آموزش کامل تصویری

ESET SMART SECURITY 6

تهیه شده توسط Hadie6z

www.ParsBook.org

معرفی صفحه اصلی ESET SMART SECURITY 6

Home

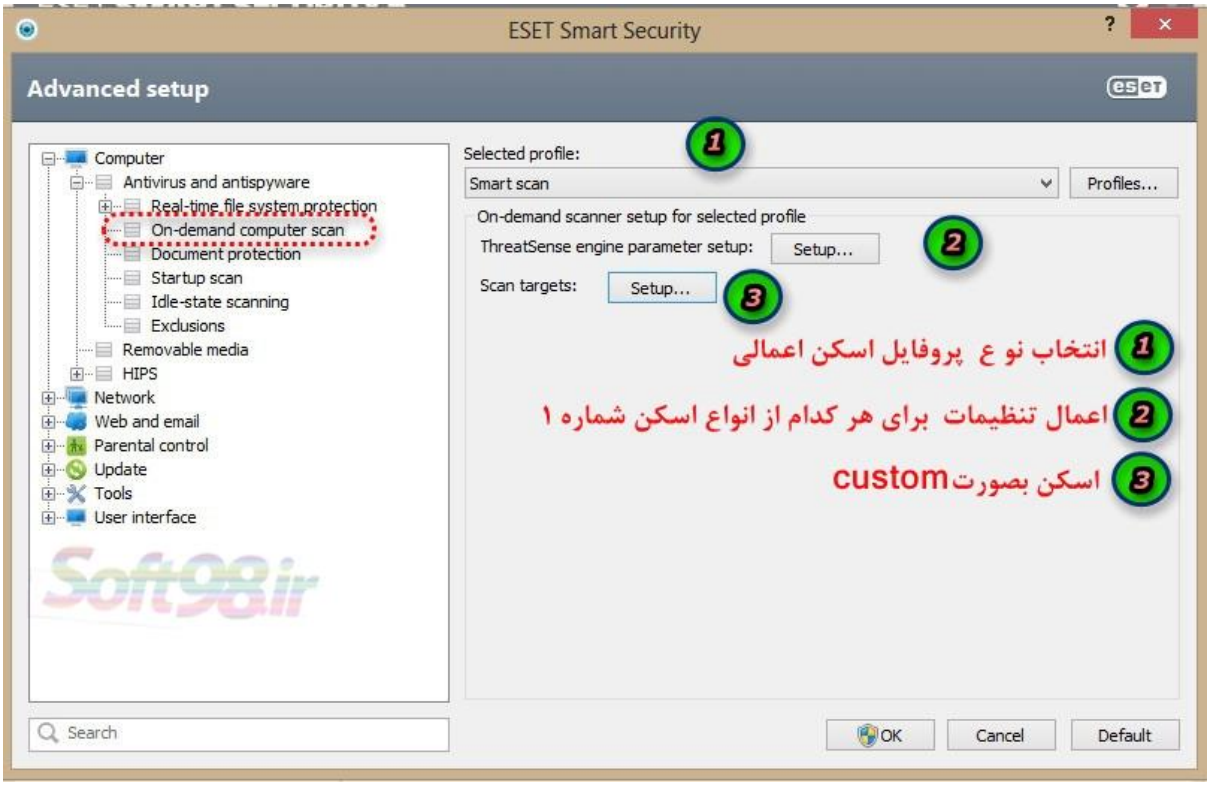
صفحه اصلی اطلاعاتی در مورد وضعیت حفاظت و امنیت هوشمند ESET می باشد.

