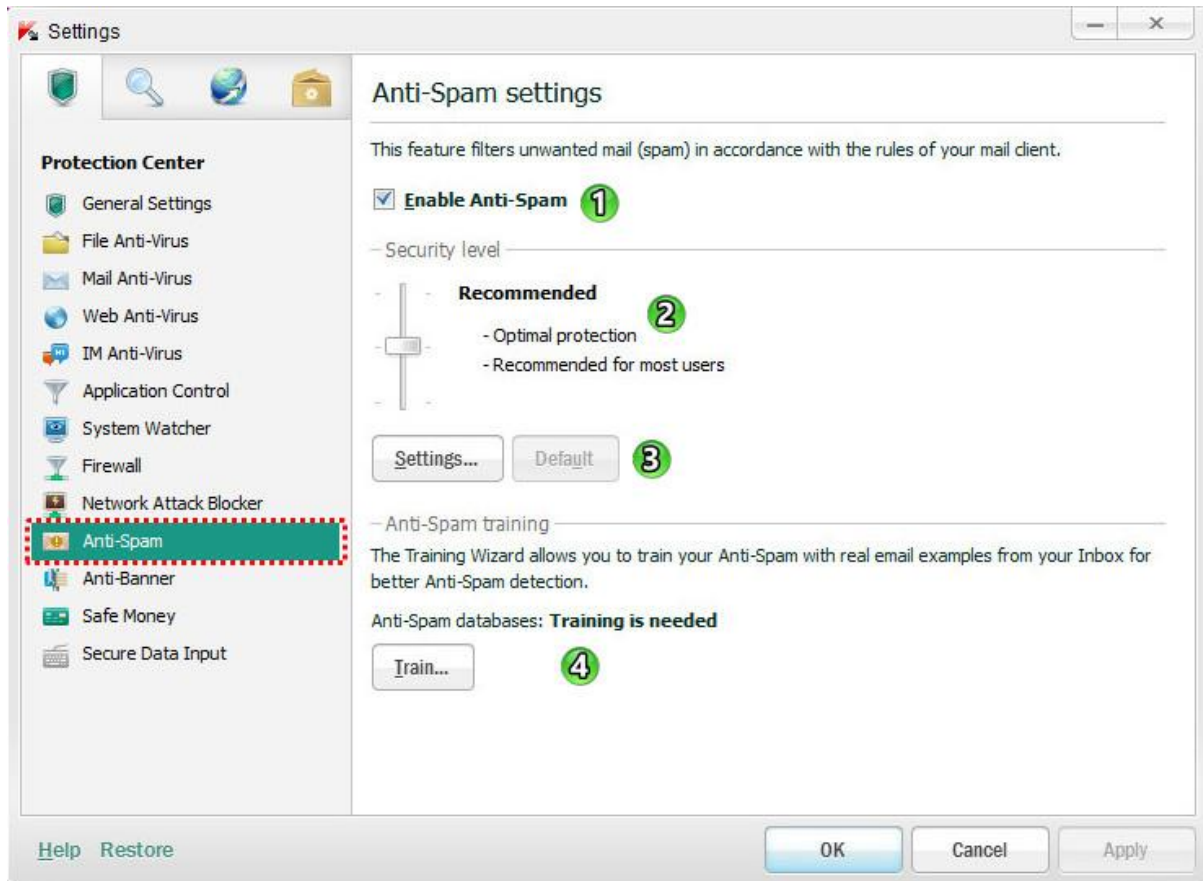
با تیکدار بودن این قسمت ، ترافیک ورودی شبکه برای فعالیت های مشخص حملات شبکه ای ، اسکن میشود. زمانی که تلاش برای حمله به رایانه شما شناسایی شود، KIS هر گونه فعالیت شبکه ای و حمله به سمت کامپیوتر شما را مسدود میکند.

۲- **Add the attacking computer to the list of blocked computers for**: اضافه کردن کامپیوتر حمله

کننده به لیست مسدود شده ها برای بازه زمانی مشخص (پیش فرض ۶۰ دقیقه)

## ۱۰- ضد هرزنامه (Anti-Spam)

این ویژگی ایمیل های ناخواسته (اسپم) را مطابق با قوانین سرویس گیرنده پست الکترونیکی شما، فیلتر میکند.



### ۱- Enable Anti-Spam : فعال کردن ضد هرزنامه (ضد اسپم)

با تیکدار بودن این قسمت، ایمیل های ناخواسته (اسپم) تشخیص داده میشود و مطابق با قوانین سرویس گیرنده پست الکترونیکی شما، پردازش میشود.

۲- Security level (سطح امنیتی) : در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را انتخاب کرد :

#### High (زیاد) :

در این سطح امنیتی، حداکثر سطح فیلتر کردن هرزنامه ها در نظر گرفته میشود.

در این سطح امنیتی، پیامهایی که شباهت بیش از ۵۰ درصدی به اسپم دارند، در نظر گرفته میشود.

#### Recommended (توصیه شده) :

در این سطح امنیتی، تعادل بهینه بین عملکرد و امنیت تضمین میشود و برای بیشتر مواقع مناسب است.

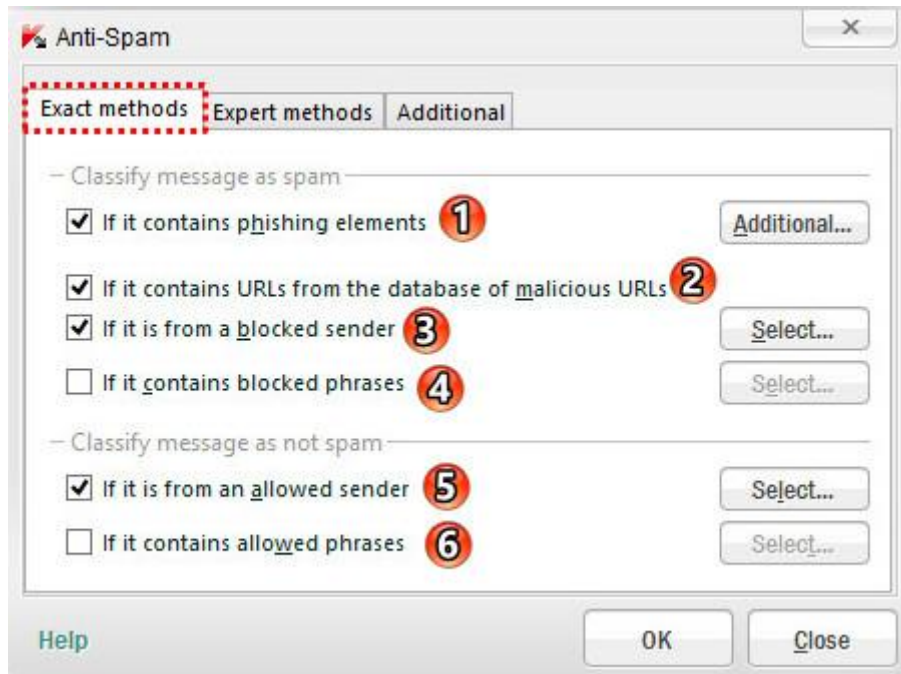
این سطح امنیتی پیش فرض است.

#### Low (کم) :

در این سطح امنیتی، حداقل فیلتر کردن هرزنامه ها را شامل میشود.

سطح امنیتی پایین در هنگام کار در یک محیط امن توصیه می شود. (برای مثال، هنگام استفاده از ایمیل های رمزگذاری شده در شرکت های بزرگ)





۱- **If it contains phishing elements**: اسکن پیام های ایمیل برای عناصر فیشینگ در متن و یا URL های موجود در لیست آدرس های فیشینگ

اگر در پیام ها ، URL های موجود در لیست آدرس های فیشینگ پیدا شود ، آن ایمیل به عنوان **هرزنامه** تشخیص داده میشود.  
۲- **If it contains URLs from the database of malicious URLs**: بررسی گنجاندن لینک های موجود در پیام ها در لیست آدرسهای مخرب

اگر در پیام ها ، URL های موجود در لیست آدرس های مخرب پیدا شود ، آن ایمیل به عنوان **هرزنامه** تشخیص داده میشود.  
۳- **If it is from a blocked sender**: اگر فرستنده در لیست مسدود شده ها باشد ، آن ایمیل به عنوان **هرزنامه** تشخیص داده میشود.

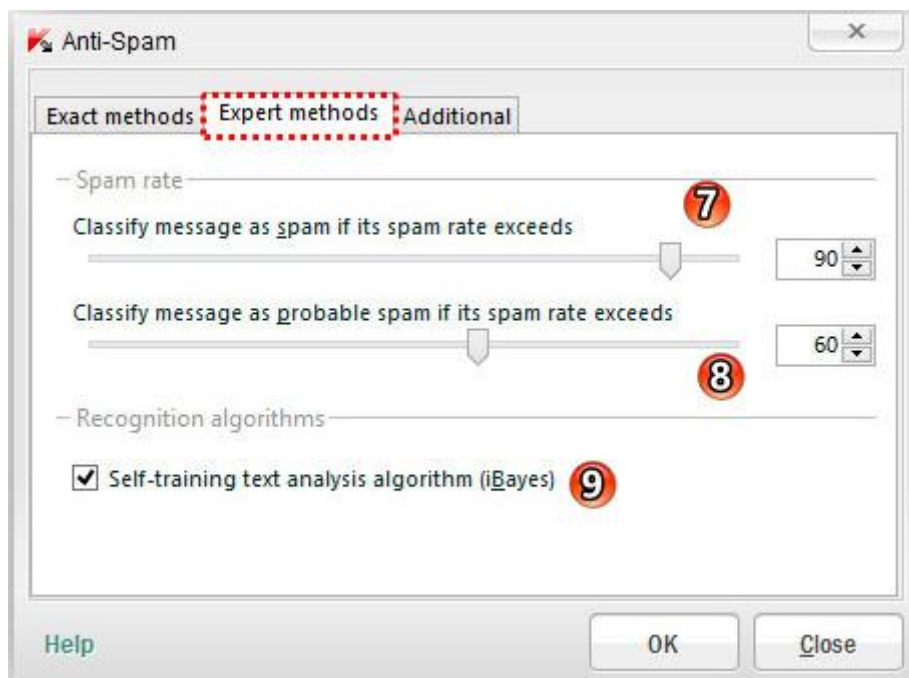
برای تعیین لیست مسدود شدگان از دکمه **select** روبروی خودش استفاده کنید.

۴- **If it contains blocked phrases**: اگر در پیام از عبارات مسدود شده استفاده شده باشد، آن پیام **هرزنامه** تشخیص داده میشود.

برای تعیین عبارات غیر مجاز ، از دکمه **select** روبروی خودش استفاده کنید.

۵- **If it is from an allowed sender**: اگر فرستنده در لیست فرستندگان مجاز باشد، ایمیلهای آن به عنوان اسپم شناخته نمیشود.

۶- **If it contains allowed phrases**: اگر در پیام از عبارات مجاز استفاده شده باشد ، آن پیام **هرزنامه** تشخیص داده نمیشود.



**Spam rate :** در بخش نرخ اسپم، می توان مقادیر تنظیمات Anti-Spam برای تشخیص اسپم و اسپمهای احتمالی در پیام ها را مشخص کرد. نرخ اسپم - یک مقدار احتمالاتی است که از Anti-Spam برای تعریف اینکه آیا پیام هرزنامه است یا نه، مشخص میشود و اگر مقدار نرخ اسپم یک ایمیل بیش از مقدار تنظیم شده باشد، آن پیام به عنوان هرزنامه یا اسپم احتمالی شناخته میشود.

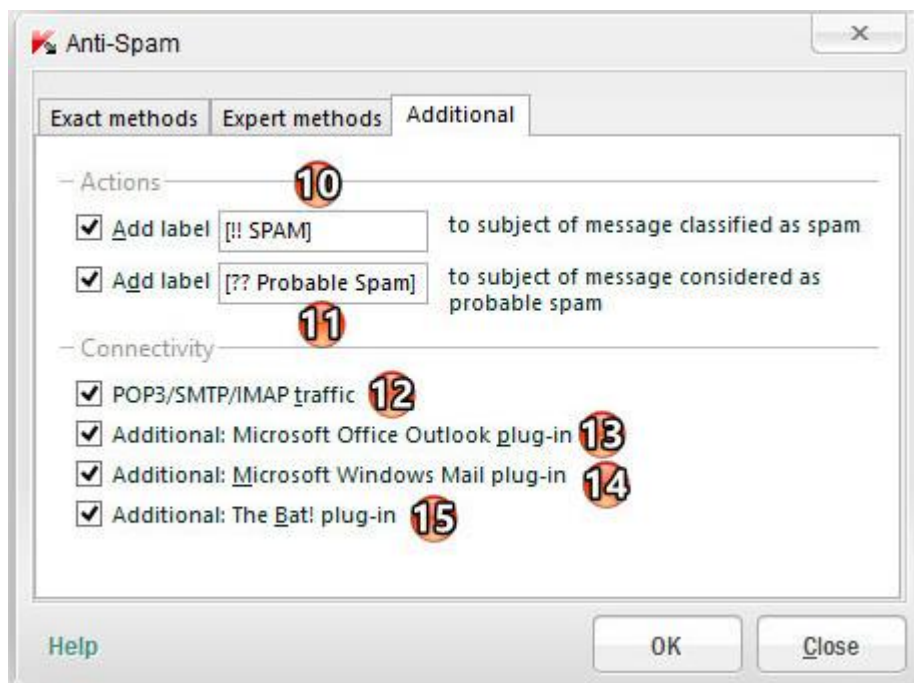
**۷- Classify message as spam if its spam rate exceeds :** طبقه بندی پیام به عنوان هرزنامه اگر نرخ اسپم آن بیش از مقدار تعیین شده باشد.

**۸- Classify message as probable spam if its spam rate exceeds :** طبقه بندی پیام به عنوان هرزنامه احتمالی اگر نرخ اسپم آن بیش از مقدار تعیین شده باشد.

**مقادیر پیش فرض قسمتهای ۷ و ۸ به سطح امنیتی انتخاب شده دارد.**

**۹- Self-training text analysis algorithm (iBayes) :** این الگوریتم (iBayes) باعث تصمیم گیری در مورد تعیین وضعیت پیام از جهت مفید یا اسپم بودن، بر اساس عبارات موجود در آن پیام است.

قبل از شروع کار، باید نمونه هایی از ایمیل های مفید و ایمیل های اسپم به الگوریتم iBayes، به عنوان مثال، آموزش داده شود.



**Actions** : در این بخش ، می توان برچسب موضوع پیامها را از جهت اسپم یا اسپم احتمالی مشخص کرد.

۱۰ - **Add label [!! SPAM] to subject of message considered as spam** : اضافه کردن برچسب [SPAM!!]

به موضوع پیامهایی که به عنوان اسپم تشخیص داده شده اند.

۱۱ - **Add label [?? Probable Spam] to subject of message considered as probable spam** : اضافه

کردن برچسب [Probable Spam??] به موضوع پیامهایی که به عنوان اسپم های احتمالی تشخیص داده شده اند.

**Connectivity** : در این بخش ، می توان تنظیمات اتصال ضد اسپم به مشترکان ایمیل برای یکپارچه سازی را مشخص کرد.

۱۲ - **POP3/SMTP/IMAP traffic** : اسکن ایمیل های ورودی از طریق پروتکل های POP3/SMTP/IMAP

۱۳ - **Additional: Microsoft Office Outlook plug-in** : فعال کردن Microsoft Office Outlook plug-in

۱۴ - **Additional: Microsoft Windows Mail plug-in** : فعال کردن Microsoft Windows Mail plug-in

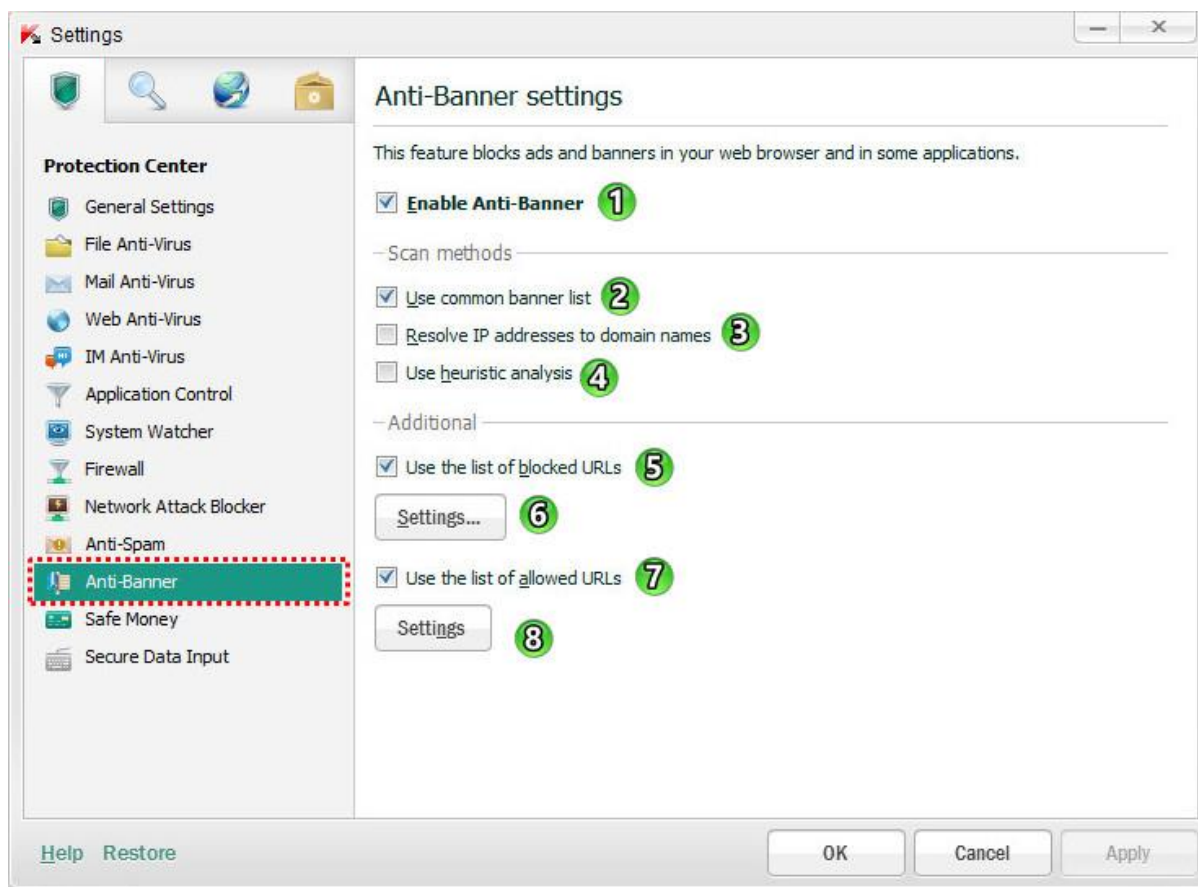
۱۵ - **Additional: The Bat! plug-in** : فعال کردن The Bat! plug-in

#### ۴ - **Train** (آموزش دیدن) :

با کلیک بر روی این دکمه یک ویزارد باز میشود که به اسکن پوشه های Microsoft Office Outlook و Microsoft

Outlook Express (ایمیل ویندوز) برای شناختن (آموزش دیدن) ایمیل های مفید و ایمیل های اسپم ، می پردازد.

بعد از اتمام آموزش ، **Anti-Spam** با استفاده از نتایج حاصل از آموزش به فیلتر پست الکترونیکی می پردازد.



۱- **Enable Anti-Banner**: با فعال کردن این قسمت ، تبلیغات روی وب سایتها مسدود میشود.

۲- **Use common banner list**: استفاده از لیست تبلیغات مشترک برای مسدود سازی تبلیغات

۳- **Resolve IP addresses to domain names**: تفکیک پذیری به صورت خودکار آدرس IP به نام دامنه در لیست

آدرسهای مجاز و آدرس مسدود شده

**این قابلیت از تکرار آدرس ها جلوگیری میکند.**

۴- **Use Heuristic Analysis**: استفاده از تجزیه و تحلیل اکتشافی

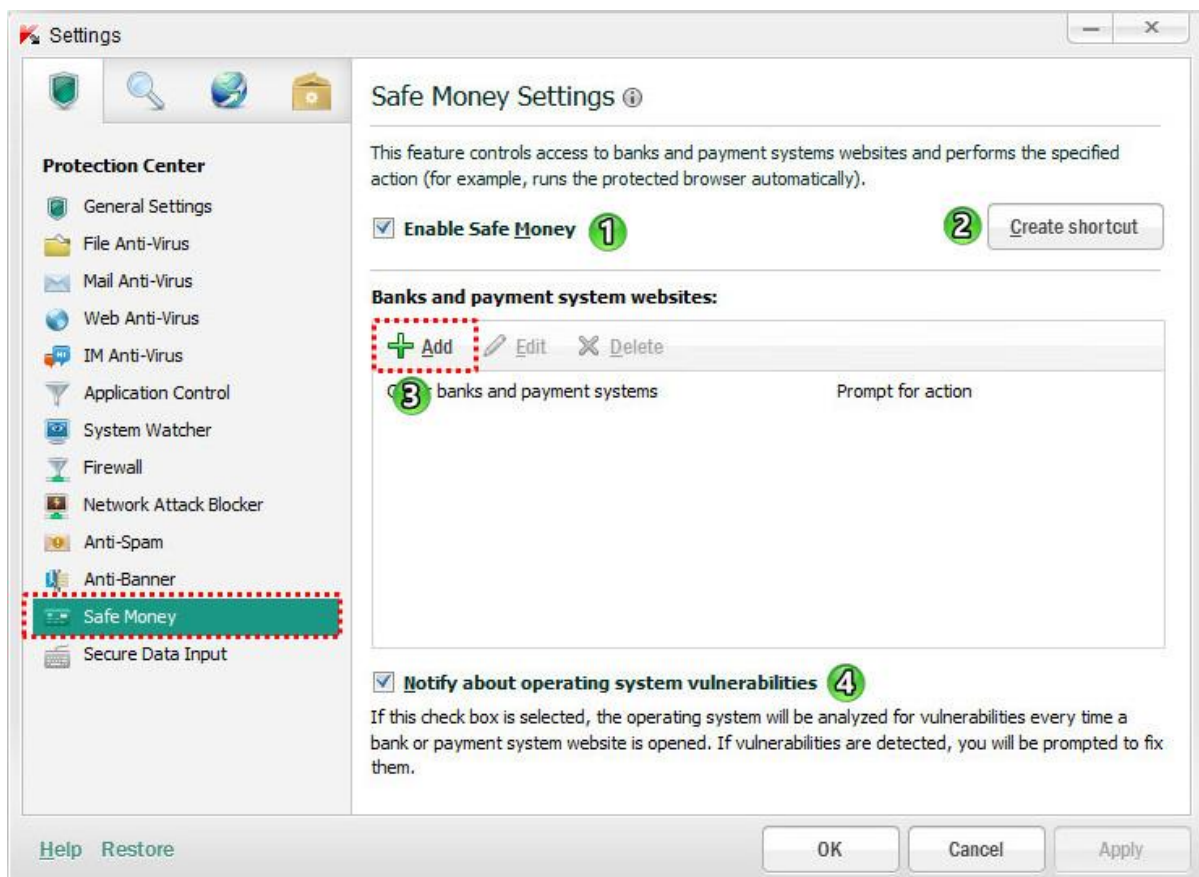
۵- **Use the list of blocked URLs**: استفاده از لیست آدرس های مسدود شده

۶- **Settings**: جهت ایجاد لیست آدرس بنرها و URL هایی که باید مسدود شود. (مثال : مسدود کردن سایت

http://peyvandha.ir که خیلی وقتها همراه لینکها نمایش داده میشه )

۷- **Use the list of allowed URLs**: استفاده از لیست آدرس ها مجاز

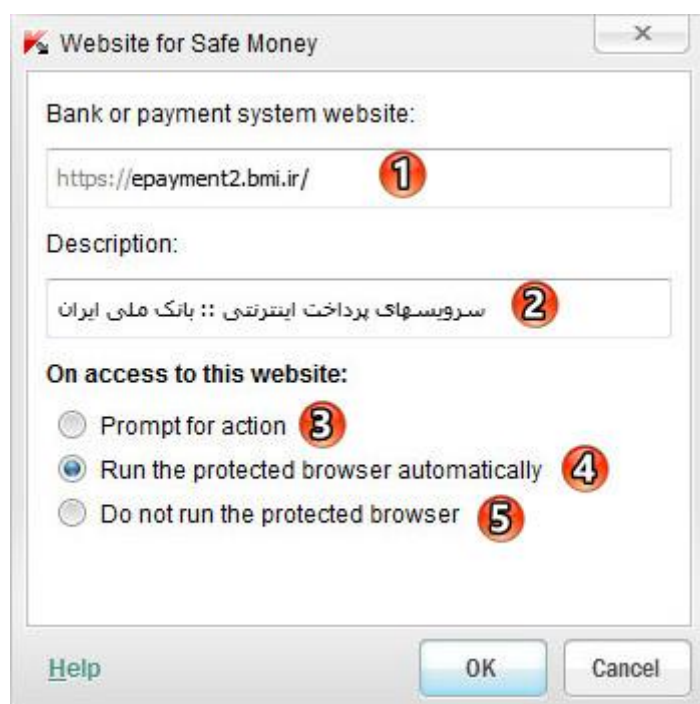
۸- **Settings**: جهت ایجاد لیست آدرسهایی که Anti-Banner نباید آنها را مسدود کند.