www.ParsBook.org

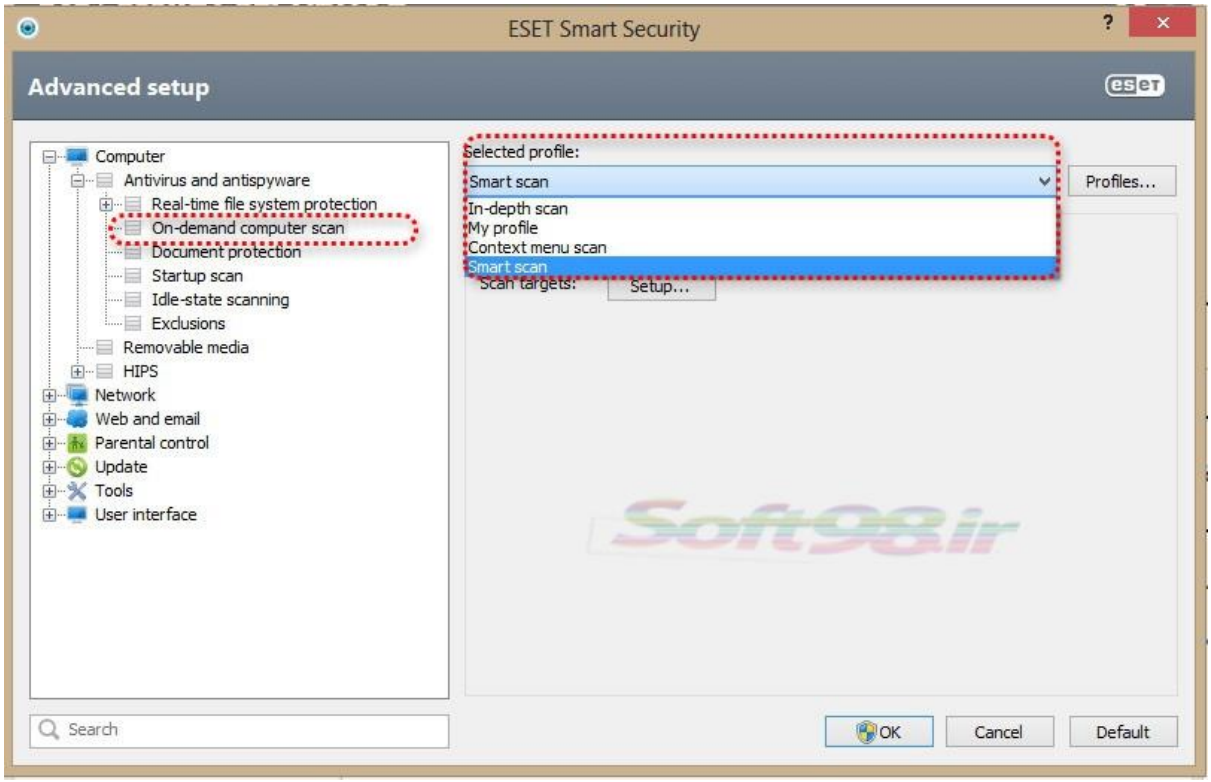
Computer scan

با استفاده از این گزینه شما می توانید به پیکربندی و راه اندازی اسکن هوشمند و یا اسکن سفارشی بپردازید.

توضیحات قسمت ۶ (تنظیمات پیشرفته برای اسکن)



www.ParsBook.org



۱- In-depth scane اسکن عمیق و دقیق

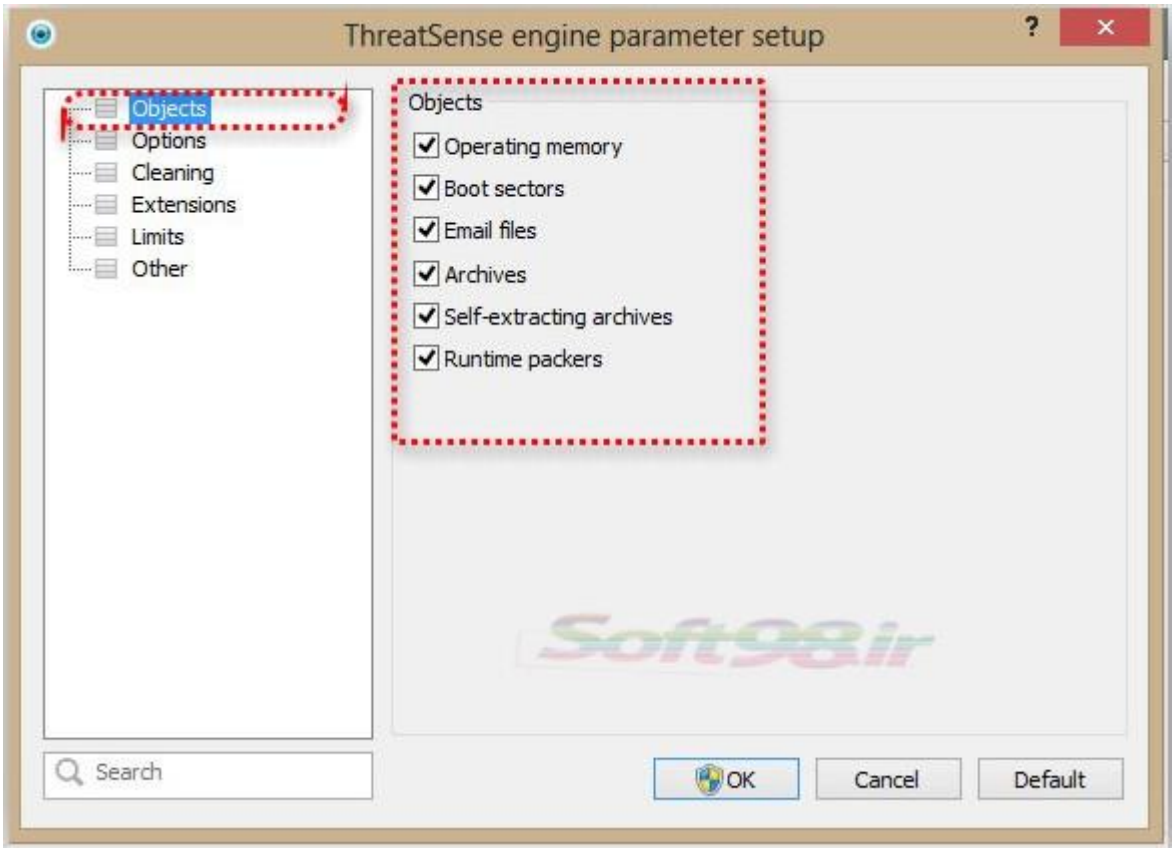
۲- My profile اسکن بصورت تنظیمات پروفایل شخصی

۳-Context menu scan تنظیمات درجه اسکن قرار گرفته در راست کلیک

۴- Smart scan اسکن سریع و هوشمند

فایلهای مورد اسکن :

تنظیمات فایلها بر اثرنوع اسکن In-depth scane و My profile و Context menu scan و Smart scan



www.ParsBook.org

اهدافی که باید مورد اسکن قرار بگیرند:

۱-حافظه اصلی(operating memory)

در زمان انتخاب این گزینه حافظه در حال کارکرد (منظورRAM است) سیستم مورد اسکن قرار میگیرد.

۲-سکتورهای راه اندازی (Boot sector)

۳- فایلهای موجود در نامه های الکترونیک

۴-فایلهای آرشیو

۵- فایلهای آرشیو شده خود اجرا

۶-"runtime packer"

توجه:توضیحات بیشتر کلیه موارد در قسمت Real time به طور کامل داده میشود.

Update

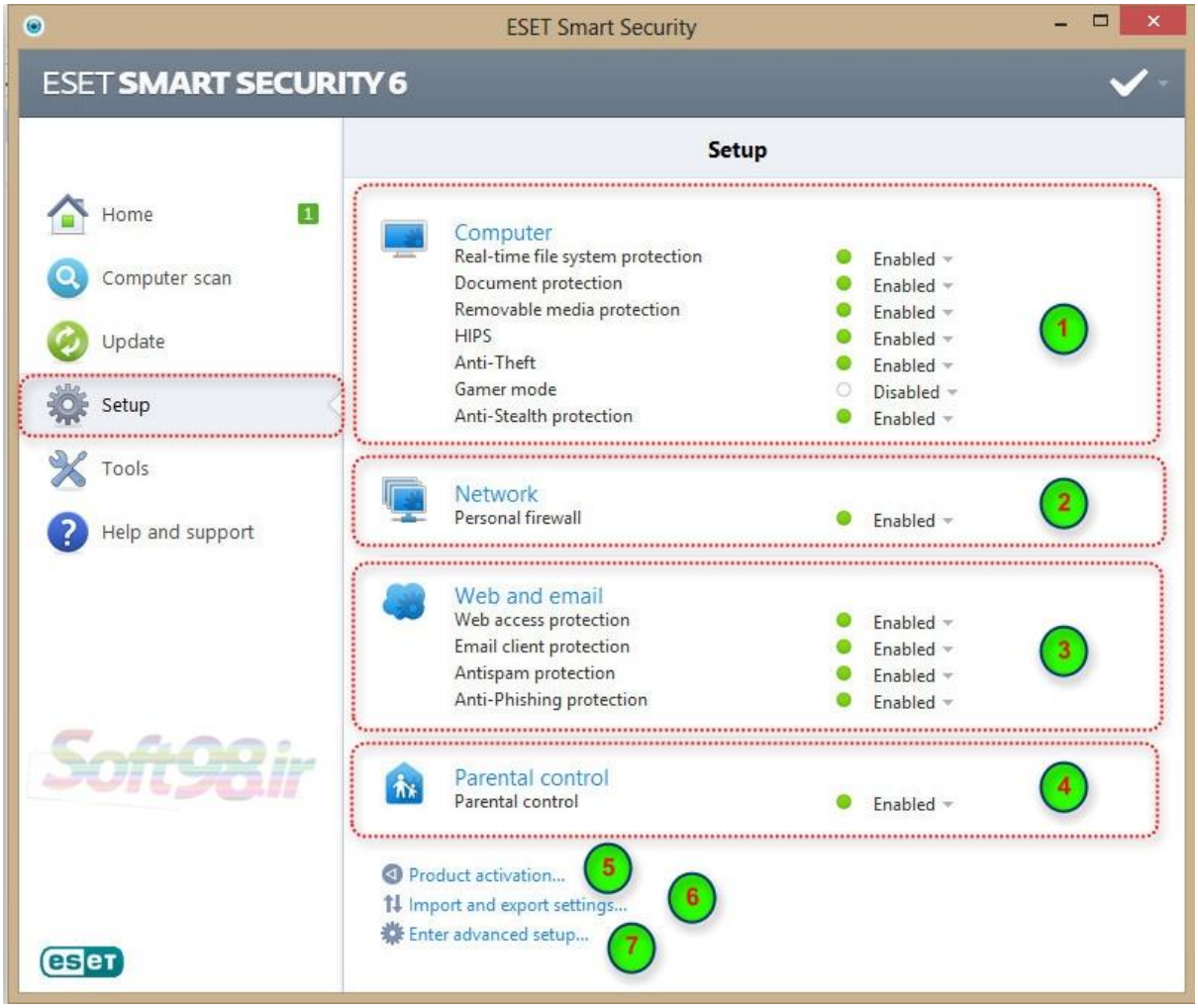
نمایش اطلاعات مربوط به بروزرسانی آنتی ویروس و دیتابیس

توجه: توضیحات بیشتردر مورد تنظیمات آپدیت در قسمت تنظیمات (Advanced setup) داده میشود.

www.ParsBook.org

Setup

این گزینه برای تنظیم سطح امنیتی برای کامپیوتر خود ، وب و پست الکترونیک، شبکه و کنترل والدین است.