۱- **Enable Safe Money**: با فعال کردن این قسمت، نظارت بر همه تلاش های دسترسی به وب سایت بانک ها و یا سیستم های پرداخت نظارت میشود.

۲- **Create shortcut**: ایجاد میانبر برای دسترسی سریعتر به لیست وب سایتهای پرداخت و خرید اینترنتی امن که برای دسترسی به آنها نیاز به مرورگر محافظت شده می باشد.

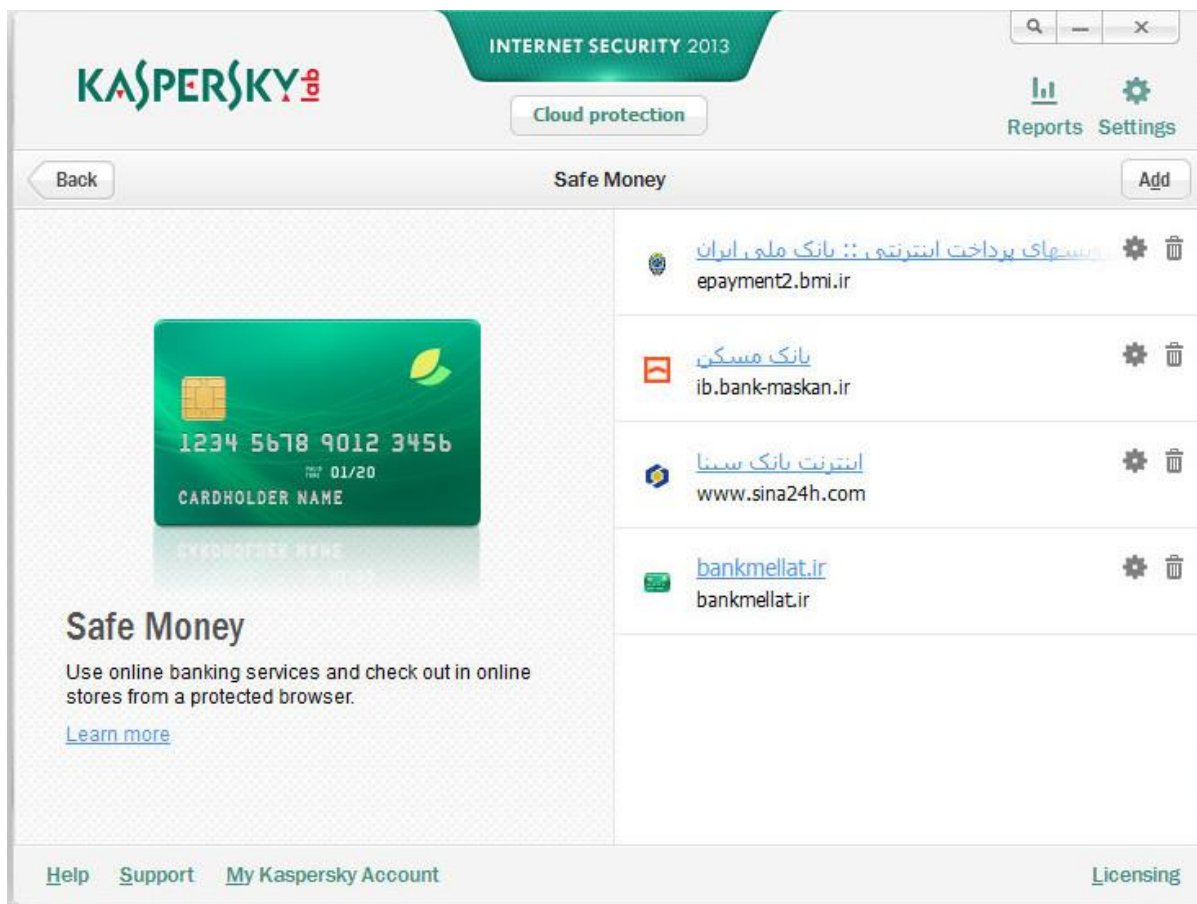
۳- **Add**: اضافه کردن وب سایت یک بانک یا سیستم پرداخت





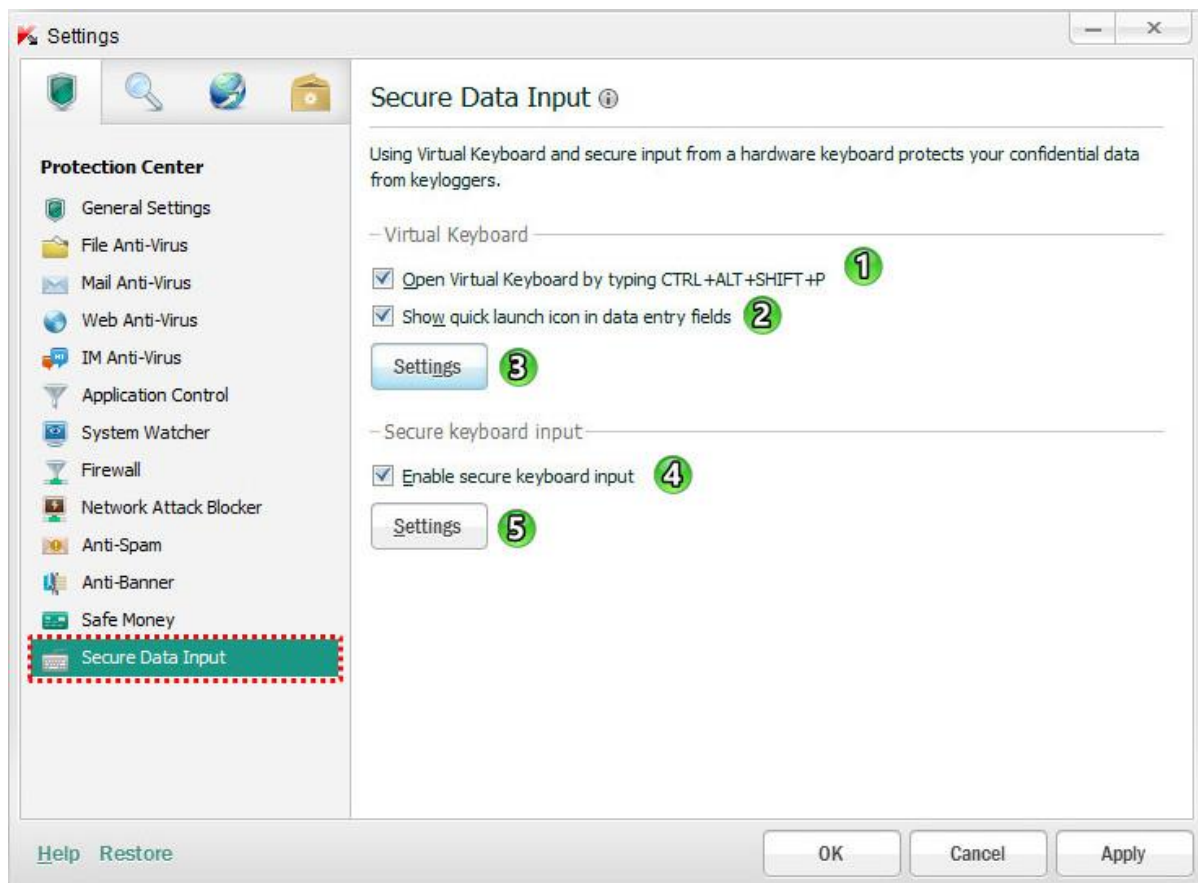
- ۱- **Bank or payment system website**: وارد کردن آدرس وب سایت یک بانک یا یک سیستم پرداخت
- ۲- **Description**: شرحی از وب سایت یا سیستم های پرداخت که باید نمایش داده شود. (برای مثال، نام بانک) اگر در این قسمت هیچی وارد نکنیم بعد از تأیید بصورت خودکار اضافه میشود.
- ۳- **Prompt for action**: بی درنگ برای عمل
- ۴- **Run the protected browser automatically**: اجرای مرورگر حفاظت شده به صورت خودکار
- ۵- **Do not run the protected browser**: عدم اجرای مرورگر حفاظت شده

### پنجره Safe Money بعد از اضافه کردن بانکها



- ۴- **Notify about operating system vulnerabilities**: خبر در مورد آسیب پذیری های سیستم عامل

**نکته:** قابلیت Safe Money در Microsoft Internet Explorer 10 سبک مترو (Metro style) در دسترس نیست.

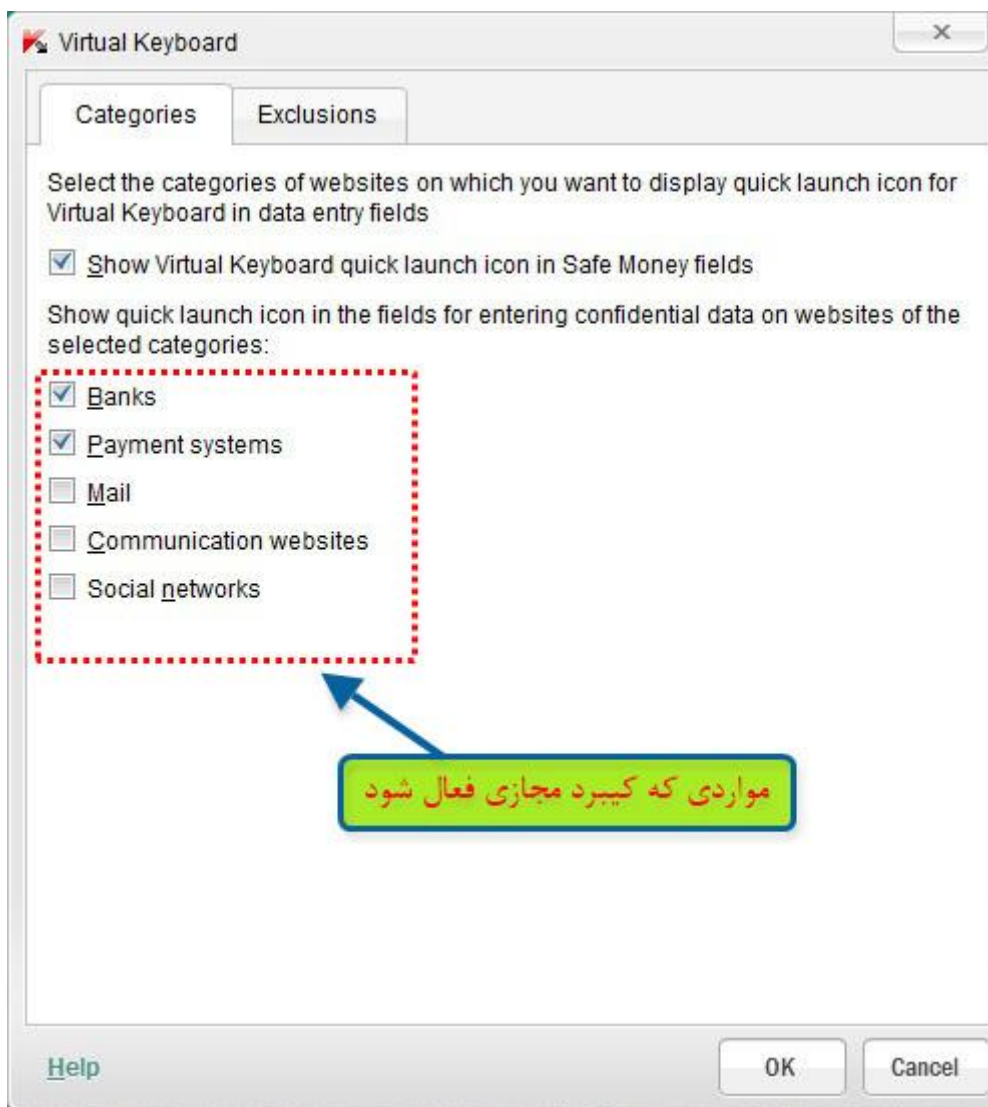


۱- **Open Virtual Keyboard by typing CTRL+ALT+SHIFT+P**: باز کردن صفحه کلید مجازی با فشار

دادن کلیدهای CTRL + ALT + SHIFT + P

۲- **Show quick launch icon in data entry fields**: نمایش آیکون راه اندازی سریع صفحه کلید مجازی در زمینه

های ورود اطلاعات



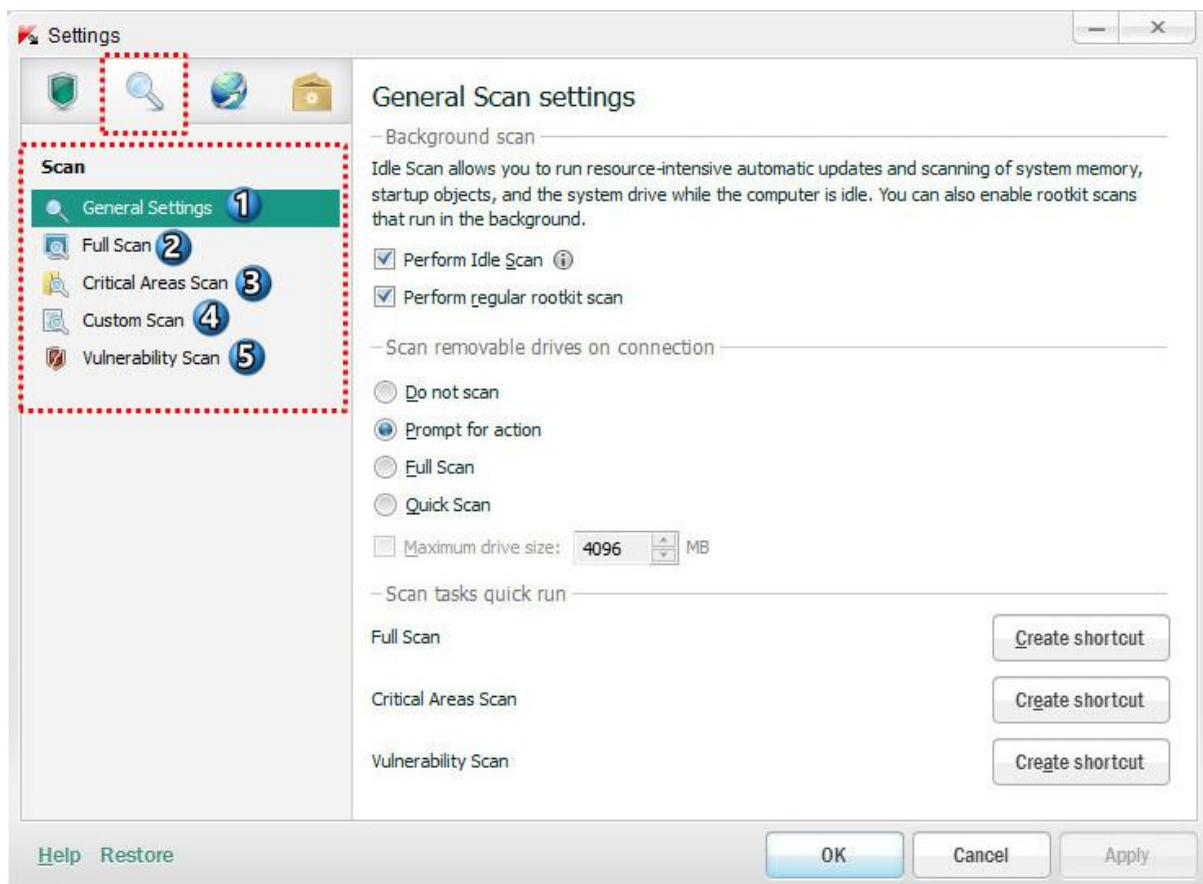
- ۱- وب سایت بانکها ( Banks )
- ۲- ورود به وب سایت سیستم های پرداخت ( Payment systems )
- ۳- ورود در وب سایت های ارائه دهنده خدمات ایمیل ( Mail )
- ۴- ورود در وب سایت های طراحی شده برای ارتباطات کاربران اینترنت ( Communication websites )
- ۵- ورود به وب سایت های شبکه های اجتماعی ( Social networks )



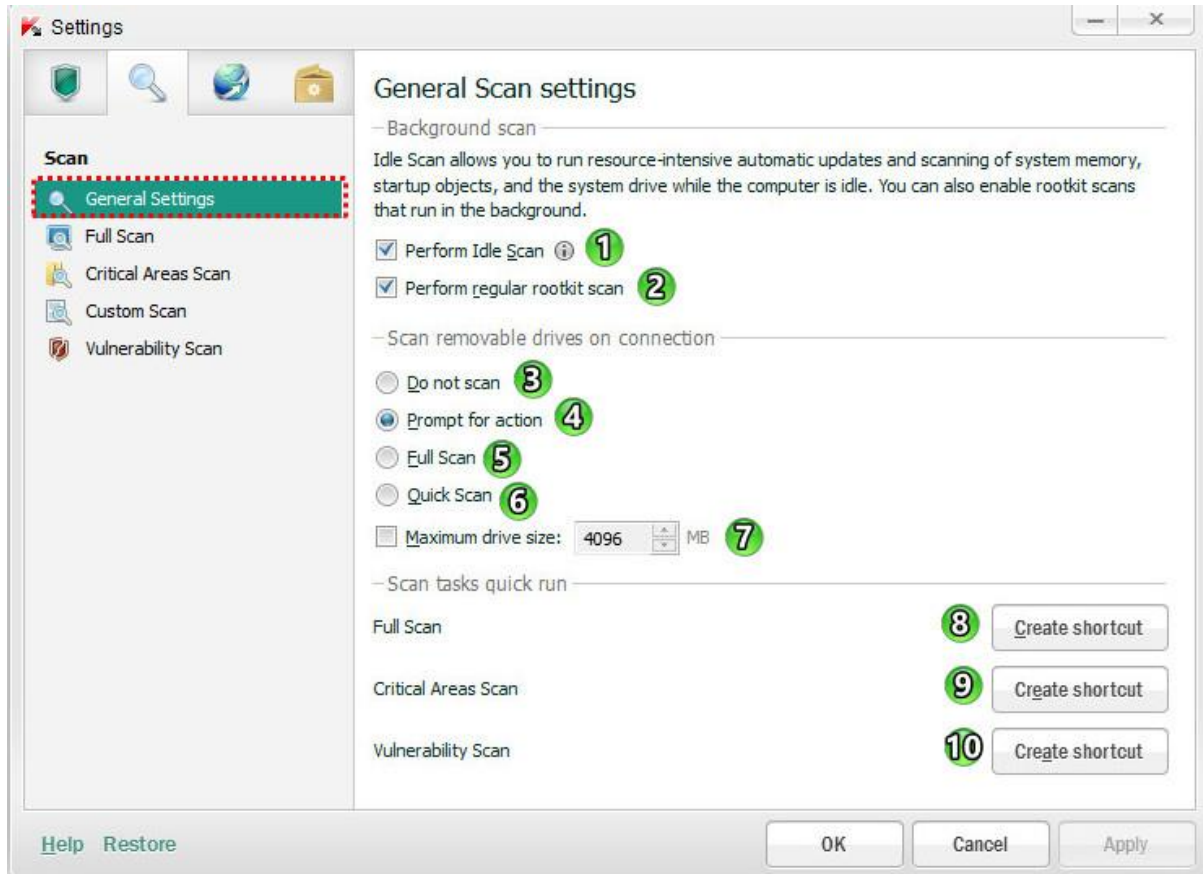
۴- **Enable secure keyboard input**: فعال کردن قسمت ورودی داده ها با کیبرد امن

۵- **Settings (تنظیمات)**: همانند تنظیمات قسمت قبل

**نکته:** قابلیت **Secure Data Input** در **Microsoft Internet Explorer 10** سبک مترو (**Metro style**) در دسترس نیست.







۱- **Perform Idle Scan**: با فعال بودن این گزینه، سیستم (حافظه سیستم، پارتیشنهای سیستم و startup) در حالت بیکاری اسکن میشود. در حال اجرا از وظایف اسکن (و وظایف بروز رسانی اتوماتیک در حالی که کامپیوتر قفل شده است و یا محافظ صفحه نمایش فعال است).

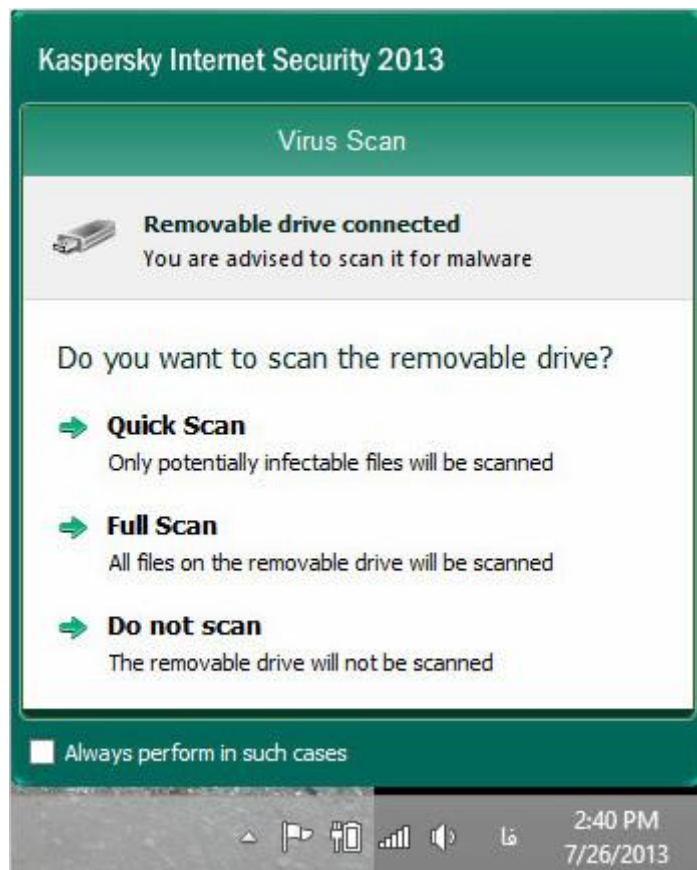
اگر لپ تاپ با باتری روشن باشد، هیچ گونه اسکنی در حالت بیکاری صورت نمی گیرد.