Computer -۱

Real-time file system protection

حفاظت"real–time" از سیستم فایلها به معنی کنترل تمامی رخدادهایی در رایانه است که با ماژول ضدویروس ارتباط دارند حفاظت"real–time" ، از سیستم فایلها (گارد نرم افزار) تمامی واحدهای حافظه (فلش و هاردهای اکسترنال و...) را به لحاظ وجود آلودگی ویروسی مورد بررسی قرار می دهد و رخدادهای گوناگون مرتبط با تهدیدات رایانه ای بر نوع این کنترل تاثیر می گذارند.

توضیحات بیشتر تنظیمات مربوطه در قسمت **Advanced setup** داده میشود

Document protection

این قسمت به منظور حفاظت از اسناد میباشد.

توضیحات بیشتر تنظیمات مربوطه در قسمت **Advanced setup** داده میشود.

Removable media

حفاظت از وسایل Removable media مانند USB,CD,DVD و...

توضیحات بیشتر تنظیمات مربوطه در قسمت **Advanced setup** داده میشود.

www.ParsBook.org

HIPS (Host-based Intrusion Prevention System)

HIPS برای محافظت از سیستم شما در برابر فعالیت نرم افزارهای مخرب و ناخواسته ای که سعی دارند تاثیر مخرب و منفی از خود باقی بگذارند می باشد. HIPS با بهره گیری از پیشرفته تجزیه و تحلیل رفتاری همراه با قابلیت تشخیص شبکه فیلتر برای نظارت بر فرایندهای در حال اجرا و فایل ها و کلید های رجیستری است. HIPS جدا از حفاظت Real time ازیک فایل سیستمی ، یک فایروال نیست و نظارت تنها فرایندهای در حال اجرا در سیستم عامل را بر عهده دارد.

هشدار: تغییرات تنظیمات HIPS باید فقط توسط یک کاربر با تجربه باید انجام شود.

توجه: تغییرات فعال کردن HIPS و فعال کردن تنظیمات دفاع از خود پس از راه اندازی مجدد سیستم عامل ویندوز عمل خواهد کرد. غیر فعال کردن کل سیستم HIPS نیز نیاز به راه اندازی مجدد کامپیوتر دارد.

مهم : غیر فعال کردن مکانیسم دفاع از خود باعث می شود که HIPS در برابر تهدیدات بالقوه نتواند کاری انجام دهد بنابراین این کار توصیه نمی شود.

Anti-Theft

Anti-Theft به شما اجازه می‌دهد تا در صورت اتصال سیستم دزدیده شده به اینترنت، بتوانید با استفاده از اطلاعات اتصال به اینترنت محل سیستم خود را پیدا کنید همچنین با استفاده از Built-in Camera موجود در لپ تاپ از شخصی که به لپ تاپتان دسترسی دارد عکس تهیه کنید.

Gamer mode

Gamer Mode حالتی است که با فعال کردن آن آنتی ویروس دست از اسکن های اتوماتیک و پیامهای هشدار برمیدارد و کمتر از منابع سیستم (RamوCpu) استفاده میکنه تا در بازی دچار مشکل نشین پیشنهاد میشود اگر از سیستم قوی استفاده می کنین این گزینه را فعال نکنید.

البته در این حالت حفاظت از سیستم در پس زمینه اجرا می شودو هیچ تعاملی با کاربر را ندارد.

Anti-Stealth Protection

کار این تکنولوژی، یک سیستم پیچیده تشخیص برنامه های خطرناک مانند روت کیت ها است که می توانند خود را از سیستم عامل پنهان کنند و آنها را با استفاده از تکنیک های تست معمولی نمی توان تشخیص داد.

Configure Anti-Theft

۱- در صفحهٔ اصلی(Home) برای گام اول بر روی Configure Anti-Theft now کلیک کنید تا صفحهٔ جدیدی برای شما باز شود.

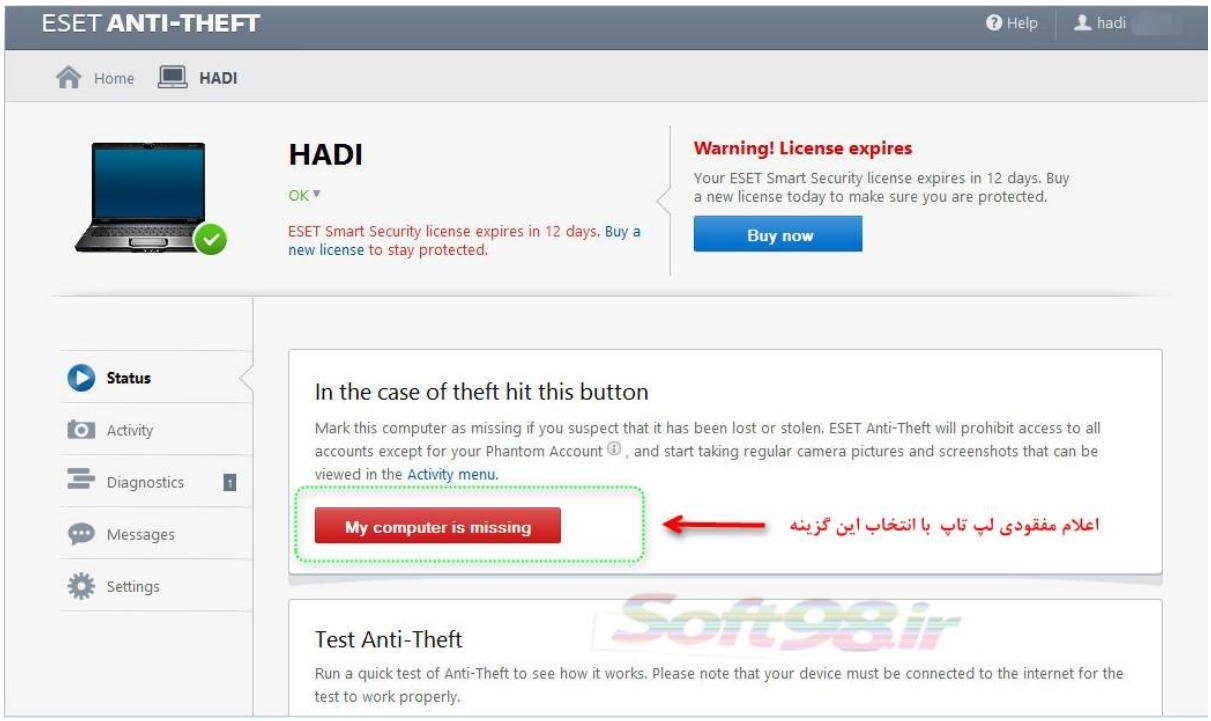
۲- اکنون درصفحه جدید از شما email و password اکانت شما در Eset را درخواست می کند در صورتی که فعلا اکانتی ندارید با استفاده از گزینه Create new ESET account یک اکانت جدید برای خود بسازید با انتخاب این گزینه شما را به صفحه اصلی شرکت Eset لینک خواهد کرد تا اکانت جدید باز کنید.
(در صورتی که حساب دارید و پسورد خود را فراموش کرده اید گزینه I forget my password را انتخاب کنید)

۳- بعد از تکمیل فرم و ایجاد account در سایت Eset اکنون میتواند اطلاعات حساب خود را در صفحه config برنامه وارد کنید.اگر تمام اطلاعات را به درستی وارد کرده باشید صفحه اتمام config نشان داده خواهد شد.

www.ParsBook.org

اعلام مفقودی لپ تاپ :

۱- ابتدا باید به سایت https://my.eset.com مراجعه کرده و مشخصات مربوط به حساب خود را که قبلا ایجاد کرده اید وارد کنید:



با اعلام مفقودی سیستم،هر زمان که سیستم شما آنلاین شود در عرض ۳ دقیقه به صورت اتوماتیک restart شده و دسترسی به تمام userهای local در سیستم شما سلب شده و خود برنامه یک fake account یا حساب مجازی (Phantom Account)ایجاد و سیستم با این حساب کاربری login خواهد شد و monitoring سیستم شما به مدت ۱۴ روز شروع خواهد شد که در صورت پیدا نشدن سیستم میتوانید ۵ روز مانده به پایان این زمان مجددا آن را تمدید کنید.

اکنون در قسمت Activity مربوط به panel حساب خود میتوانید به موارد زیر دسترسی داشته باشید:

محل جغرافیایی سیستم شما بر اساس IP
عکسهای گرفته شده با استفاده از built-in camera
Screenshot -های مربوط به desktop

معمولاً اطلاعات در این قسمت به صورت یک فایل zip جمع آوری شده و قابل دانلود می‌باشد.

www.ParsBook.org

بخش Diagnostics نیز مربوط به ارزیابی وضعیت امنیتی سیستم شما از قبیل بررسیPhantom Account

Real account autologin و...می‌باشد.

در بخش مربوط به Messages نیز میتوانید یک پیغام یک طرفه به سیستم خود بفرستید به گونه‌ای که در صفحه سیستم مفقود شده قابل نمایش باشد.این پیام ۵ دقیقه بعد از آنلاین شدن سیستم شما نمایش داده خواهد شد.اما توجه به این نکته هم ضروریست ، در صورتی که فرد بداند که سیستم track میشود بدون شک سیستم را از دسترس خارج خواهد کرد بنابراین در استفاده از این پیام باید دقت کرد.

بخش setting هم مربوط به تنظیمات مثلا نام device ،تنظیماتnotification ها و .... می‌باشد.

اگر بخواهید نحوه کار این برنامه را به صورت آزمایشی ارزیابی کنید کافیست بعد از وارد شدن به حساب کاربری خود در بخش activityگزینه Test را انتخاب کنید در این صورت یک پیغام مبنی بر اینکه درخواست تست داده شده آیا موافق هستید یا نه بر روی سیستم نمایش داده خواهد شد که با تایید این پیغام میتوانید قسمتی از قابلیت‌های آن را بررسی نمایید.