۲- **Perform regular rootkit scan**: اسکن منظم برای روت کیت‌های فعال در پس زمینه

**Scan removable drives on connection**: در این بخش می توان نوع عملیات هنگام اتصال هر نوع درایو removable به کامپیوتر را انتخاب کرد.

۳- **Do not scan**: عدم اسکن

۴- **Prompt for action**: در صورت انتخاب این گزینه هنگام اتصال درایوهای removable از کاربر نوع اسکن سوال میشود.



۵- **Full Scan** : اسکن کامل

۶- **Quick Scan** : اسکن سریع

۷- **Maximum drive size** : ایجاد محدودیت حجمی برای اسکن درایوها

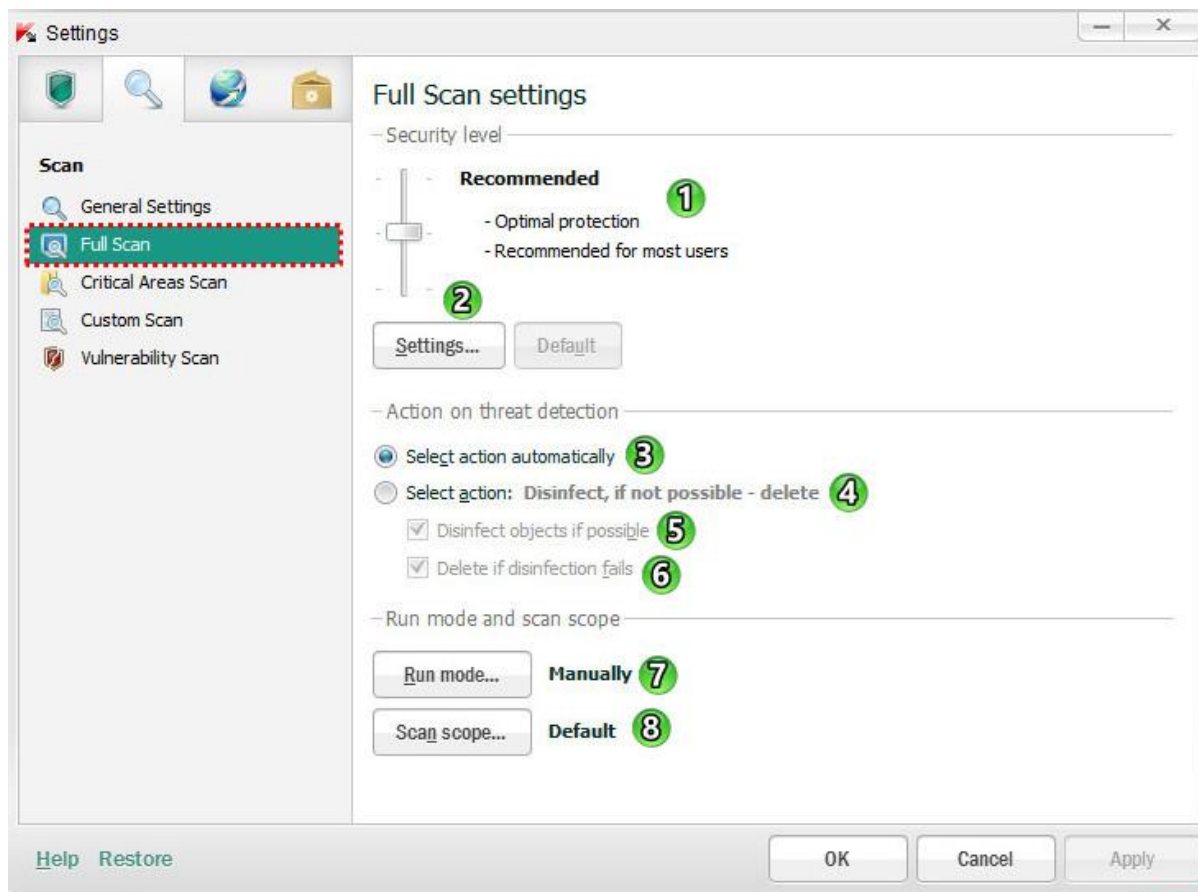
با فعال بودن این گزینه ،، درایوهایی که حجمشان از حجم تعیین شده تجاوز کند (پیش فرض ۴۰۹۶ مگا بایت) اسکن نمیشود.

**Scan tasks quick run** : ایجاد کلید میانبر برای دسترسی سریع به انواع اسکن

۸- **Full Scan - Create shortcut** : ایجاد میانبر برای اسکن کامل

۹- **Critical Areas Scan - Create shortcut** : ایجاد میانبر برای اسکن قسمتهای بحرانی

۱۰- **Vulnerability Scan - Create shortcut** : ایجاد میانبر برای اسکن قسمتهای آسیب پذیر



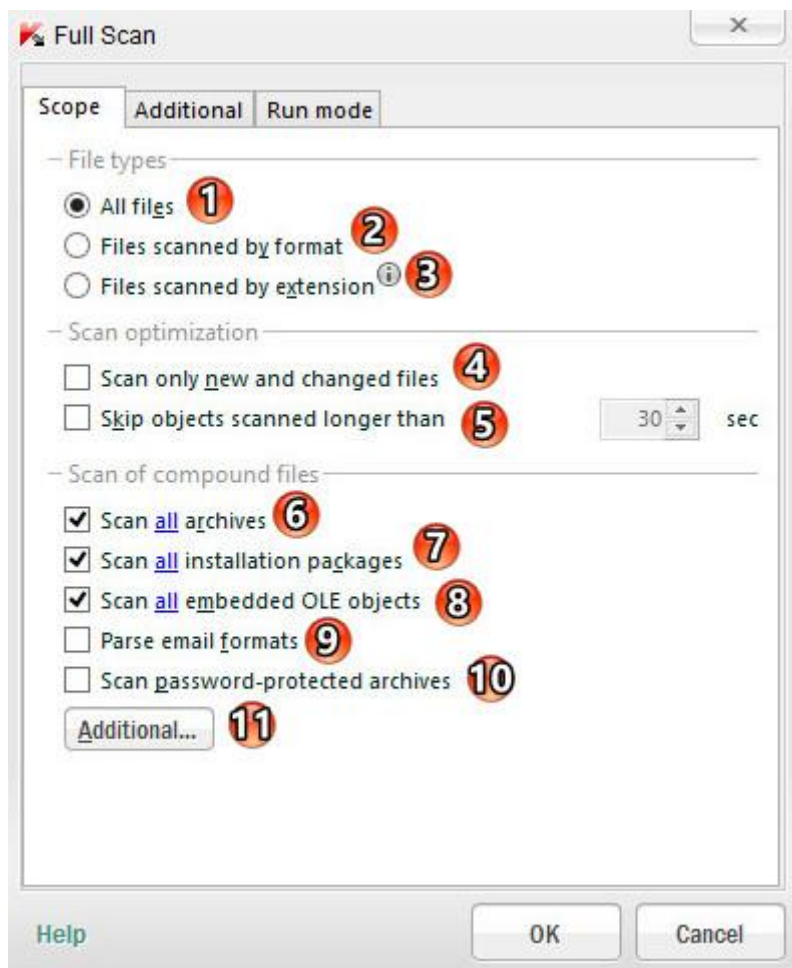
۱- **Security level (سطح امنیتی):** در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را برای فایل ها و حافظه انتخاب کرد.

**High** (بالاترین سطح امنیتی)

**Recommended** (سطح امنیتی توصیه شده)

**Low** (کمترین سطح امنیتی)

۲- **Setting (تنظیمات):** با کلیک بر روی این دکمه پنجره تنظیمات باز میشود.



**File types :** در این قسمت مواردی که باید اسکن شود را میتوان تعیین کرد.

۱- **All files :** اسکن تمام فایلها ، فرمتها و پسوندها

۲- **Files scanned by format :** اسکن فایلهایی که ممکن است ویروس به داخل آن نفوذ کند.

۳- **Files scanned by extension :** اسکن فایلها بر اساس پسوند آنها

**Scan optimization :** در بخش بهینه سازی اسکن، می توان تنظیماتی جهت کاهش مدت زمان اسکن اعمال کرد.

۴- **Scan only new and changed files :** فقط اسکن فایل های جدید و تغییر یافته پس از آخرین اسکن

۵- **Skip objects scanned longer than :** اگر مدت زمان اسکن یک فایل ، بیشتر از بازه زمانی مشخص شده طول بکشد، اسکن فایل قطع شود. (پیش فرض ۳۰ ثانیه)

**Scan of compound files :** اسکن فایل های مرکب (اسکن اجزای فایل)

۶- **Scan All archives :** اسکن همه فایلهای فشرده RAR, ARJ, ZIP, CAB, LHA, JAR و ICE

۷- **Scan All installation packages :** اسکن همه بسته های نصب و راه اندازی

۸- **Scan All embedded OLE objects :** اسکن همه موارد تعبیه شده در OLE (مانند: صفحات Microsoft Office

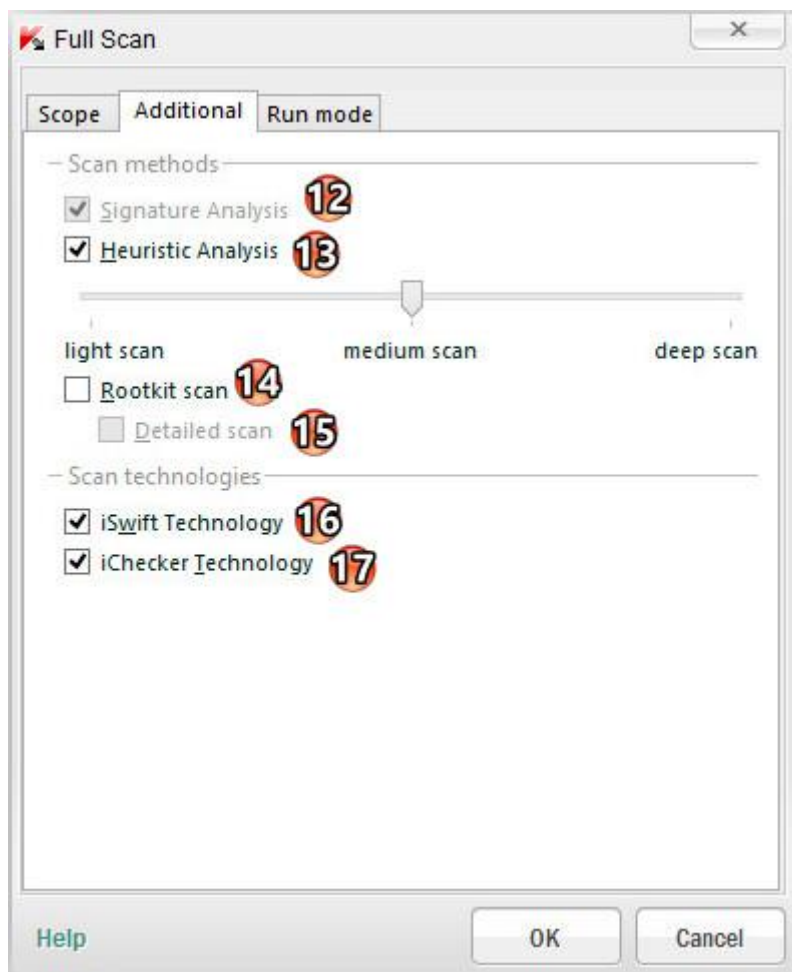
Excel یا ماکروهای تعبیه شده در Microsoft Office Word یا فایلهای پیوست در ایمیل)

۹- **Parse email formats :** تجزیه و تحلیل فرمت های ایمیل (فایلهای پیوست) برای ویروس

۱۰- **Scan password-protected archives :** اسکن فایلهای فشرده محافظت شده با پسورد (با فعال بودن این قسمت

هنگام اسکن فایلهای فشرده رمزدار از شما رمز فایل درخواست میشود).

۱۱- **Additional :** با تنظیم کردن این قسمت میتوان یک محدودیت حجمی برای اسکن فایلهای مرکب ایجاد کرد.



### روشهای اسکن : Scan methods

۱۲- **Signature Analysis**: با استفاده از پایگاه داده کسپرسکی که حاوی شرح تهدیدات و راههای شناخته شده برای خنثی کردن آنها است

۱۳- **Heuristic Analysis**: تجزیه و تحلیل اکتشافی (قبلا توضیح داده شده است)

۱۴- **Rootkit scan**: اسکن روت کیتها

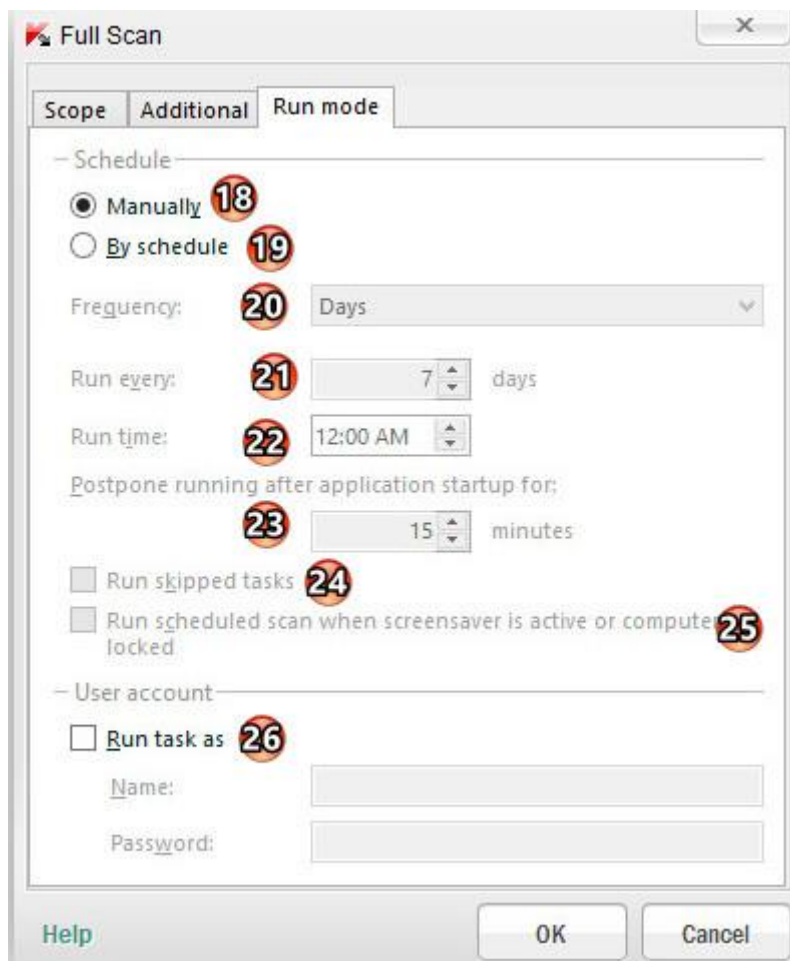
۱۵- **Detailed scan**: اسکن مفصل

### فناوری اسکن : Scan technology

۱۶- **iSwift Technology**: استفاده از فناوری iSwift

۱۷- **iChecker Technology**: استفاده از فناوری iChecker





**Schedule** : برنامه زمانبندی برای اسکن خودکار

۱۸ - **Manually** : بصورت دستی

۱۹ - **By schedule** : توسط برنامه زمانبندی

۲۰ - **Frequency** : فاصله بین اسکن برنامه ریزی شده (بعد از هر دقیقه ، هر ساعت ، هر روز ، هر هفته ، در زمان مشخص ، هر ماه ، بعد از استارت آپ برنامه ها ، بعد از هر آپدیت)

۲۱ - **Run every** : تعداد اجرا شدن در ماه (پیش فرض ۷ بار اجرا شدن در ماه است که میتوان تا ۳۱ بار اجرا در ماه افزایش داد)

۲۲ - **Run time** : اجرا شدن سر ساعت تعیین شده

۲۳ - **Postpone running after application startup for** : به تعویق انداختن اجرا پس از برنامه های استارت آپ برای مدت زمان تعیین شده (پیش فرض ۱۵ دقیقه)

۲۴ - **Run skipped tasks** : اجرای وظایف از قلم انداخته شده (صرفه نظر شده) برای مثال، زمانیکه کامپیوتر خاموش است . با فعال بودن این قسمت ، وظیفه از قلم انداخته شده (صرفه نظر شده) در اسرع وقت انجام می شود.

۲۵ - **Run scheduled scan when screensaver is active or computer is locked** : اجرای اسکن برنامه ریزی شده زمانی که محافظ صفحه فعال است و یا زمانیکه کامپیوتر قفل است.

**Scan methods** : روشهای اسکن

۲۶ - **Run task as** : انجام اسکن با استفاده از حساب کاربری انتخاب شده (حساب کاربری و پسورد را وارد میکنیم)

## Action on threat detection : در این بخش اقداماتی که آنتی ویروس باید بر روی ، تهدیدات تشخیص داده شده

، موارد آلوده یا احتمالاً آلوده انجام شود را انتخاب میکنیم که شامل دو عملکرد زیر میشود:

### ۳- Select action automatically (انتخاب عملکرد اتوماتیک): پس از تشخیص موارد خطرناک، آنتی ویروس به

طور خودکار اعمال توصیه شده توسط متخصصین آزمایشگاه کسپرسکی را انجام می دهد. آنتی ویروس موارد مخرب را پاکسازی یا حذف میکند و اگر برای موارد احتمالاً آلوده قادر به پاکسازی نباشد ، آنرا نادیده میگیرد.

آنتی ویروس قبل از تلاش برای پاکسازی و یا حذف یک مورد آلوده، یک نسخه پشتیبان برای بازسازی پس از پاکسازی تهیه میکند.

### ۴- Select action : انتخاب عملکرد

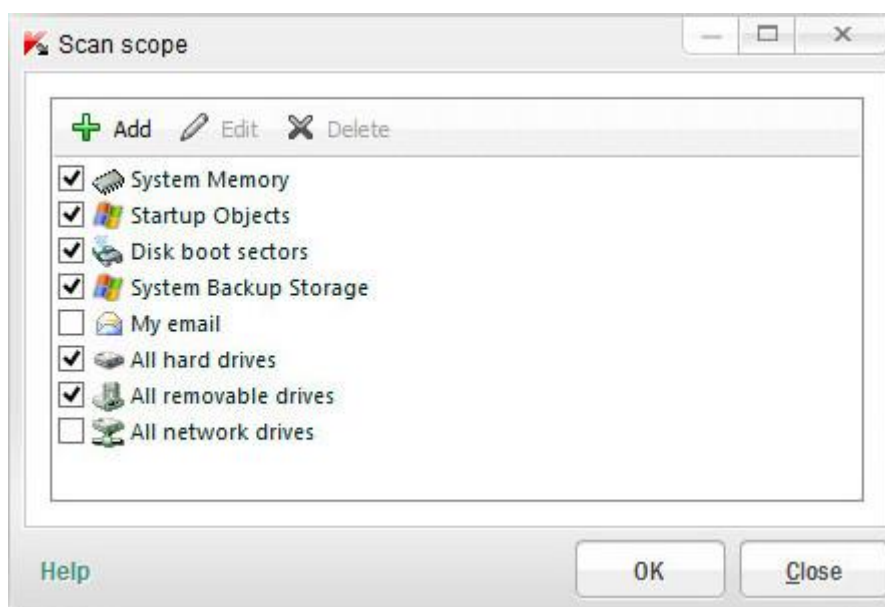
۵- Disinfect objects if possible : پاکسازی کردن فایل در صورت امکان

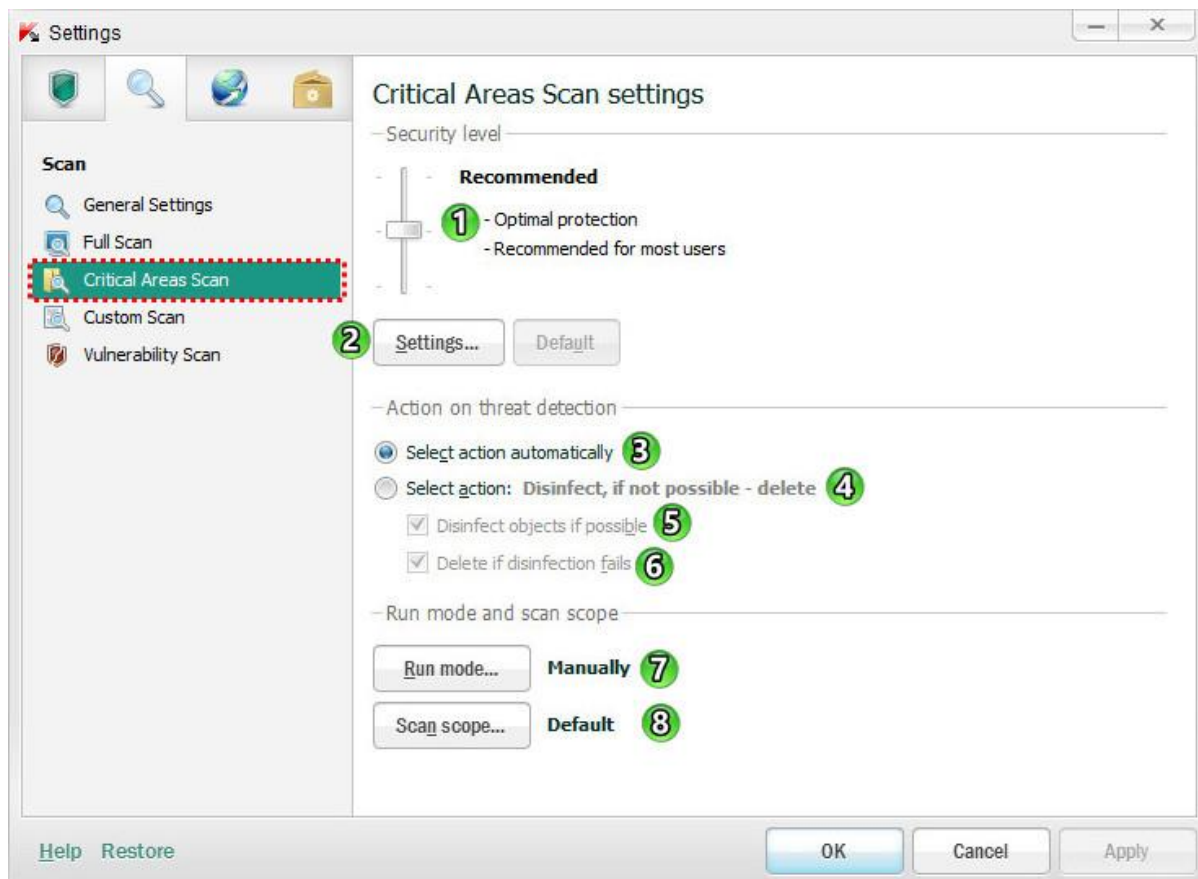
۶- Delete if disinfection fails : حذف کامل در صورت عدم امکان پاکسازی

## :Run mode and scan scope

۷- Run mode : حالت اجرا (بصورت دستی یا برنامه زمانبندی شده برای اسکن)

۸- Scan scope : قسمتهایی که باید اسکن شود.





۱- **Security level (سطح امنیتی):** در بخش تعیین سطح امنیتی، می‌توان سه سطح حفاظت از پیش تعیین شده را برای فایل‌ها و حافظه انتخاب کرد.

**High** (بالا ترین سطح امنیتی)

**Recommended** (سطح امنیتی توصیه شده)

**Low** (کمترین سطح امنیتی)

۲- **Setting (تنظیمات):** با کلیک بر روی این دکمه پنجره تنظیمات باز میشود. (در قسمت **Full Scan** به طور کامل توضیح داده شده است).

**Action on threat detection:** در این بخش اقداماتی که آنتی ویروس باید بر روی **تهدیدات تشخیص داده شده**، **موارد آلوده** یا **احتمالا آلوده** انجام شود را انتخاب میکنیم که شامل دو عملکرد زیر میشود:

۳- **Select action automatically (انتخاب عملکرد اتوماتیک):** پس از تشخیص موارد خطرناک، آنتی ویروس به طور خودکار اعمال توصیه شده توسط متخصصین آزمایشگاه کسپر斯基 را انجام می‌دهد. آنتی ویروس موارد مخرب را پاکسازی یا حذف میکند و اگر برای موارد احتمالا آلوده قادر به پاکسازی نباشد، آنرا نادیده میگیرد. آنتی ویروس قبل از تلاش برای پاکسازی و یا حذف یک مورد آلوده، یک نسخه پشتیبان برای بازسازی پس از پاکسازی تهیه میکند.

۴- **Select action:** انتخاب عملکرد

۵- **Disinfect objects if possible:** پاکسازی کردن فایل در صورت امکان

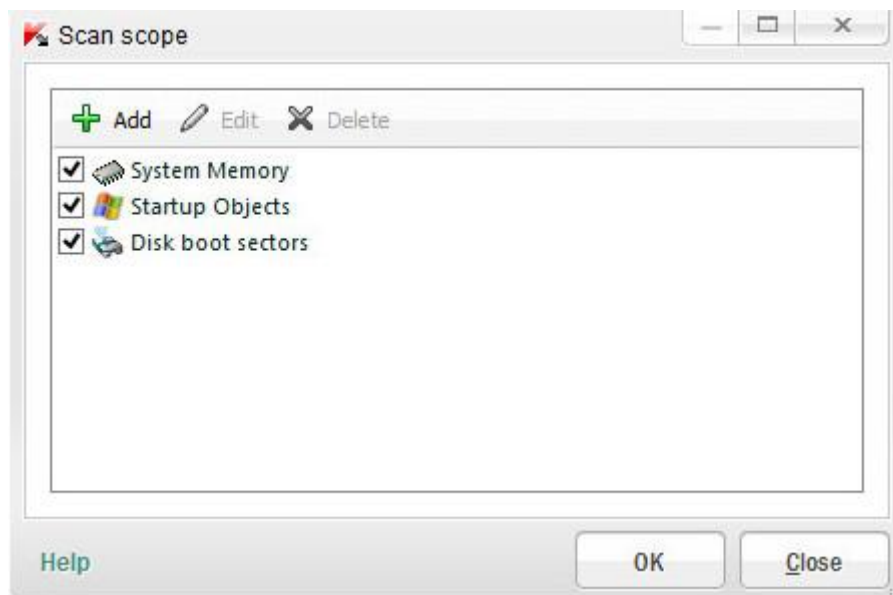
۶- **Delete if disinfection fails** : حذف کامل در صورت عدم امکان پاکسازی

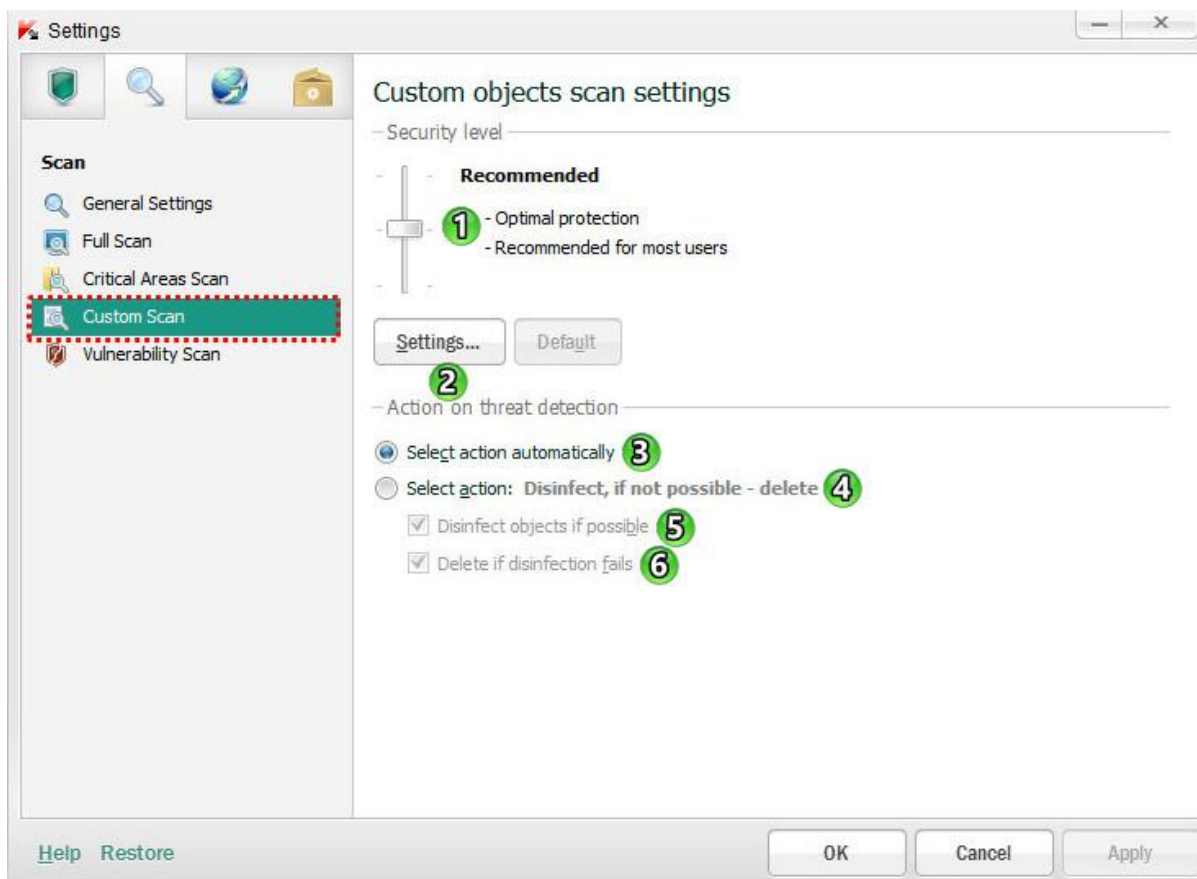
### **Run mode and scan scope**

۷- **Run mode** : حالت اجرا (بصورت دستی یا برنامه زمانبندی شده برای اسکن)

۸- **Scan scope** : قسمتهایی که باید اسکن شود.

در این قسمت فقط میتوان قسمتهای بحرانی (پیش فرض : حافظه سیستم، startup، سکتور های بوت دیسک) را برای اسکن انتخاب نمود.





۱- **Security level (سطح امنیتی)**: در بخش تعیین سطح امنیتی، می توان سه سطح حفاظت از پیش تعیین شده را برای فایل ها و حافظه انتخاب کرد.

**High** (بالاترین سطح امنیتی)

**Recommended** (سطح امنیتی توصیه شده)

**Low** (کمترین سطح امنیتی)

۲- **Setting (تنظیمات)**: با کلیک بر روی این دکمه پنجره تنظیمات باز میشود. ( در قسمت **Full Scan** به طور کامل توضیح داده شده است).

**Action on threat detection**: در این بخش اقداماتی که آنتی ویروس باید بر روی **تهدیدات تشخیص داده شده**، موارد آلوده یا احتمالاً آلوده انجام شود را انتخاب میکنیم که شامل دو عملکرد زیر میشود:

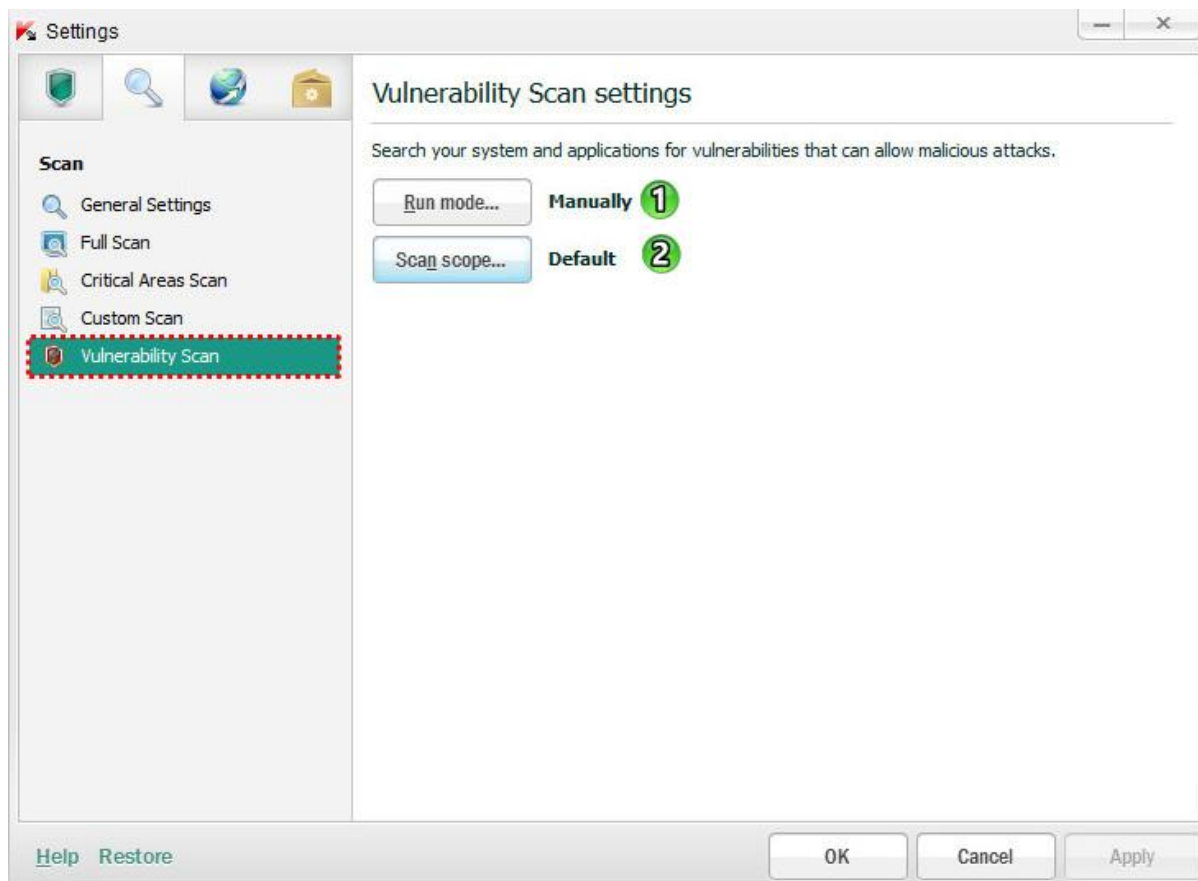
۳- **Select action automatically (انتخاب عملکرد اتوماتیک)**: پس از تشخیص موارد خطرناک، آنتی ویروس به طور خودکار اعمال توصیه شده توسط متخصصین آزمایشگاه کسپرسکی را انجام می دهد. آنتی ویروس موارد مخرب را پاکسازی یا حذف میکند و اگر برای موارد احتمالاً آلوده قادر به پاکسازی نباشد، آنرا نادیده میگیرد. آنتی ویروس قبل از تلاش برای پاکسازی و یا حذف یک مورد آلوده، یک نسخه پشتیبان برای بازسازی پس از پاکسازی تهیه میکند.

۴- **Select action**: انتخاب عملکرد

۵- **Disinfect objects if possible**: پاکسازی کردن فایل در صورت امکان

۶- **Delete if disinfection fails**: حذف کامل در صورت عدم امکان پاکسازی





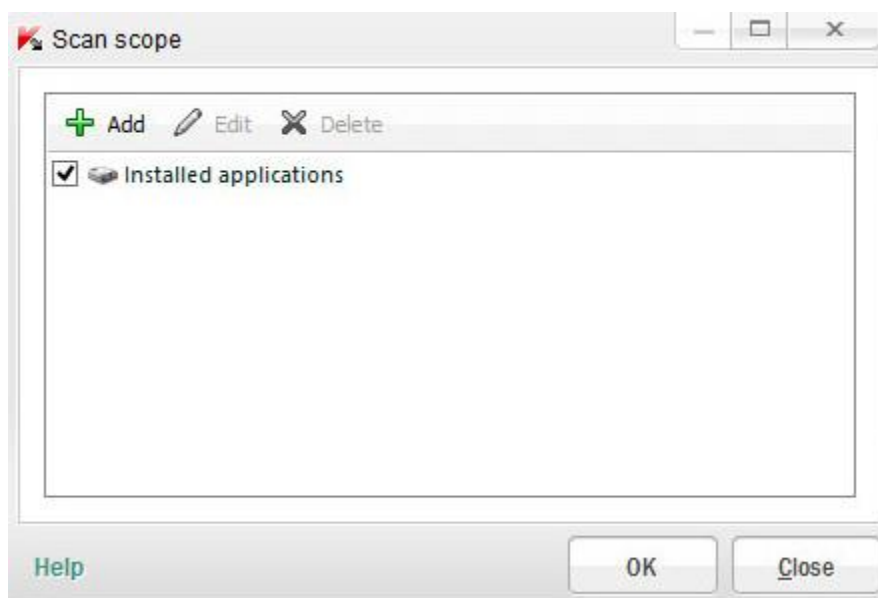
### :Run mode and scan scope

۱- **Run mode**: حالت اجرا (بصورت دستی یا برنامه زمانبندی شده برای اسکن)

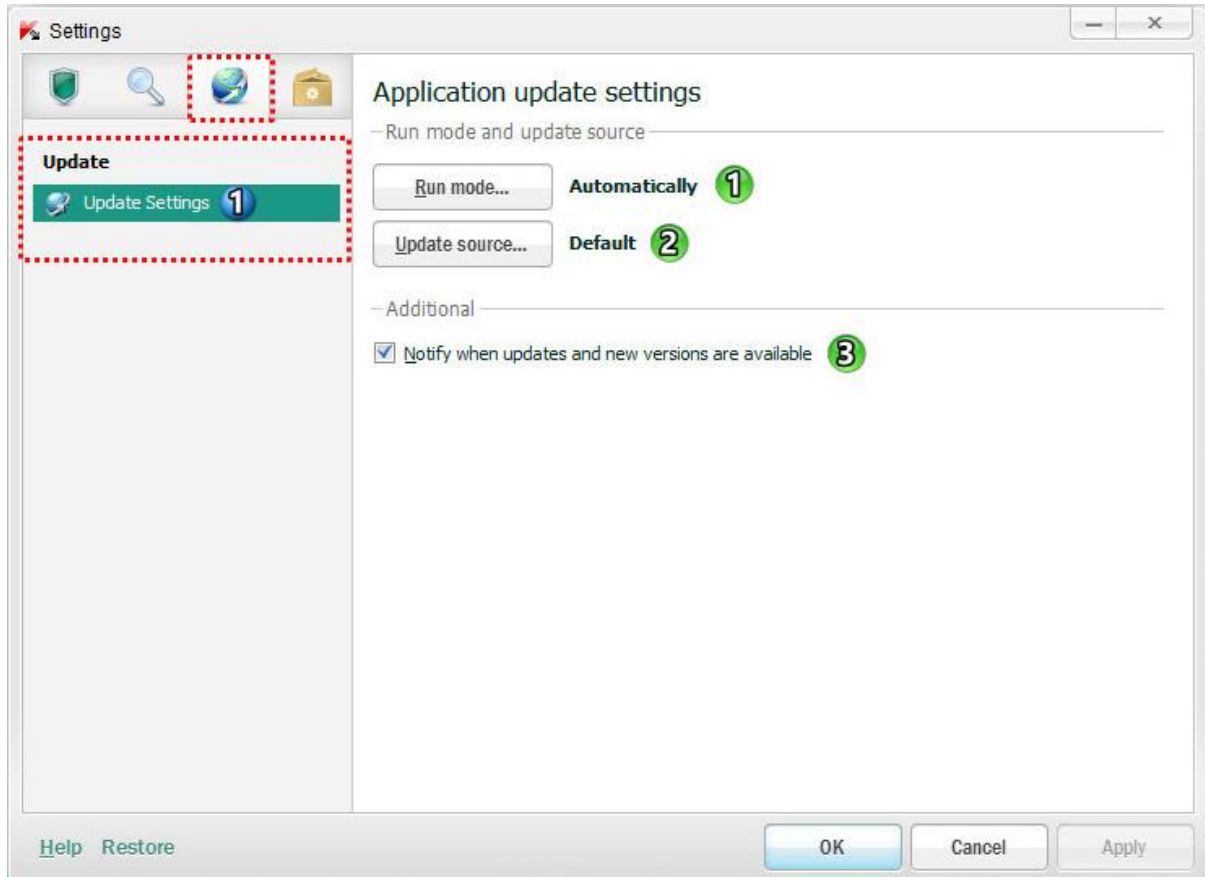
قسمت زمانبندی برای اسکن در **Full Scan** توضیح داده شده است.

۲- **Scan scope**: قسمتهایی که باید اسکن شود.

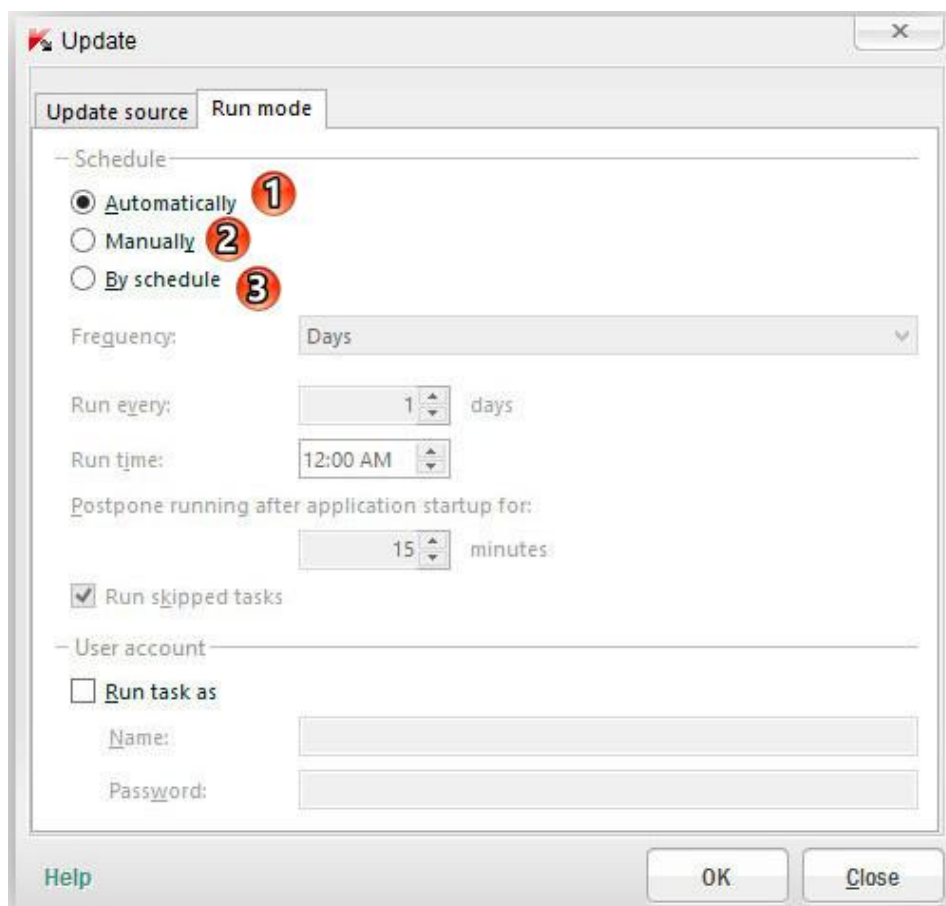
در این قسمت میتوان قسمتهای آسیب پذیر (پیش فرض: نرم افزارهای نصب شده روی کامپیوتر) را برای اسکن انتخاب نمود.



## ۳- سربرگ Update



۱- Run mode: حالت اجرا که شامل سه حالت برای آپدیت نرم افزار میباشد:



۱- **Automatically** : بصورت اتوماتیک

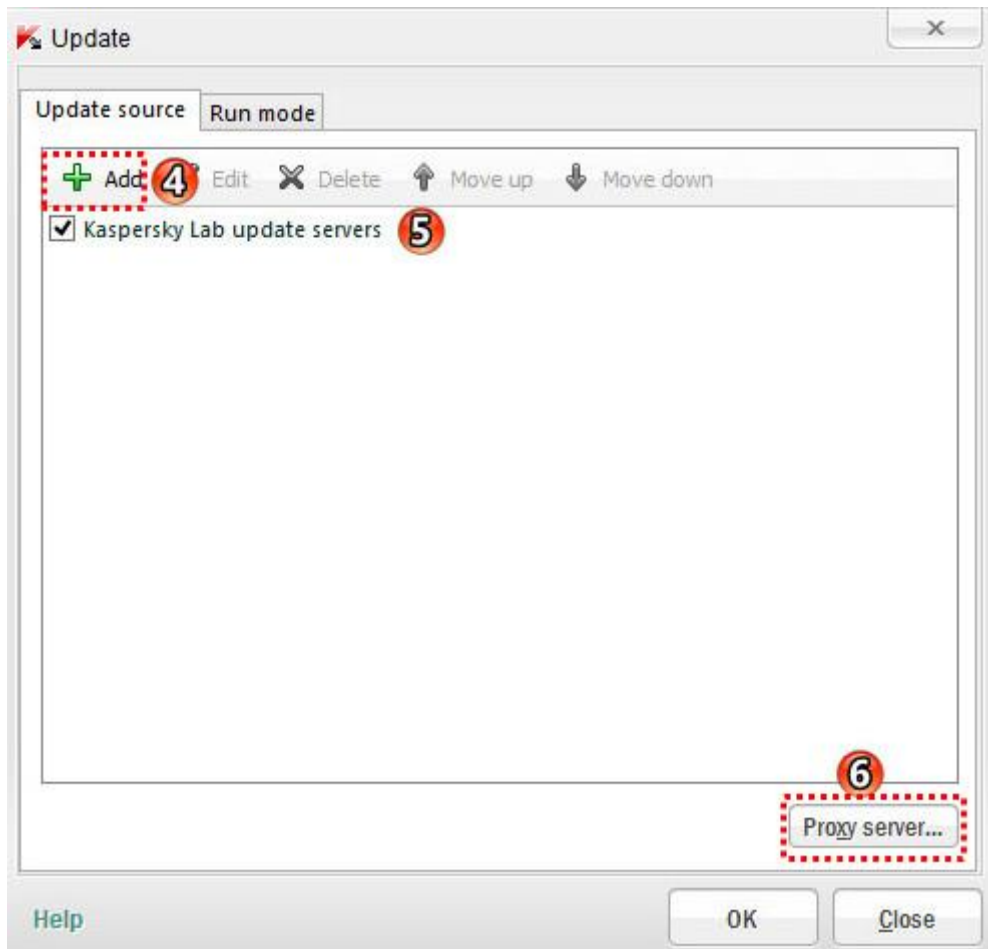
۲- **Manually** : بصورت دستی

۳- **By schedule** : توسط برنامه زمانبندی شده

سایر قسمت‌ها همانند توضیحات قسمت تنظیمات **Full Scan** میباشد. (موارد توضیح داده شده برای آپدیت صدق میکند).