۲- Network

Personal firewall

ماژول **firewall** مانع از دسترسی کاربران غیرمجاز به کامپیوتر شما و استفاده از داده های شخصی شما می شود.

۳- Web and Email

Web access protection

حفاظت در برابر دسترسی به وب سایت

اتصال به اینترنت از ویژگی های استاندارد در یک کامپیوتر شخصی است ولی متاسفانه، می تواند رسانه اصلی برای انتقال کد مخرب باشد .این قسمت نظارت بر ارتباطات بین مرورگرهای وب و سرویس دهنده های از راه دور، و مطابق باپروتکل انتقال ابرمتن (HTTP) و ارتباطات رمزگذاری شده (HTTPS) دارد.

دسترسی به صفحات وب سایت با محتوای مخرب همیشه مسدود است.

هشدار: توصیه میشود این گزینه همیشه فعال باشد.

توضیحات بیشتر تنظیمات مربوطه در قسمت **Advanced setup** داده میشود.

www.ParsBook.org

Email client protection

باستفاده از پلاگین در Microsoft Outlook و دیگر برنامه های مدیریت ایمیل، Smart Security ESET کنترل همه ارتباطات مشتری ایمیل (POP3، MAPI، IMAP، HTTP)را انجام می دهد. هنگام بررسی پیام های دریافتی، این برنامه با استفاده از همه روش های اسکن پیشرفته ارائه شده توسط موتور اسکن ThreatSense به شناسایی برنامه های مخرب (حتی قبل از اینکه با دیتابیس آنتی ویروس همسان شود)می پردازد. اسکن از پروتکل های ارتباطی POP3 و IMAP مستقل از کلاینت ایمیل استفاده می شود.

ماژول حفاظت از ایمیل مشتریان به شرح زیر است :

Microsoft Outlook ، Outlook Express ، Windows Mail ، Windows Live Mail و Mozilla Thunderbird

محافظت از ایمیل با یک پلاگین برای این برنامه ها کار می کند. مزیت اصلی این پلاگین در کنترل کردن آن است .هنگامی که مشتری ایمیل دریافت میکند حاوی یک پیام رمز شده است که آن را رمزگشایی کرده و به اسکنر ویروس فرستاده میشود.

Antispam protection

یکی از بزرگترین مشکلات ارتباطات الکترونیکی ،ایمیل های ناخواسته، هرزنامه(Spam) نامیده می شوند، .هرزنامه (اسپم) تا ۸۰درصد از تمام ارتباطات ایمیل را در بر می گیرد. حفاظت Antispam به محافظت در برابر این مشکل می پردازد .ماژول Antispam صندوق پستی را از هرزنامه ها فیلتر می کند.

Anti-phishing protection

فیشینگ اصطلاح تعریف یک فعالیت جنایی است(هدف به دست آوردن اطلاعات محرمانه کاربر است)
فیشینگ اغلب برای به دست آوردن اطلاعات حساس مانند شماره حساب بانکی، شماره PINو غیره استفاده می شود.
حفاظت Anti-phishing در ESET Smart Security به حفاظت در مقابل این صفحات می پردازد و صفحاتی که از نظر نوع محتوا فیشینگ تشخیص دهد را مسدود می کند.

هنگامی که ناخواسته به یک وب سایت فیشینگ هدایت شوید، پیغام زیر را در مرورگر خود را دریافت خواهید کرد .

هشدار: توصیه میشود این گزینه همیشه فعال باشد.

Parental control-۴

ماژول کنترل والدین به شما اجازه پیکربندی تنظیمات کنترل والدین را میدهدکه پدر و مادر با ابزاری خودکار به حفاظت از فرزندان خود و تنظیم محدودیت برای استفاده از دستگاه ها و خدمات کمک میکند. هدف این ماژول، جلوگیری از دسترسی به

www.ParsBook.org

صفحات با محتوای نامناسب یا مضر برای کودکان و بزرگسالان جوان است. علاوه بر این، والدین می توانند دسترسی به بیش از ۴۰ وب سایت از پیش تعریف شده را دسته بندی کرده و در بیش از ۱۴۰ زیر شاخه اعمال ممنوعیت کنند.

توضیحات بیشتر تنظیمات مربوطه در قسمت **Advanced setup** داده میشود.

۵- Product activation

۶-Import and export setting

این ویژگی ها جهت پشتیبان گیری از تنظیمات جاری برای استفاده های بعدی کاربرمورد استفاده قرار می گیرد.

ویژگی "export"برای کاربرانی که قصد دارندتنظیمات انجام شده بر روی ESET Smart Security یک رایانه ر ا بر روی رایانه های دیگر (به صورت مشابه) انجام دهند، بسیار موردتوجه می باشد چرا که کافی است فایل".xml"تولید شده (طی فرایندexport)را درکلاینت های دیگرimport (وارد) نمایند.