## ۲- **Update source** (برای تعیین کردن سرور آپدیت نرم افزار)

شامل آدرس مکانهای دریافت و نصب بروز رسانی دیتابیس نرم افزار (آدرس های قابل پشتیبانی : سرورهای FTP یا HTTP و شبکه و یا پوشه های محلی)



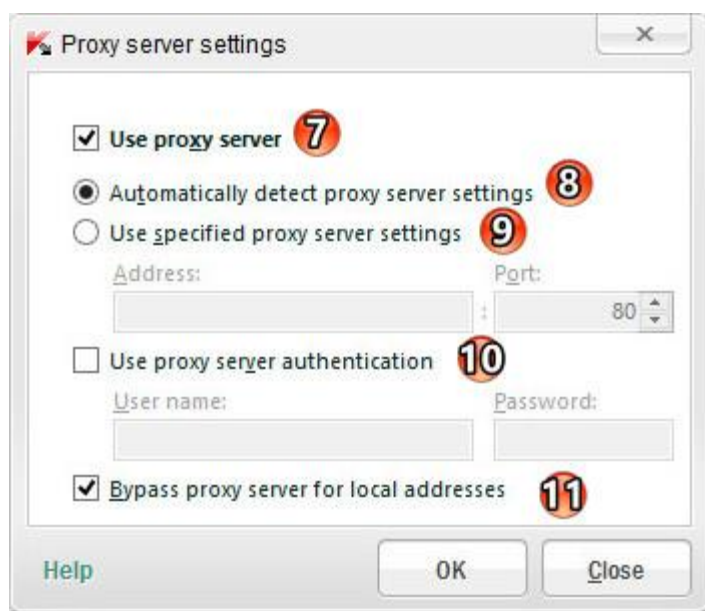
۴- **Add** : اضافه کردن منبع بروزرسانی

۵- **Kaspersky Lab update servers** : سرور آپدیت اصلی کسپرسکی

**نکته** : در صورت داشتن چند سرور در لیست ، تقدم با سروری میباشد که در بالای لیست قرار دارد. (بوسیله **Move**

**up** و **Move down**)

۶- Proxy server : در این قسمت می توان تنظیمات دسترسی به اینترنت از طریق سرور پروکسی را پیکربندی کرد.



۷- Use proxy server : فعال کردن استفاده از سرور پروکسی

۸- Automatically detect the proxy server settings : تشخیص خودکار تنظیمات سرور پروکسی

۹- Use specified proxy server settings : استفاده از تنظیمات سرور پروکسی مشخص شده

در این قسمت باید آدرس سرور و پورت وارد شود.

۱۰- Use proxy server authentication : در صورتی که سرور مورد نظر دارای یوزر و پسورد باشد با فعال کردن این

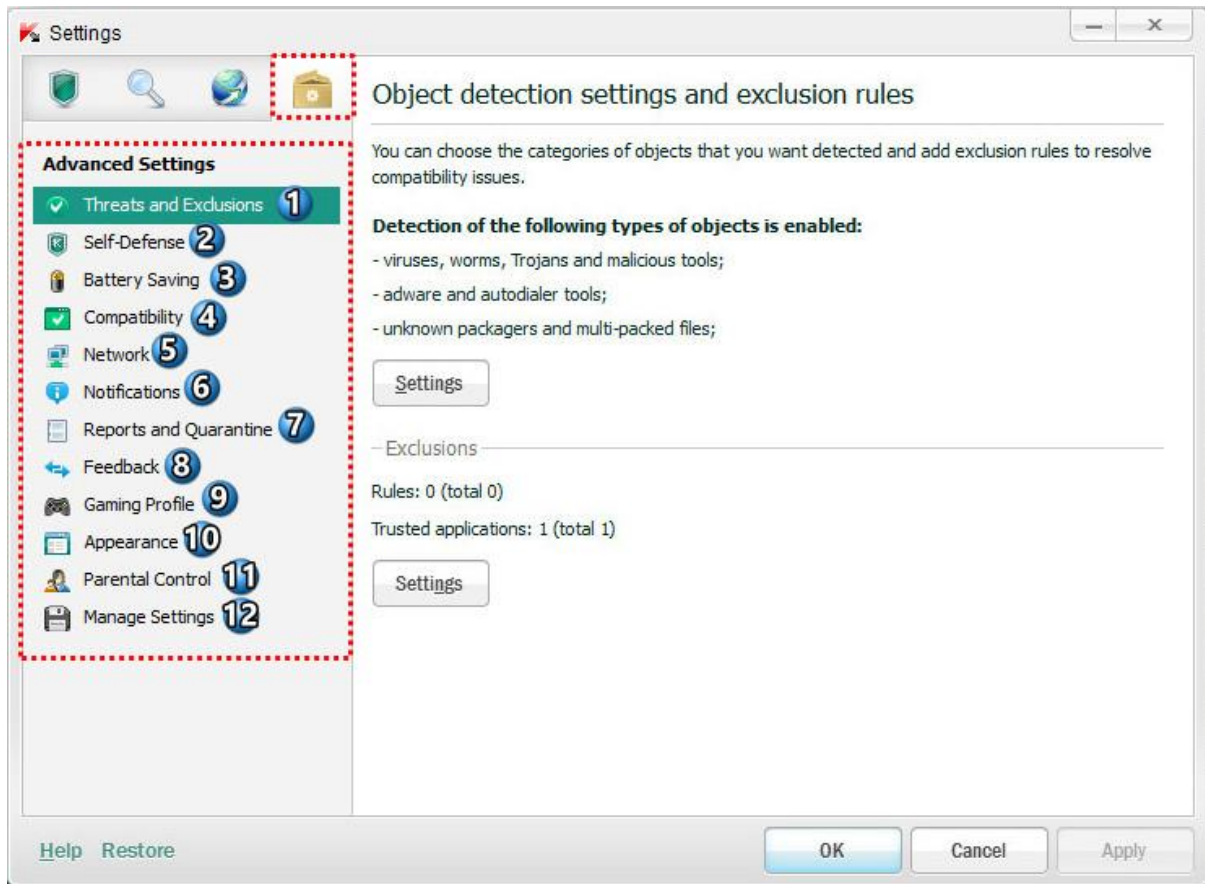
قسمت میتوان یوزر و پسورد را وارد کرد.

۱۱- Bypass proxy server for local addresses: عدم استفاده از سرور پروکسی زمانیکه بروز رسانی از پوشه های

محلی یا شبکه انجام میگردد.

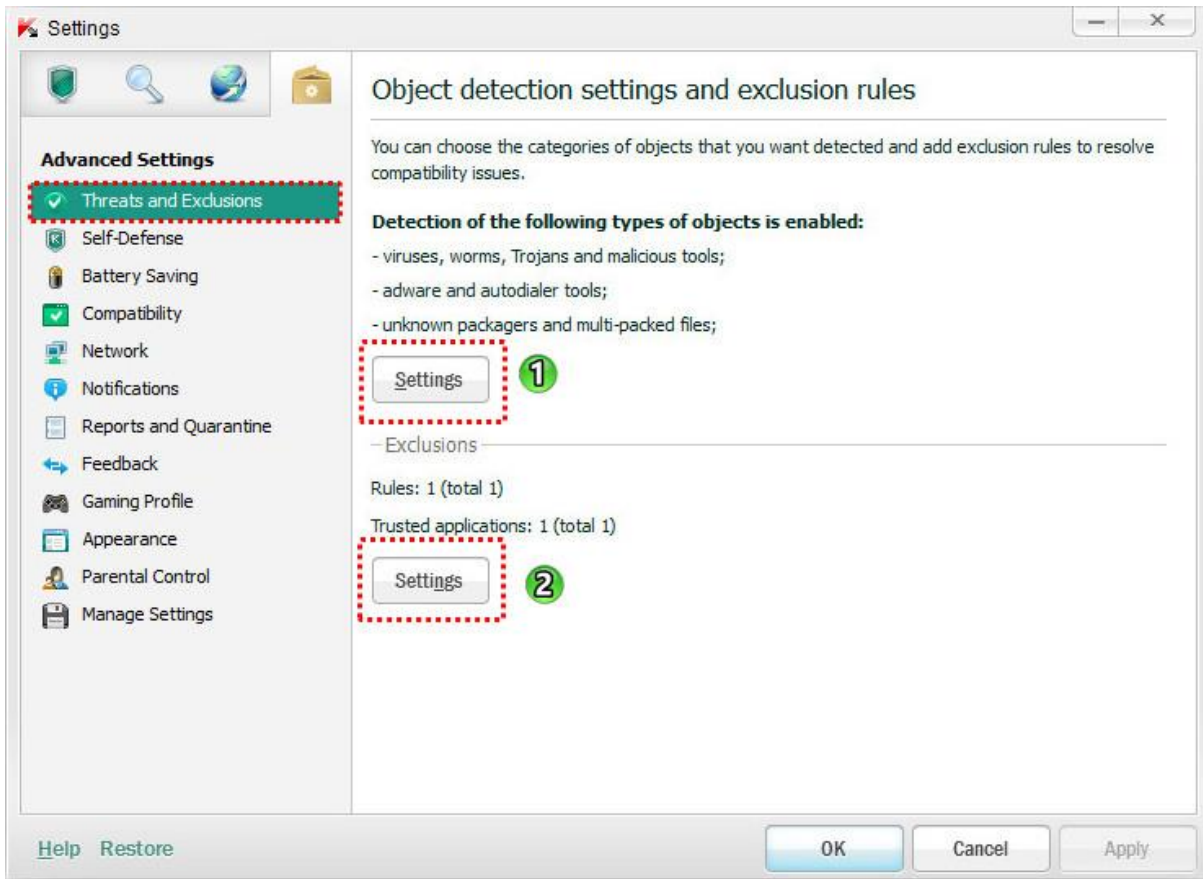
۳- Notify when updates and new versions are available : اطلاع رسانی هنگام بروز رسانی ها و نسخه

های جدید نرم افزار

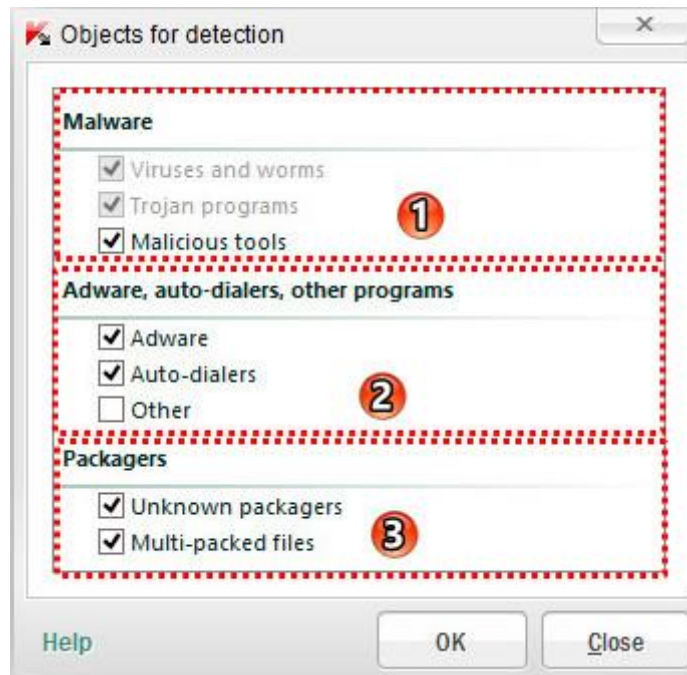




## ۱- تهدیدات و استثنائات (Threats and Exclusions)



۱- **Setting**: با کلیک کردن روی این دکمه پنجره ای باز می شود که مواردی که باید تشخیص داده شود را میتوان تعیین کرد.



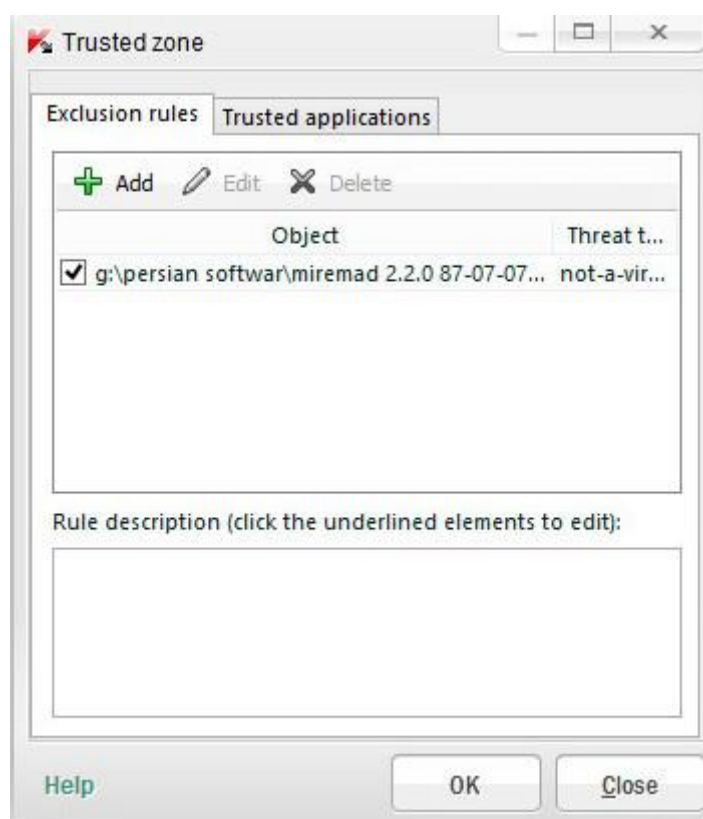
۱- در این بخش نوع بدافزاری (ویروس ها و کرمها ، تروجان ها ، ابزارهای مخرب) که کسپرسکی باید شناسایی و بلوکه کند ، را می توان انتخاب کرد.

۲- در این بخش می توان تعیین کرد که ابزارهای تبلیغاتی مزاحم ، Auto-dialer ها و دیگر تهدیدات (برای مثال، سایت های چت اینترنتی ، دانلود برنامه های کاربردی، نظارت بر برنامه های کاربردی، برنامه های مدیریت از راه دور، و دیگر برنامه های از این قبلی) باید شناسایی و بلوکه شود.

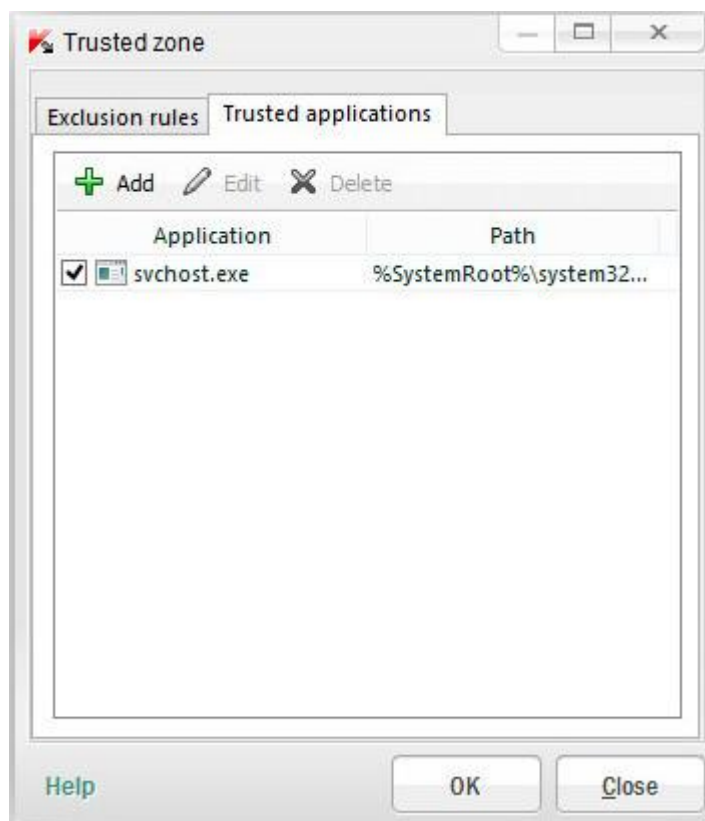
۳- در این بخش می توان نظارت بر تهدیداتِ فایل‌های فشرده ( پکیج های ناشناخته ، فایل‌های چند بار فشرده شده ) را فعال کرد.

۲- **Setting** : با کلیک کردن روی این دکمه پنجره ای باز می شود که میتوان در این قسمت قوانین مستثناء و برنامه های مورد اعتماد را تعیین کرد.

### سربرگ Exclusion rule



در این قسمت میتوان از اسکن یک پوشه یا برنامه و... توسط آنتی ویروس جلوگیری کرد.  
برای اضافه کردن یک پوشه یا برنامه باید روی Add کلیک نموده و پس از آن مسیر پوشه یا برنامه را مشخص نمود.

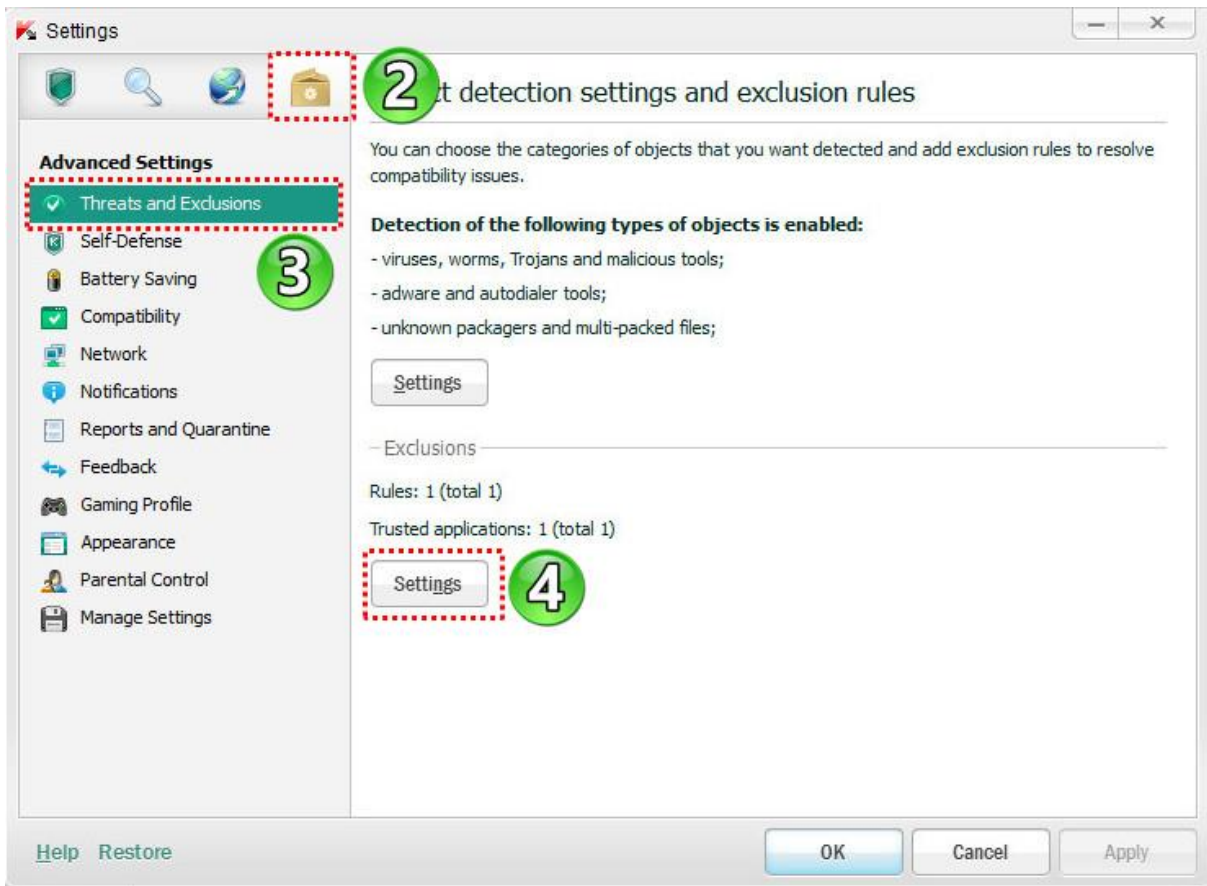


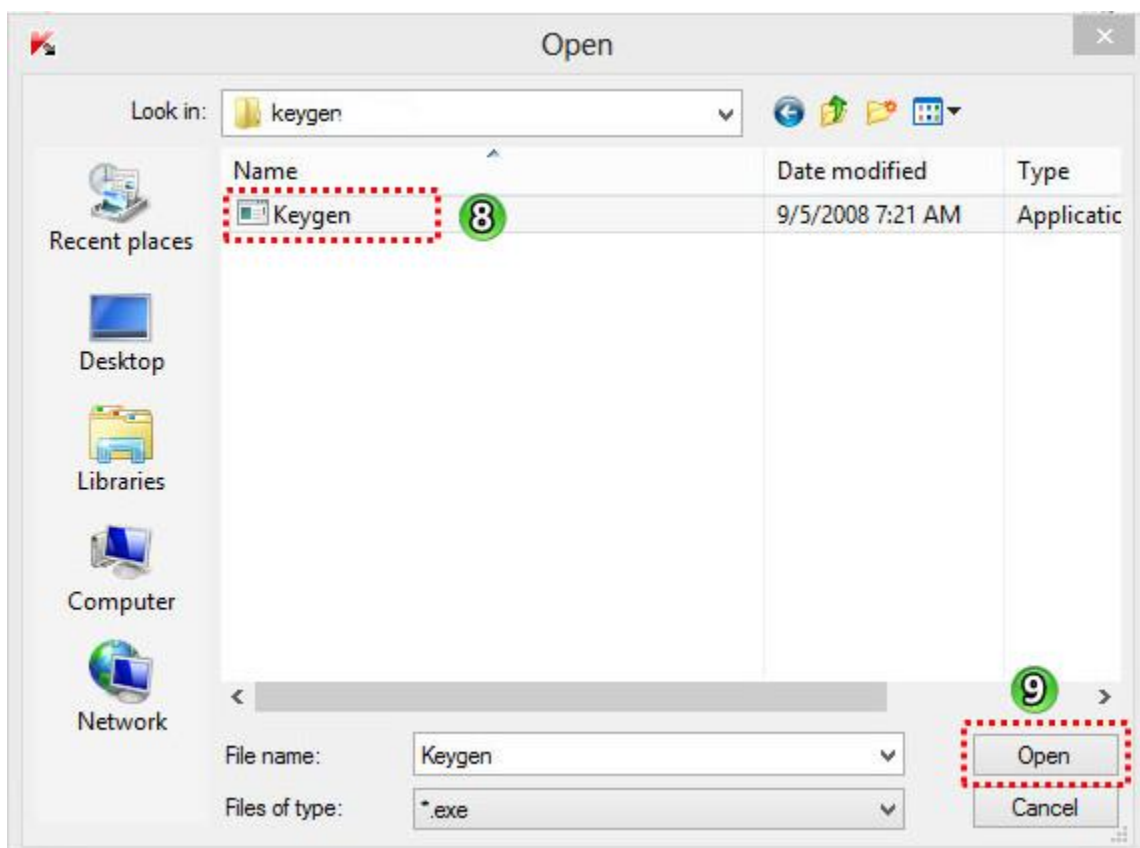
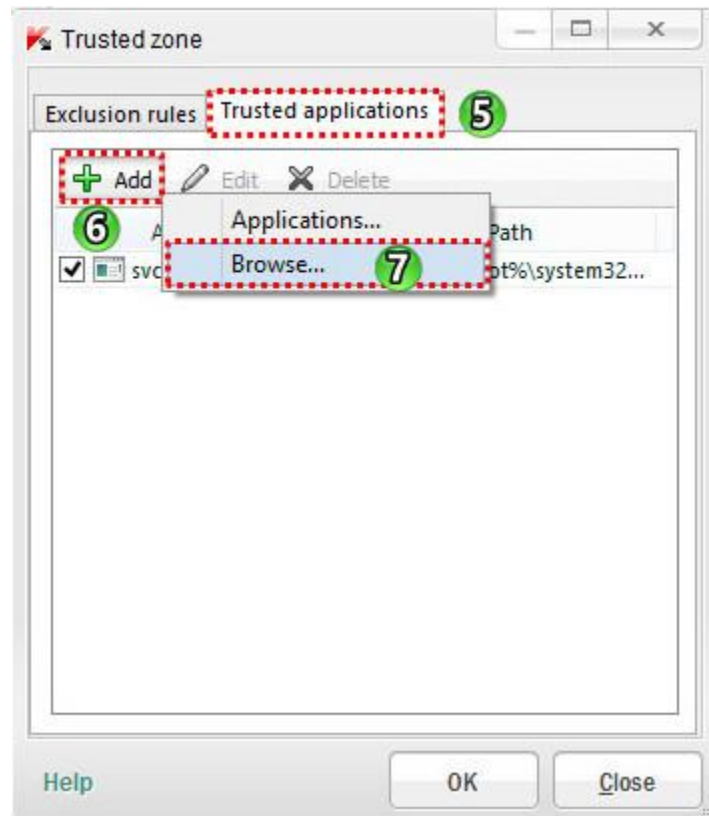
این قسمت شامل برنامه های مورد اعتمادی میشود که قصد جلوگیری از اسکن شدن توسط آنتی ویروس را داریم. به طور پیش فرض، پروسه svchost.exe در لیست برنامه های مورد اعتماد قرار دارد.

**کاربرد این قسمت رو با یک مثال توضیح بیشتر میدم:**

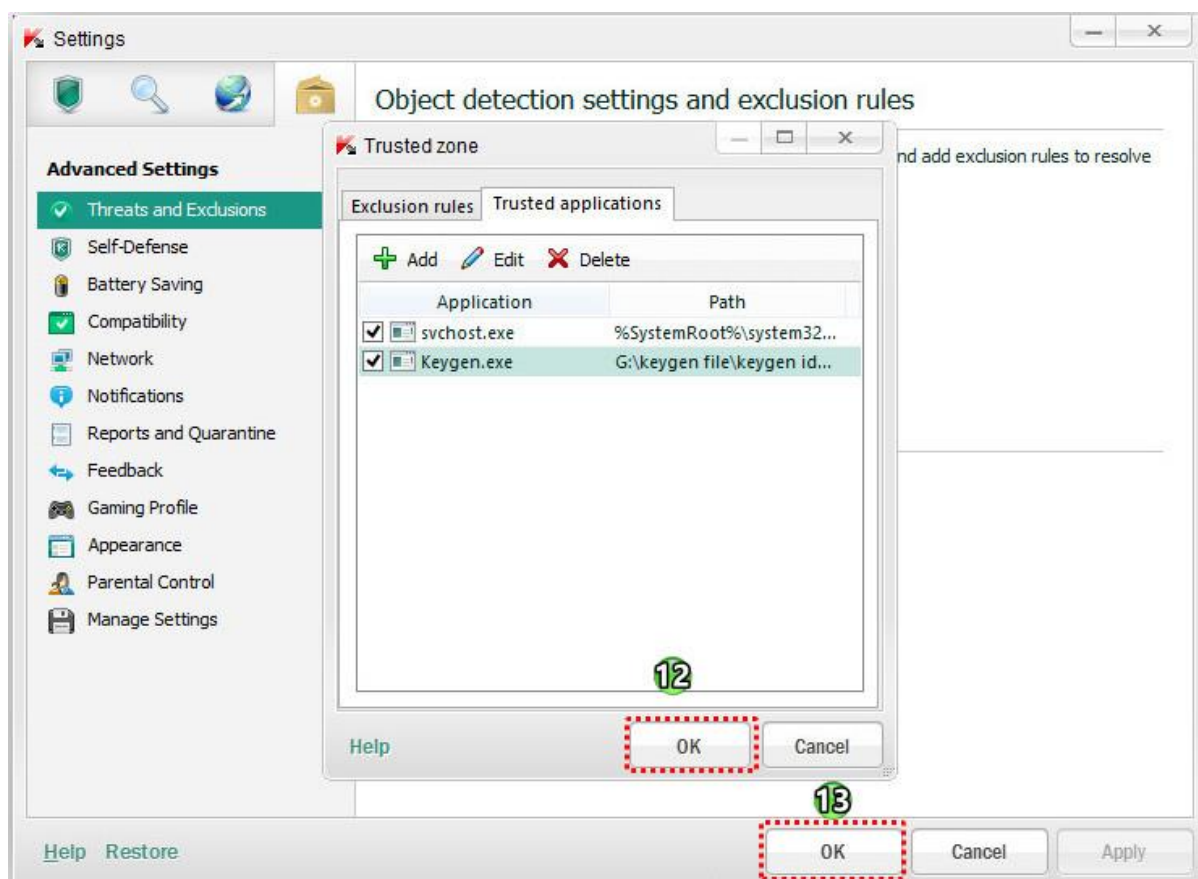
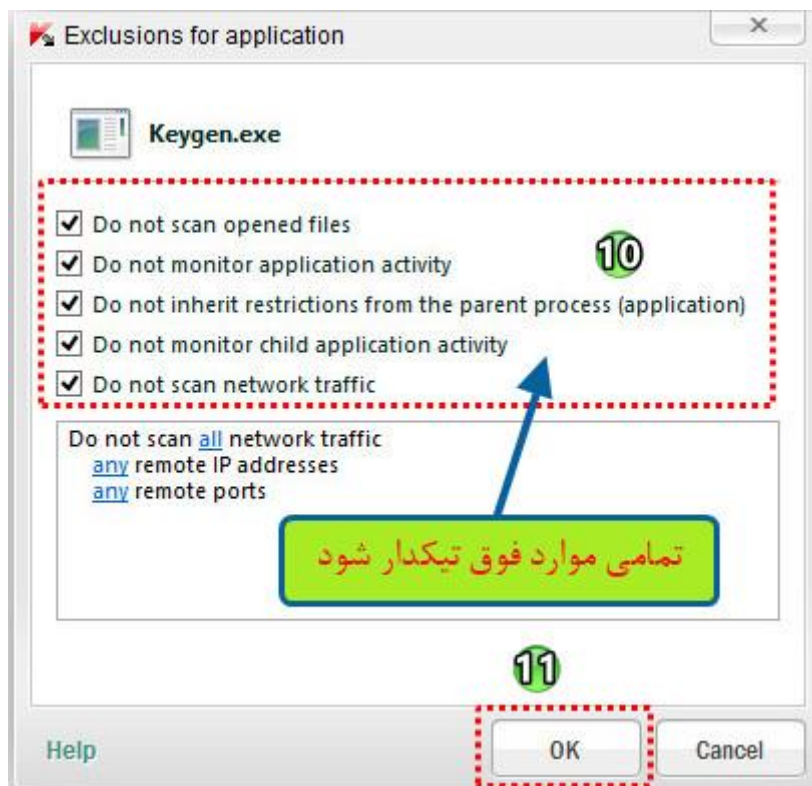
## **اعتماد سازی یک فایل به Kaspersky Internet Security 2013**

آنتی ویروسها معمولا با کرک و پچ ها میانه خوبی ندارند به همین جهت اقدام به پاکسازی و حذف آنها میکنند. برای معرفی کردن یک فایل به عنوان فایل سالم باید مراحل زیر طی شود. بعد از اینکه آنتی ویروس فایل را قرنطینه کرد اولین قدم غیرفعال کردن موقتی آنتی ویروس و بازگشت فایل (Rstore) می باشد. مراحل بعدی را طبق اسکرین شاتها عمل کنید.

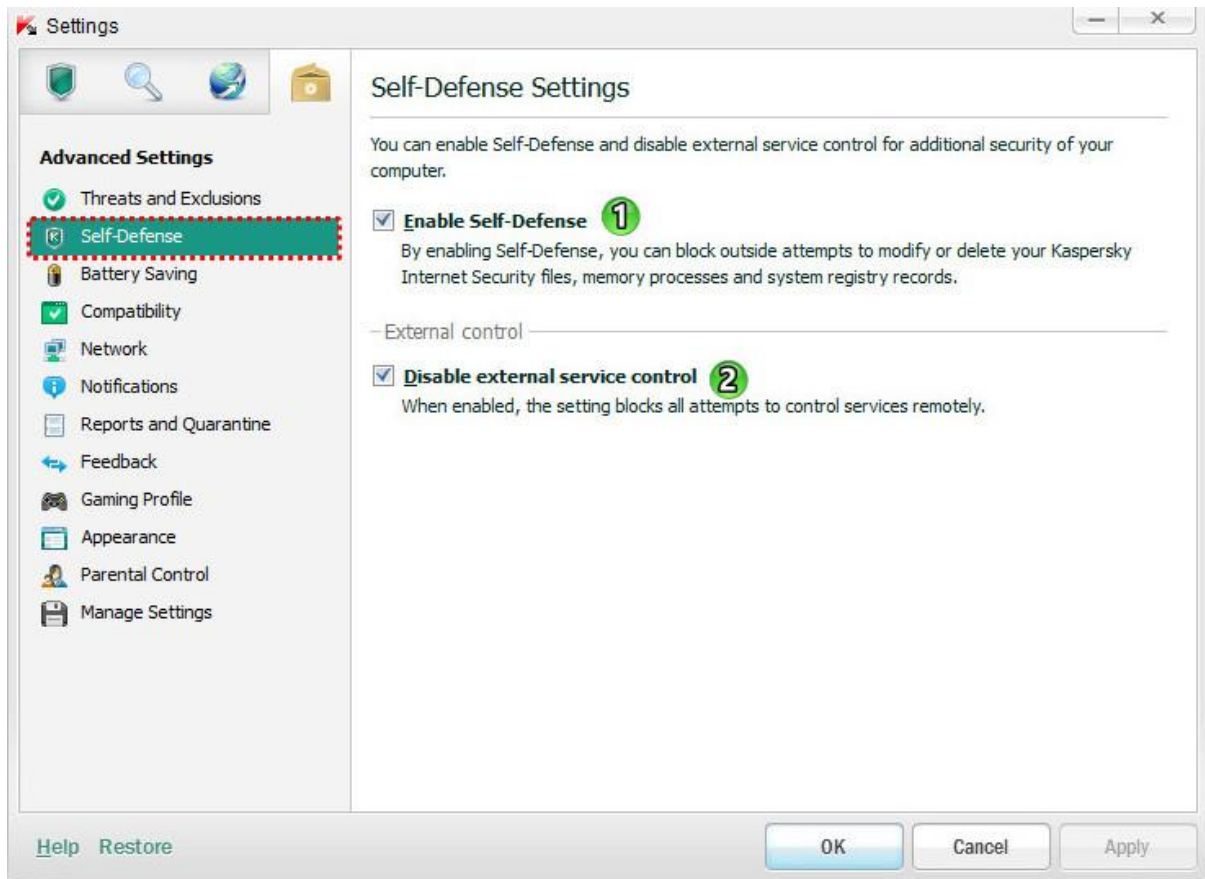






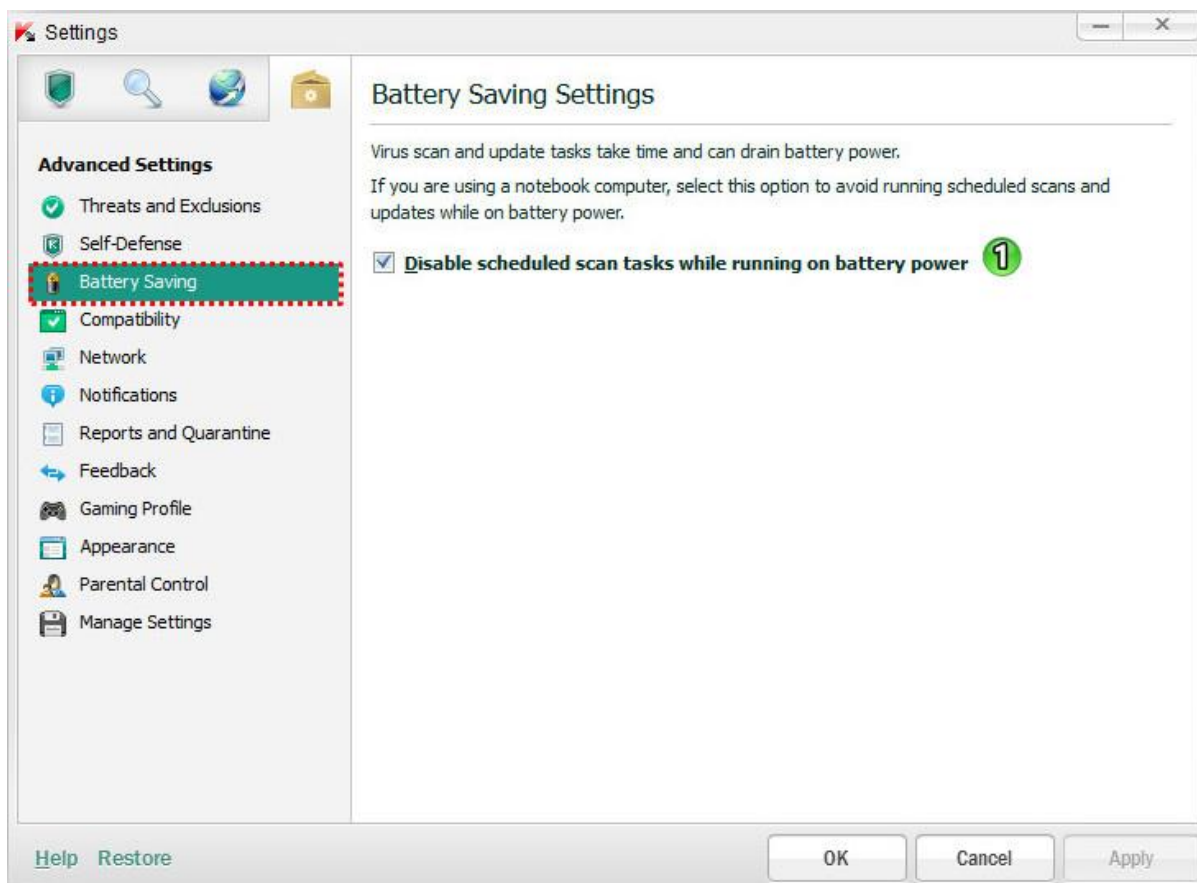


از این به بعد دیگه فایل keygen.exe اسکن نمیشه.



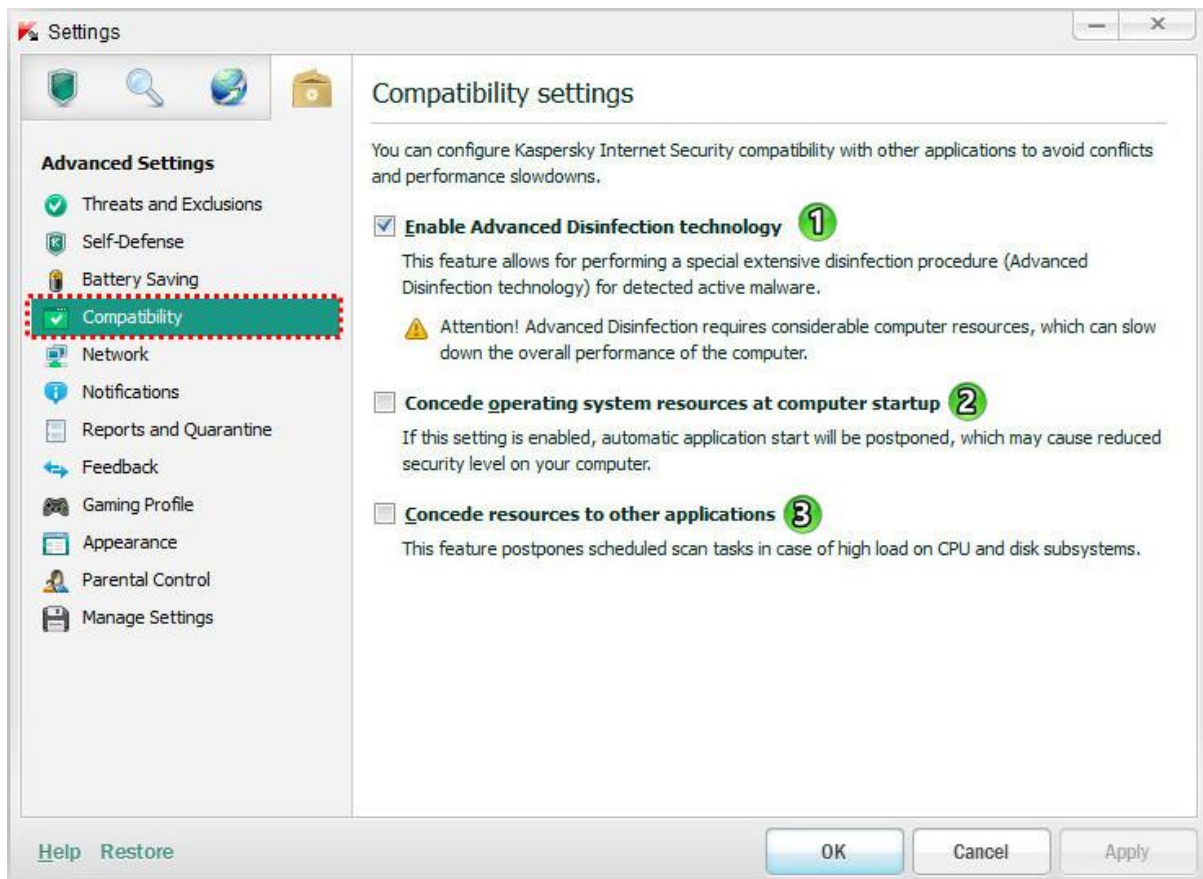
۱- **Enable Self-Defense**: با تیکدار بودن این قسمت ، مکانیزم های حفاظتی Kaspersky Internet Security در برابر تغییر و یا حذف فایل های خود را از روی هارد دیسک، پروسه های موجود در RAM و سوابق رجیستری سیستم ، فعال میشود.

۲- **Disable external service control**: با تیکدار بودن این قسمت ، تمامی تلاشهای برای کنترل از راه دور نرم افزار مسدود میشود.



**: Disable scheduled scan tasks while running on battery power -1**

غیر فعال کردن اسکن های برنامه ریزی شده و آپدیت ، زمانی که لپ تاپ با باتری کار میکند.



### ۱- Enable Advanced Disinfection technology: فعال کردن تکنولوژی پاکسازی پیشرفته

با تیکدار بودن این قسمت ، هنگامی که یک فعالیت مخرب در سیستم تشخیص داده شود، یک روش خاص پاکسازی برای خنثی سازی و حذف تهدید ارائه میشود. پس از اتمام کار، سیستم نیاز به راه اندازی مجدد دارد.

**توجه:** فن آوری پاکسازی پیشرفته نیاز به منابع قابل توجهی از کامپیوتر دارد که ممکن است عملکرد کامپیوتر را تحت تاثیر قرار دهد.

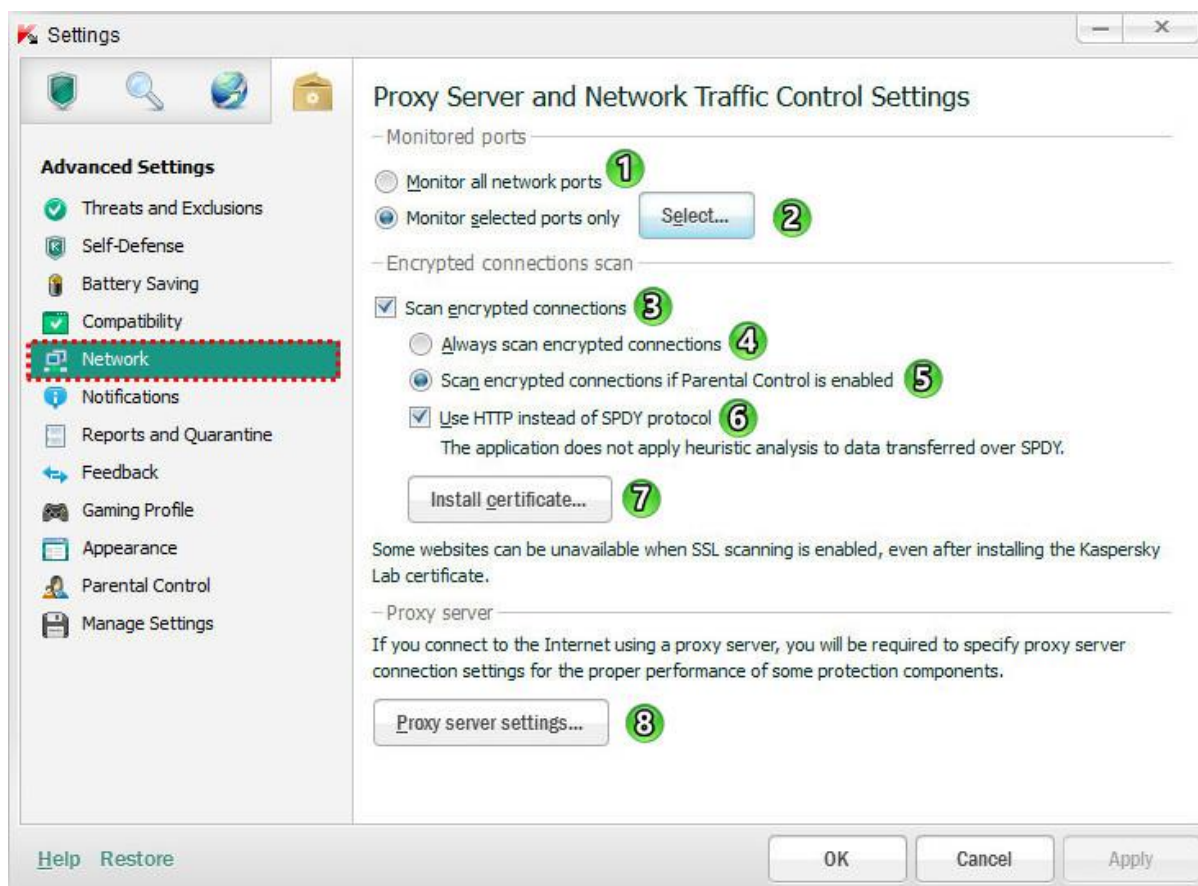
### ۲- Concede resources to the operating system when booting the computer: واگذاری منابع به

سیستم عامل در هنگام بوت شدن کامپیوتر (اجرای آنتی ویروس زمان بوت سیستم عامل با تاخیر انجام میگردد که کاربرد آن برای بوت شدن سریع تر سیستم عامل است).

**توجه:** کارشناسان کسپرسکی توصیه کرده اند که این قسمت فعال نشود ، زیرا اتصالات شبکه ای که تازه ایجاد شده ، (چون آنتی ویروس هنوز فعال نشده ) اسکن نمیشود.