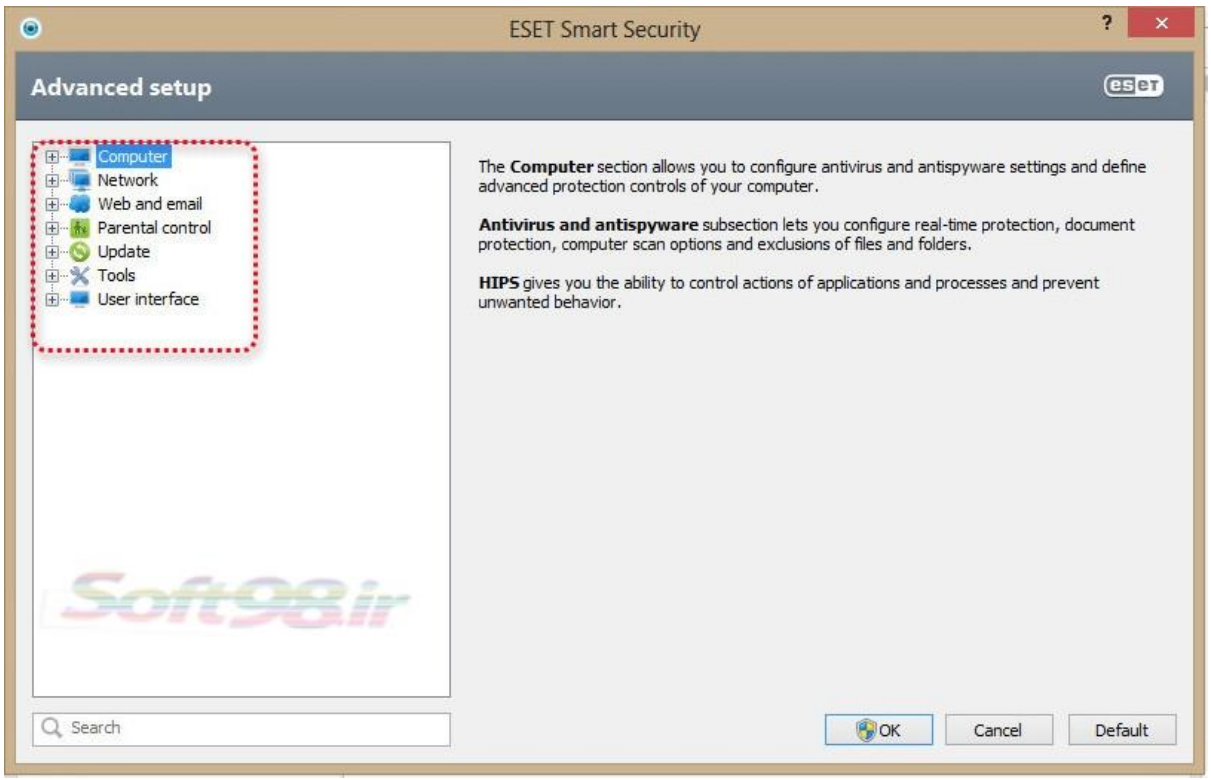
export

www.ParsBook.org

Import

۷- Enter advanced setup

ورود به صفحه تنظیمات پیشرفته



www.ParsBook.org

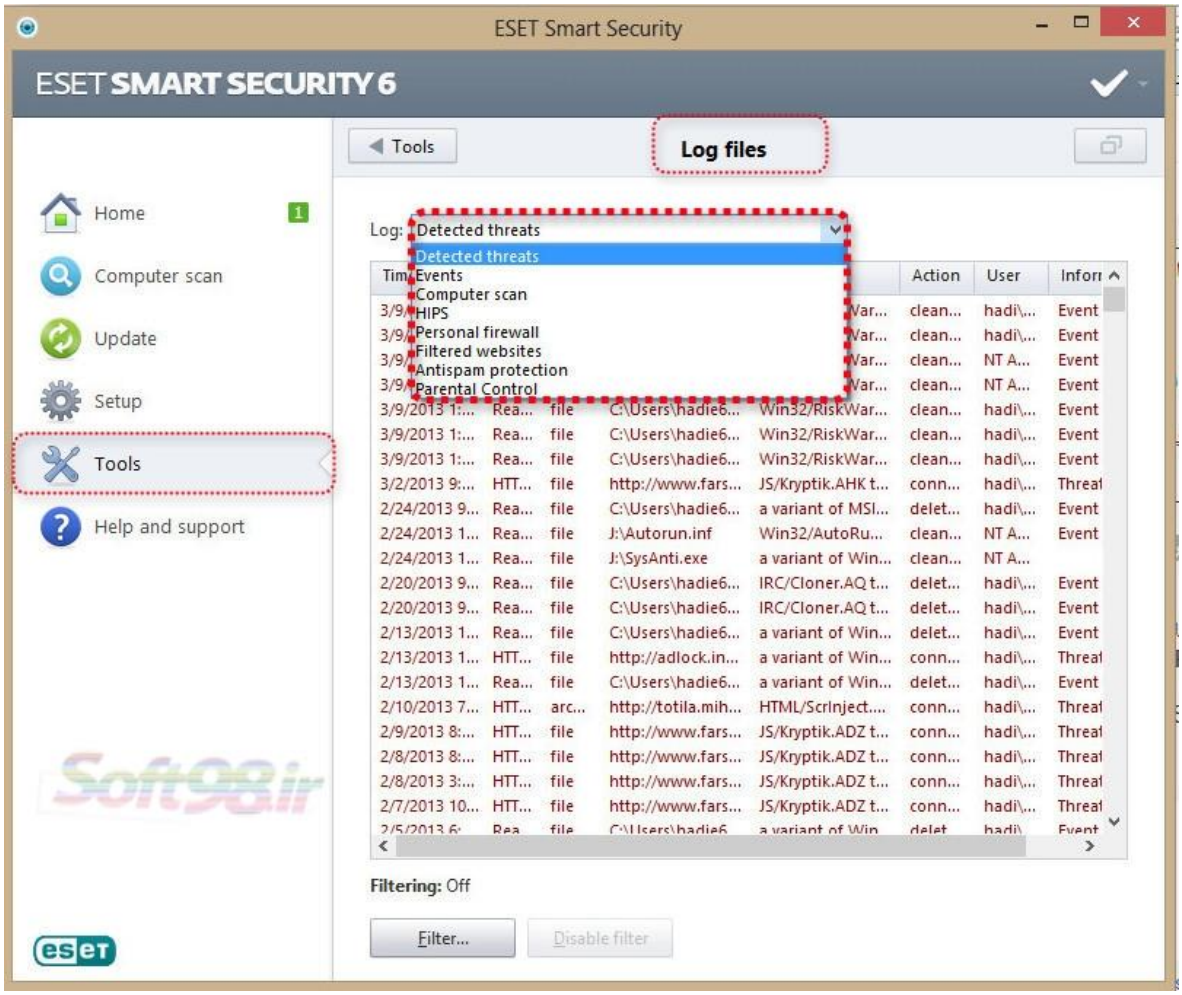
Tools

هریک از گزینه های اسکرین شات بالا به تفکیک شماره توضیح داده خواهد شد.

www.ParsBook.org

Log files–1

با استفاده از فایلهای ثبت رخدادها(log files) می توان تمامی رخدادهای مهم مربوط به نرم افزارو همچنین اطلاعات مربوط به تهدیدات شناسایی شده را مرور نمود . در واقع ثبت رخدادها برای استفاده های بعدی روش بسیار موثری در تحلیل، شناسایی تهدیدات و رفع نقص(troubleshooting) نرم افز ار است . ثبت رخدادها در پس زمینه کار رایانه انجام پذیرفته و خللی را در امور جاری کاربر ایجاد نمی نماید .همچنین اطلاعات مربوط به رخدادها بر اساس تنظیمات گوناگون مربوط به فایل ثبت رخدادهای جاری انجام می پذیرد.