### ۳- Concede resources to other applications: واگذاری منابع سیستم به برنامه های کاربردی دیگر

زمان اسکن توسط آنتی ویروس ، ممکن است حجم کار بر روی CPU و disk subsystems ، افزایش یابد و عملکرد برنامه های دیگر را تحت تاثیر قرار دهد. اگر چنین وضعیتی رخ می دهد، آنتی ویروس می تواند در پروسه اسکن مکث ایجاد کند و منابع سیستم را برای برنامه های کاربردی آزاد کند.



۱- **Monitor all network ports**: نظارت بر تمام پورت های شبکه

در این حالت ، کامپوننت های حفاظتی از قبیل Web Anti-Virus، Mail Anti-Virus، Anti-Spam بر اطلاعات منتقل شده از طریق همه پورت های باز کامپیوتر شما نظارت میکنند.

۲- **Monitor selected ports only**: فقط نظارت بر پورت های انتخاب شده

با کلیک بر روی دکمه Select می توان پورت و برنامه های مورد نظر را انتخاب کرد.

۳- **scan encrypted connections**: اسکن اتصالات رمزگذاری شده

۴- **Always scan encrypted connections**: اسکن همیشگی اتصالات رمزگذاری شده ( اسکن اتصالات رمزگذاری

شده توسط پروتکل SSL)

۵- **Scan encrypted connections if Parental Control is enabled**: اسکن اتصالات رمزگذاری شده در

صورتی که کنترل والدین فعال باشد.

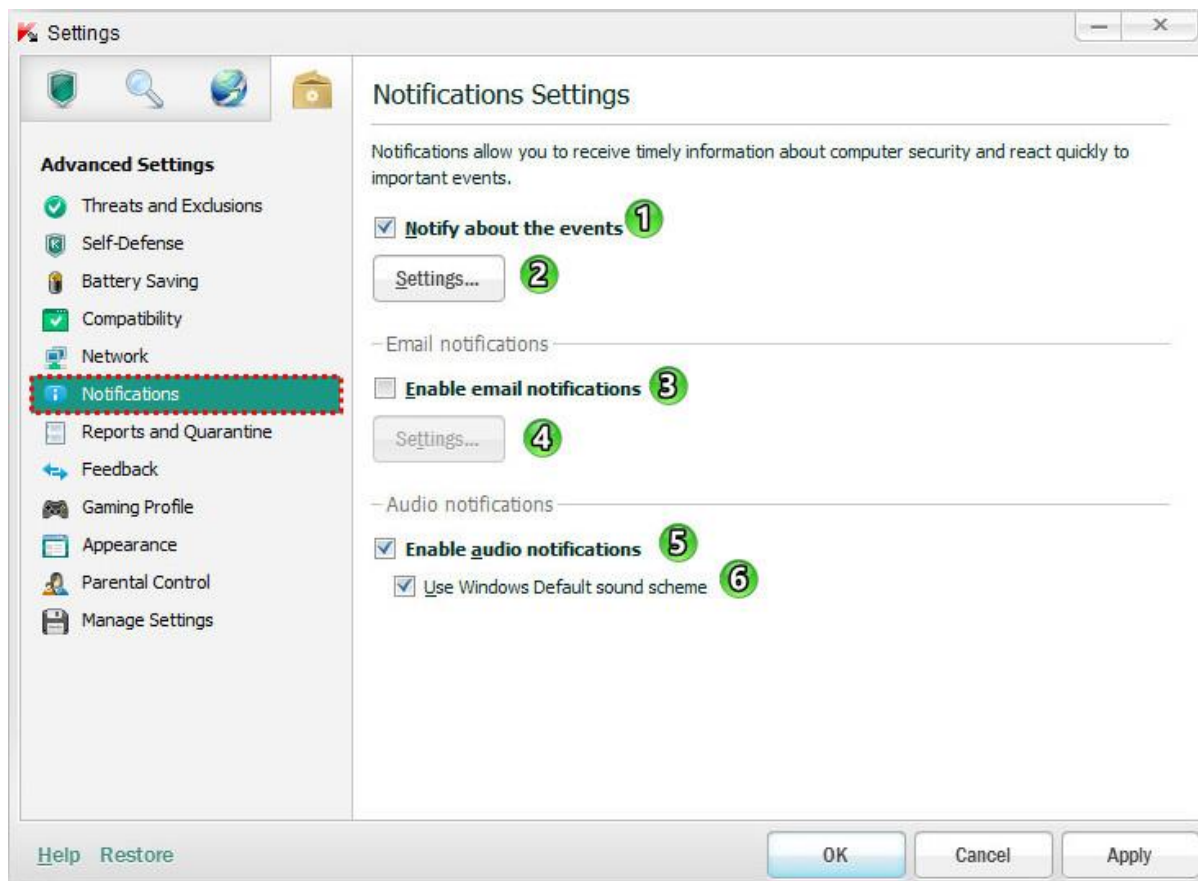
۶- **Use HTTP instead of SPDY**: استفاده از HTTP به جای SPDY

۷- **Install Certificate**: در این قسمت می توان گواهینامه Kaspersky Lab را برای حفاظت از اتصالات

(SSL/TLS) نصب نمود .

۸- **Proxy server settings**: تنظیمات سرور پروکسی (قبلا توضیح داده شده است)





۱- **notify about events** : اطلاع در مورد وقایع

۲- **Settings** : تنظیمات برای وقایعی که باید نمایش داده شود که شامل چهار نوع زیر میشود:

**Critical events** : رویدادهای مهم (به عنوان مثال، خرابی دیتابیس نرم افزار یا تمام شدن لایسنس نرم افزار )

**Functional failure** : شکست های عملکردی (به عنوان مثال، آپدیت غیر موفق)

**Important events** : رویدادهای مهم (به عنوان مثال، غیر فعال شدن حفاظت )

**Other events** : رویدادهای دیگر (به عنوان مثال ، کامل شدن آپدیت )

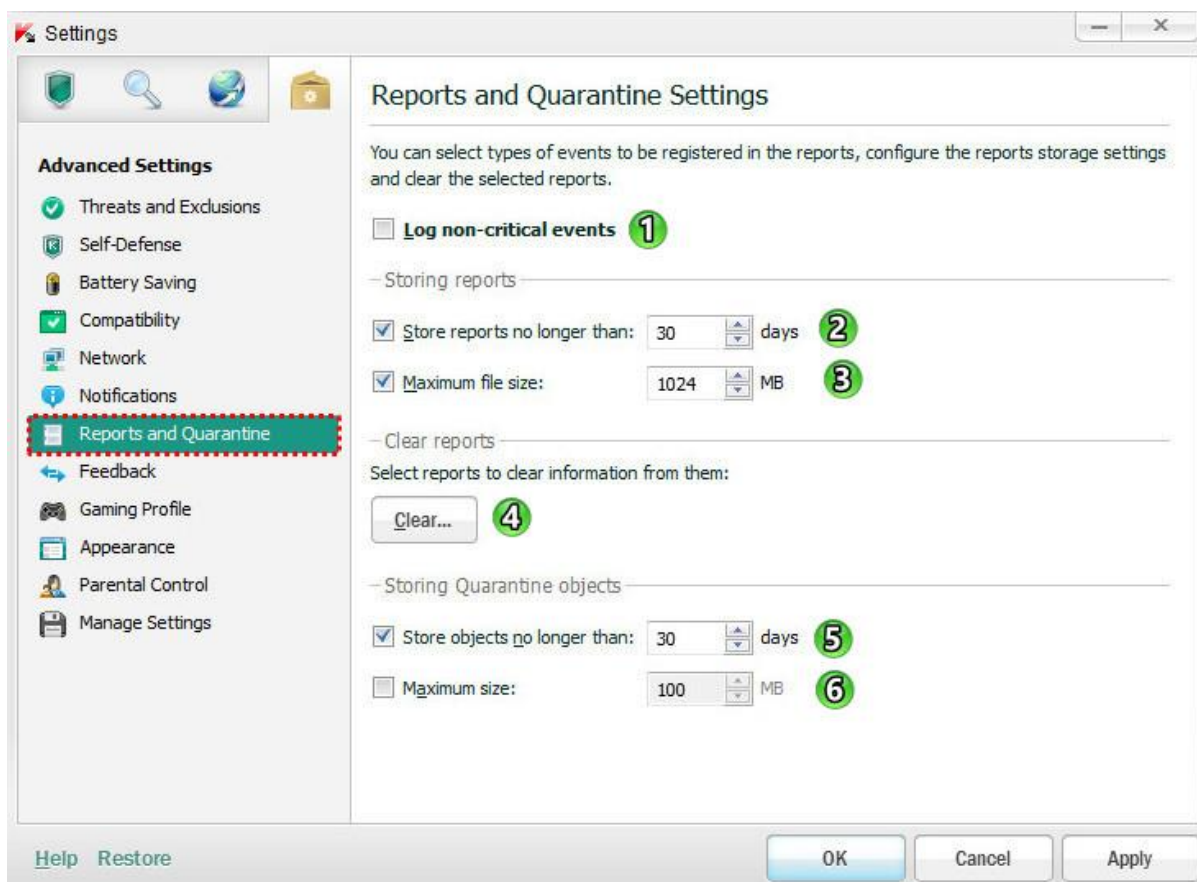
۳- **Enable email notifications** : فعال کردن اطلاع رسانی با ایمیل

۴- **Settings** : ورود به قسمت تنظیمات ایمیل (برای وارد کردن ایمیل و ... جهت اطلاع رسانی)

۵- **Enable audio notifications** : فعال کردن اعلان های صوتی (به طور پیش فرض، همه اطلاعیه ها توسط یک

سیگنال صدا همراه است).

۶- **Use Windows Default sound scheme** : استفاده از طرح صداهای استاندارد (پیش فرض) ویندوز



۱- **Log non-critical events**: گزارش وقایع غیر حساس

**Storing reports**: ذخیره سازی گزارشات

۲- **Store reports no longer than**: حداکثر مدت برای ذخیره سازی گزارشات (بر حسب روز) را می توان تعیین کرد.

۳- **Maximum file size**: تعیین حداکثر اندازه فایل گزارشات (بر حسب مگابایت)

۴- **Clear reports**: حذف گزارشات (با کلیک بر روی این دکمه می توان نوع گزارشاتی که باید پاک شود را تعیین کرد)

**Storing Quarantine objects**: اهداف ذخیره شده در قرنطینه

۵- **Store objects no longer than**: تعیین حداکثر مدت زمان ذخیره سازی اهداف (بر حسب روز) در قرنطینه

۶- **Maximum size**: تعیین حداکثر حجم ذخیره سازی داده ها در قرنطینه (بر حسب مگابایت)



۱- I agree to participate in Kaspersky Security Network : موافقت برای شرکت در شبکه امنیت

کسپرسکی (KSN)

Kaspersky Security Network (KSN) توسط لابراتوار کسپرسکی برای کمک به تسریع شناسایی انواع تهدیدها و منابع

تهدیدهای جدید و همچنین توسعه روش های خنثی کردن آنها ، ارائه شده است.



### ۱- Use Gaming Profile

این قسمت برای بازی هایی که در حالت نمایش کامل (full-screen mode) اجرا میشوند، طراحی شده است. با تیکدار بودن این قسمت، تنظیمات قسمت Profile options هنگام سوییچ به حالت فول اسکرین بازیها در آنتی ویروس اعمال میشود و هنگام خروج از فول اسکرین بازیها و بازگشت به حالت عادی، تنظیمات قبلی اعمال میشود.

### Profile options

۲- **Select action on threat detect automatically**: انتخاب عملکرد خودکار هنگام تشخیص یک تهدید

۳- **Do not run updates**: عدم آپدیت دیتابیس و نرم افزار

۴- **Do not run scheduled scan tasks**: عدم اجرای وظایف اسکن برنامه ریزی شده

۵- **Pause manually run scan tasks**: مکث دستی وظایف در حال اجرا

تنظیمات نمایش Kaspersky Internet Security



۱- **Interface Language** : انتخاب زبان رابط کاربری

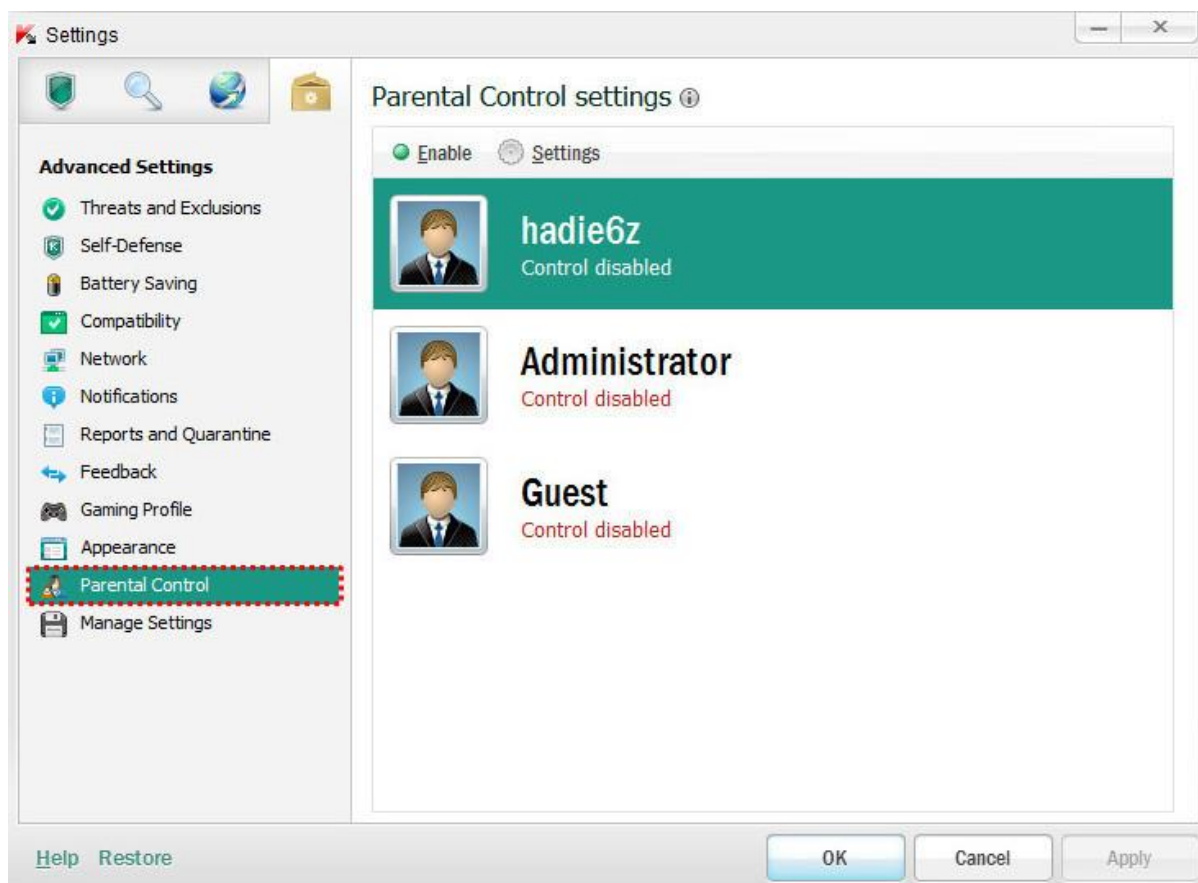
۲- **Animate taskbar icon when executing tasks** : نمایش آیکون کسپرسکی در نوار وظیفه (taskbar) هنگام

اجرای وظایف

۳- **Enable semi-transparent notification windows** : پنجره های اطلاع رسانی نیمه شفاف

۴- **Enable news notifications** : نمایش اخبار و اطلاع رسانی های لابراتوار کسپرسکی





این قسمت همراه تنظیمات به طور کامل در قسمتهای قبلی توضیح داده شده است.



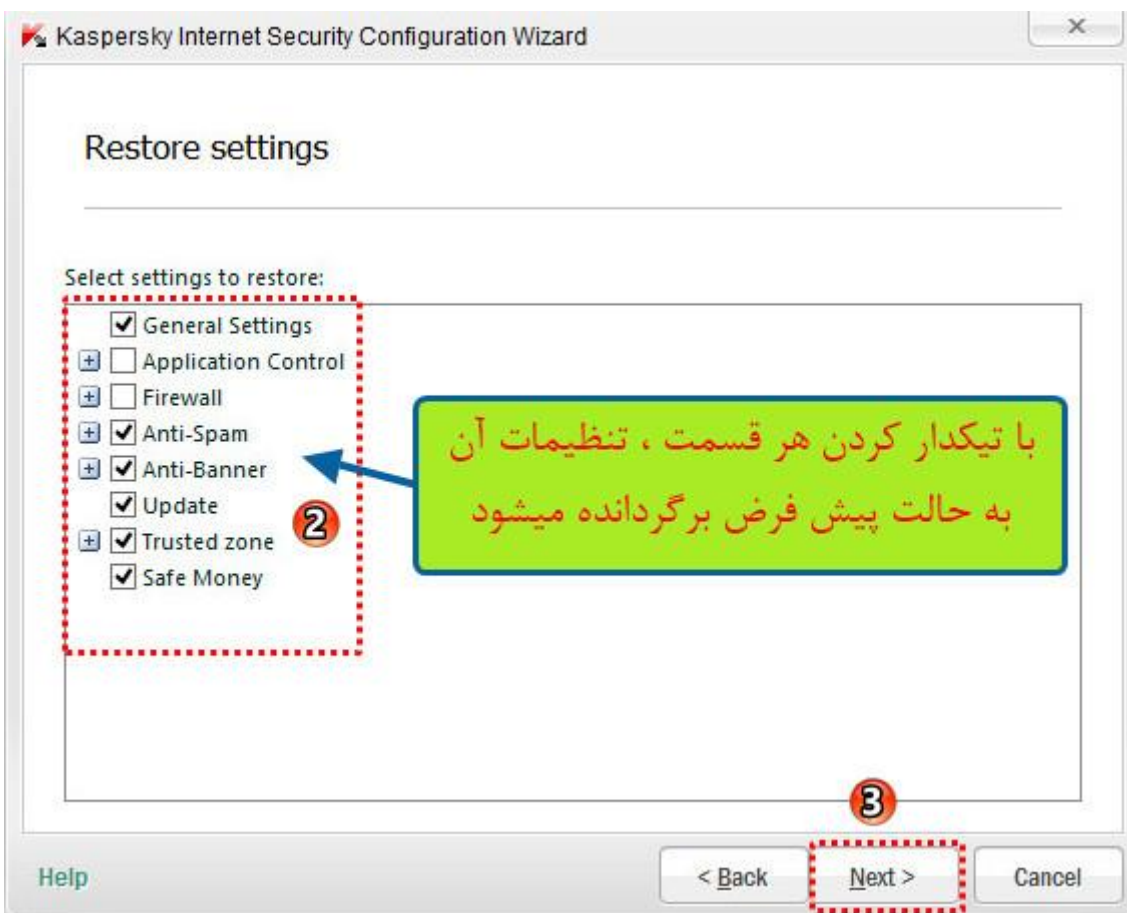
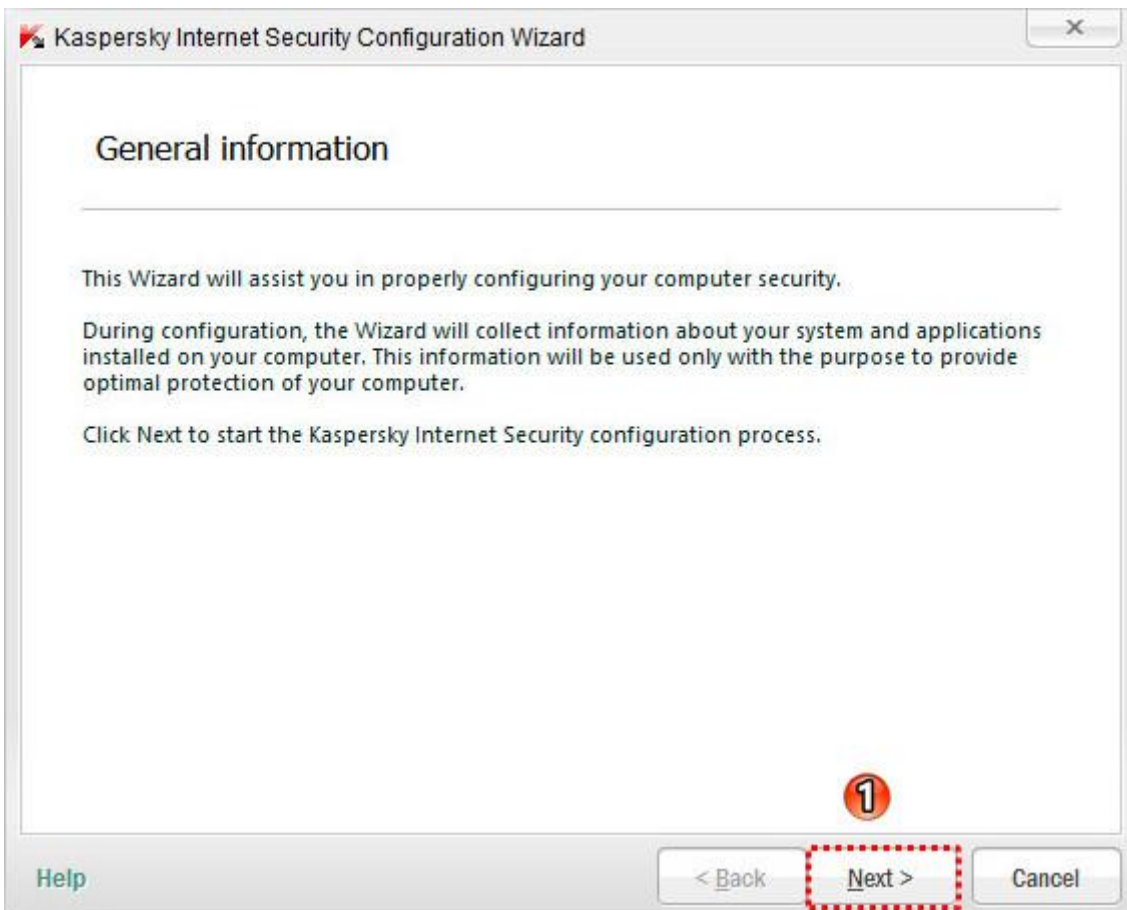
۱- **Export** : جهت ذخیره سازی تنظیمات در یک فایل (جهت استفاده پس از نصب مجدد آنتی ویروس بعد از نصب ویندوز

جدید و یا استفاده در سیستم های دیگر)

۲- **Import** : جهت وارد کردن تنظیمات به آنتی ویروس از فایل

۳- **Restore** : جهت بازگردانی تنظیمات پیش فرض کسپرسکی

مراحل انجام کار طبق اسکرین شاتها صورت میگیرد:





آموزش قابلیت‌های موجود در

# Kaspersky Pure 3



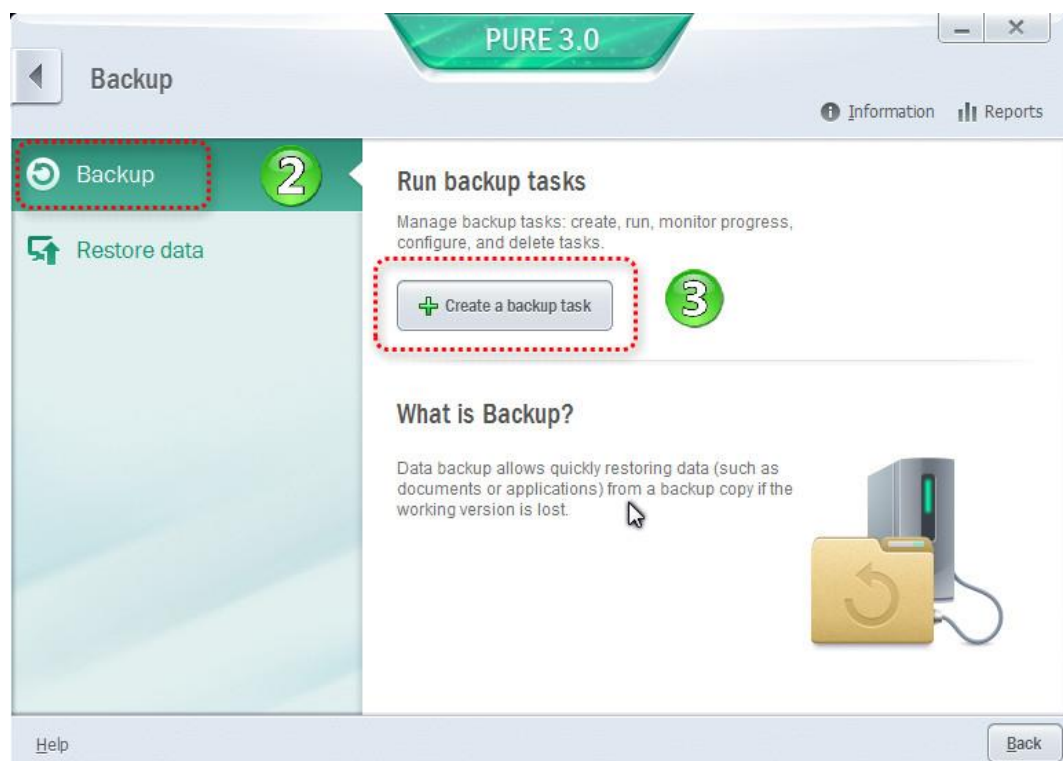
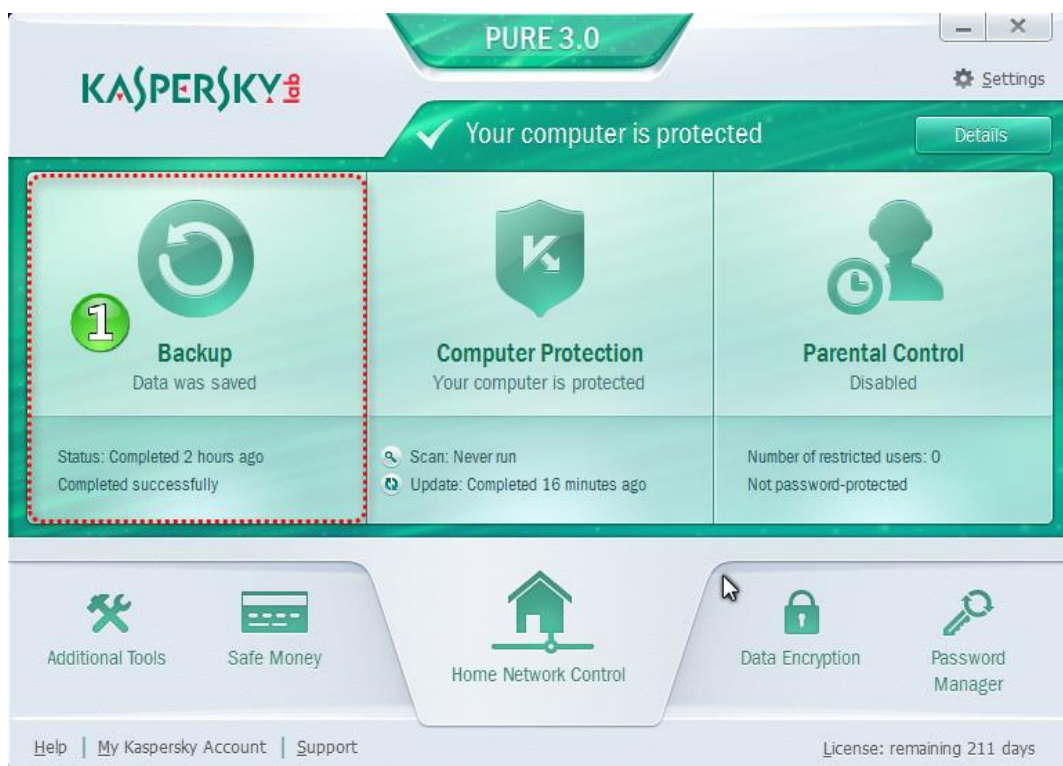
تهیه شده توسط **Nima Zapata**

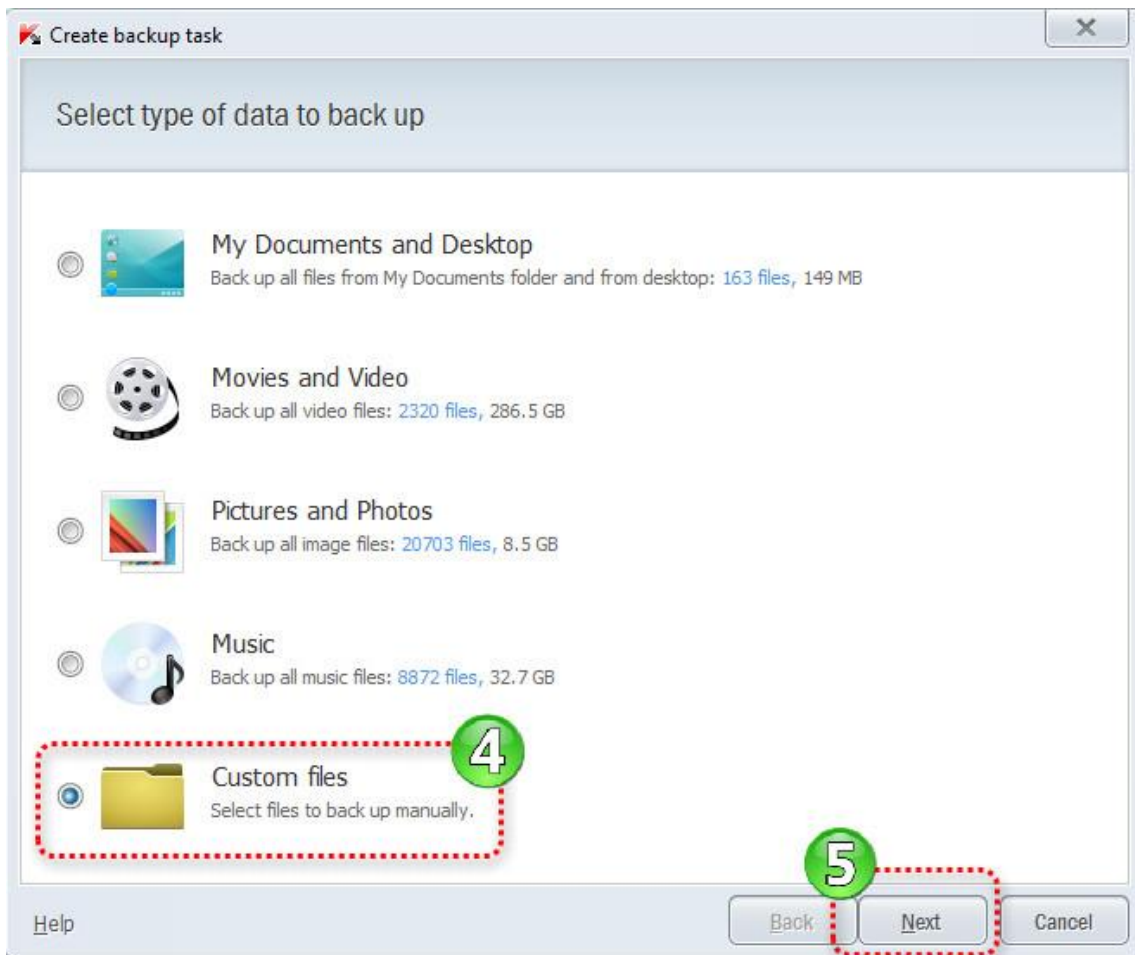


## پشتیبان گیری از اطلاعات (Backup)

یکی از قابلیت های جدیدی که به نسخه PURE اضافه شده ، قابلیت پشتیبان گیری از اطلاعات شما با بهترین امنیت می باشد.

برای این کار طبق اسکرین شات ها عمل کنید.

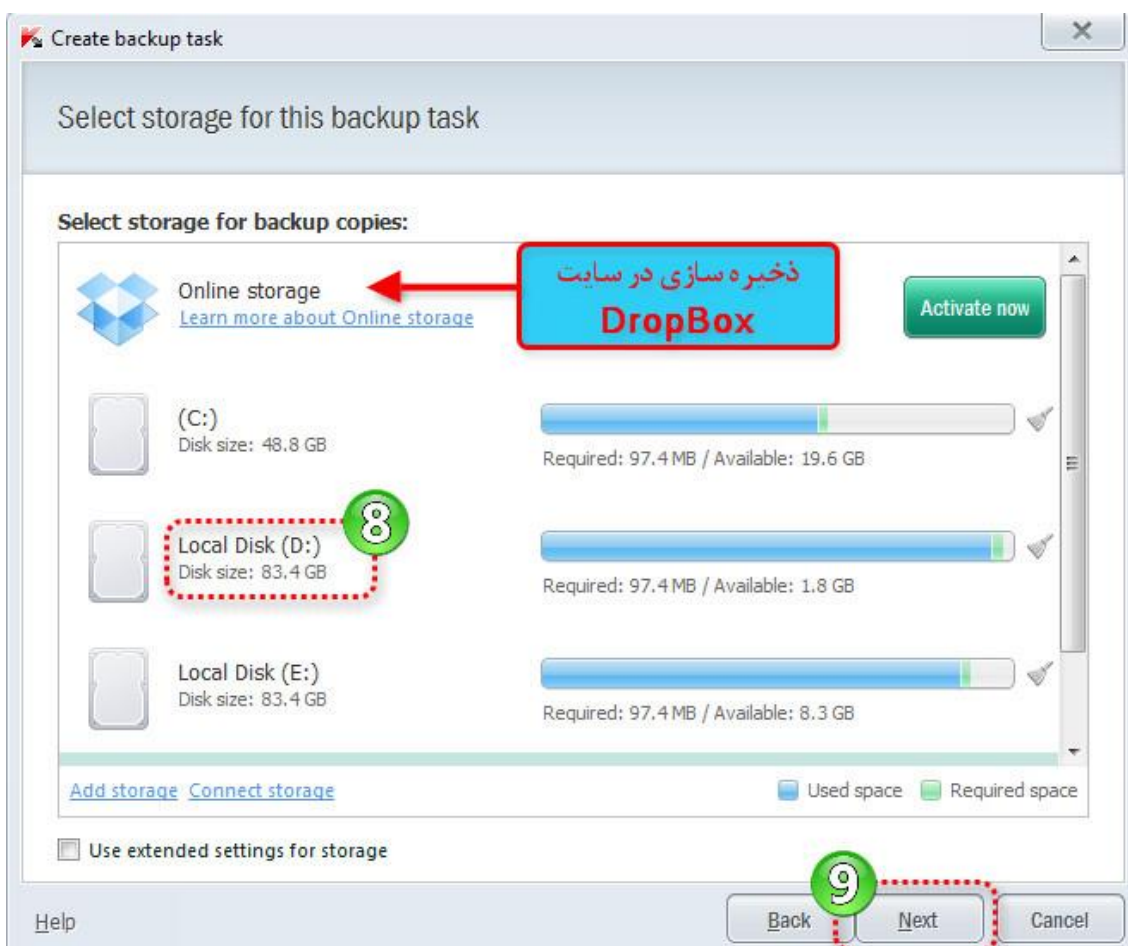




در پنجره باز شده ۵ گزینه وجود دارد که به وضوح حوزه کار هر کدام مشخص است. (پشتیبان گیری از تمام فایل های موسیقی ، فیلم ، عکس و ...)  
ما در اینجا آخرین گزینه یعنی Custom files رو که قابلیت پشتیبان گیری از هر نوع فایلی رو داره انتخاب میکنیم.

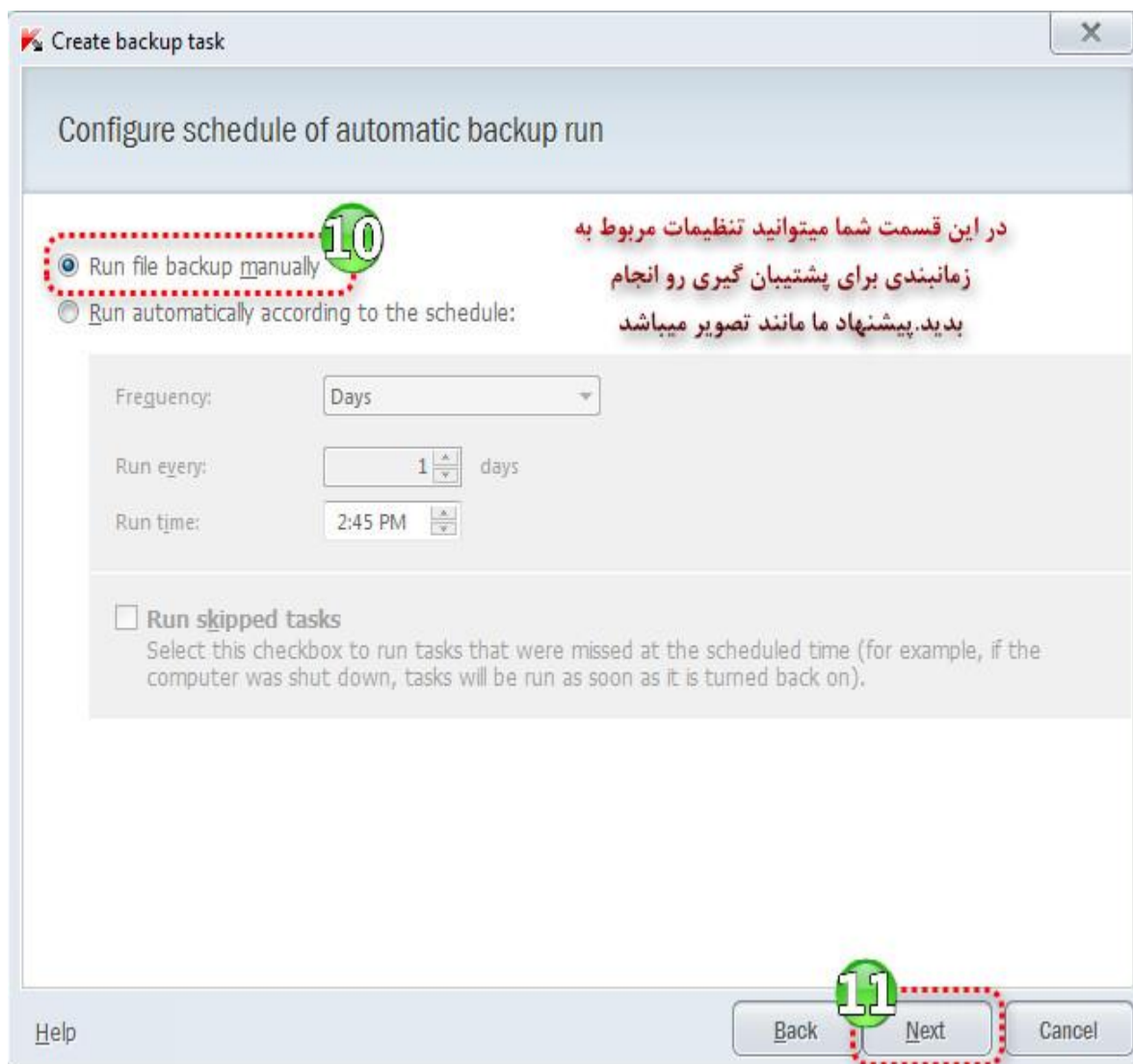


در قسمت بعد محل ذخیره سازی فایل Backup از شما پرسیده میشود.



گزینه اول برای ذخیره سازی آنلاین در سایت Dropbox میباشد که 2GB فضای رایگان در اختیار شما میگذارد. با زدن دکمه Activate Now شما وارد سایت Dropbox میشوید و پس از ثبت نام قادر به استفاده از فضای این سایت خواهید بود.

ما به عنوان نمونه درایو D رو به عنوان محل ذخیره سازی انتخاب میکنیم و روی Next کلیک میکنیم. و سپس :



در پنجره بعد پس از انتخاب نام فایل مورد نظر بر روی Finish کلیک کنید. اکنون فایل Backup شما ساخته میشود.

## Restore data

برای بازگرداندن فایل های پشتیبان گیری شده میتوانید مانند شکل زیر عمل کنید...

The screenshot displays the PURE 3.0 Backup application window. The title bar shows 'PURE 3.0' and standard window controls. The sidebar on the left has 'Backup' and 'Restore data' (highlighted with a red dashed box). The main area is titled 'Restore data from backup' and contains the following information:

- Online storage:** Available: 2.00 GB of 2.00 GB, Tasks: No tasks, Data size: 243.87 KB. A 'Restore data' button is present.
- Local Disk (D:):** Available: 1.68 GB of 83.38 GB, Location: D:\Backup, Tasks: 126\_\_01. A 'Restore data' button is present and highlighted with a red dashed box.

At the bottom, there is a 'Help' button on the left and a 'Back' button on the right.

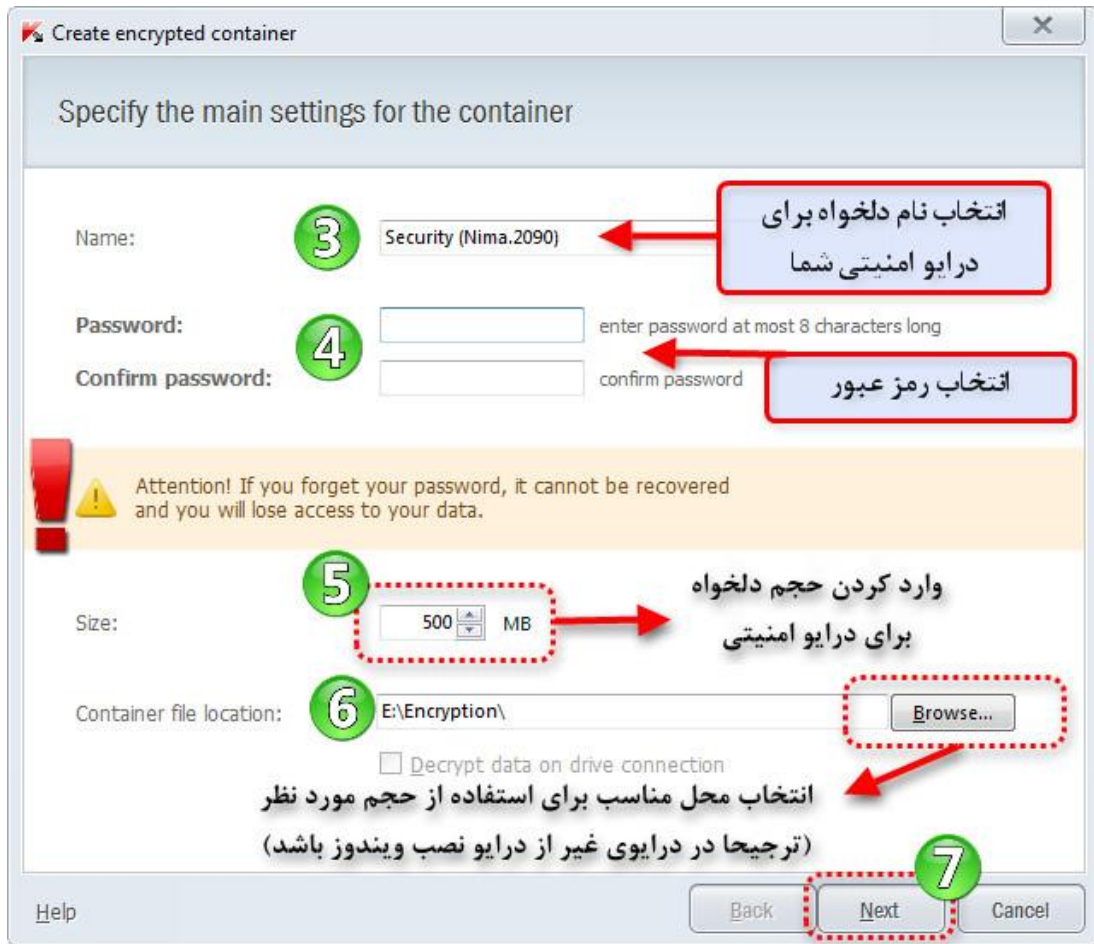


# Data Encryption

قابلیت جدیدی که در نسخه PURE اضافه شده که بوسیله آن می‌توانید اطلاعات شخصی خودتان را با ایجاد یک درایو امنیتی جدید محافظت کنید.

طبق اسکرین شات ها عمل کنید:

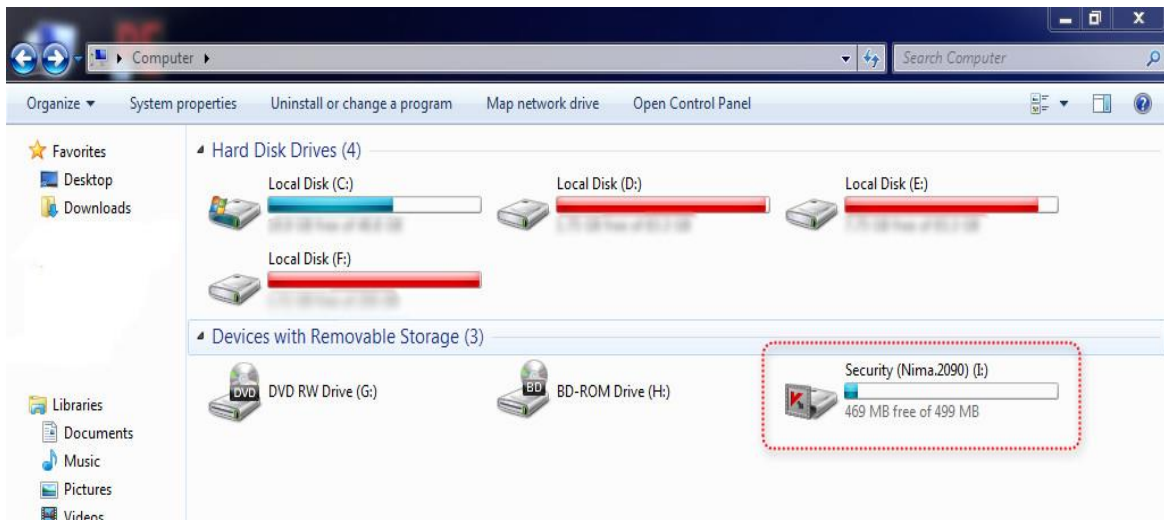




**توجه مهم:** در صورت فراموشی رمز عبور ، اطلاعات شخصی شما به هیچ وجه قابل دسترسی نمی باشد...

پس از آن بر روی Next و سپس بر روی Finish کلیک کنید.

درایو مجازی شما ساخته شده است (مانند شکل زیر)



اکنون میتوانید اطلاعات خودتان را در این درایو کپی کنید. پس از این کار شما به دو روش میتوانید درایو خود را مخفی کنید.

**روش اول:** با باز کردن کاسپر و کلیک بر روی **Data Encryption** و سپس مانند شکل زیر:



**روش دوم:** به اسکرین شات توجه کنید



پس از این کار درایو شما مخفی می شود و از طریق My Computer قابل مشاهده نمی باشد.

برای مشاهده مجدد درایو وارد کسپرسکی شوید و بر روی Data Encryption کلیک کنید و سپس :



**HaD!e6z**

۱۰ مرداد ۹۲