نوع فایل ثبت رخدادهای مورد نظر را از منوی بازشونده"log" :

Detected threats : فایل ثبت رخدادهای مربوط به تهدیدات شناسایی شده

Event : فایل ثبت وقایع

Computer scan : فایل ثبت رخدادهای مربوط به اسکن کامپیوتر

HIPS : فایل ثبت رخدادهای مربوط به HIPS

Personal firewall : نمایش تمامی حملات از راه دور شناسایی شده، توسط فایروال

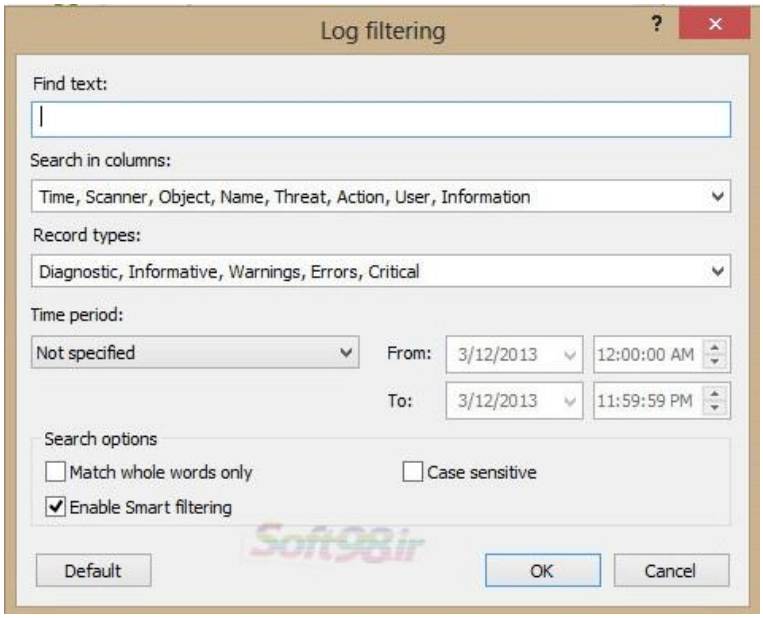
Filtered websites :نمایش لیستی از وب سایت هایی که با Web access protection یا Parental control مسدود شد.

Antispam protection : سوابق مربوط به ایمیل های هرزنامه (Spam)

Parental control : نمایش صفحات وب مسدود شده و یا مجاز شده و سایر محدودیتهای اعمالی توسط کنترل والدین

www.ParsBook.org

با استفاده از گزینه Filter میتوان فیلترهائی مانند زمان و ...جهت دیدن log های مورد نظر اعمال کرد.

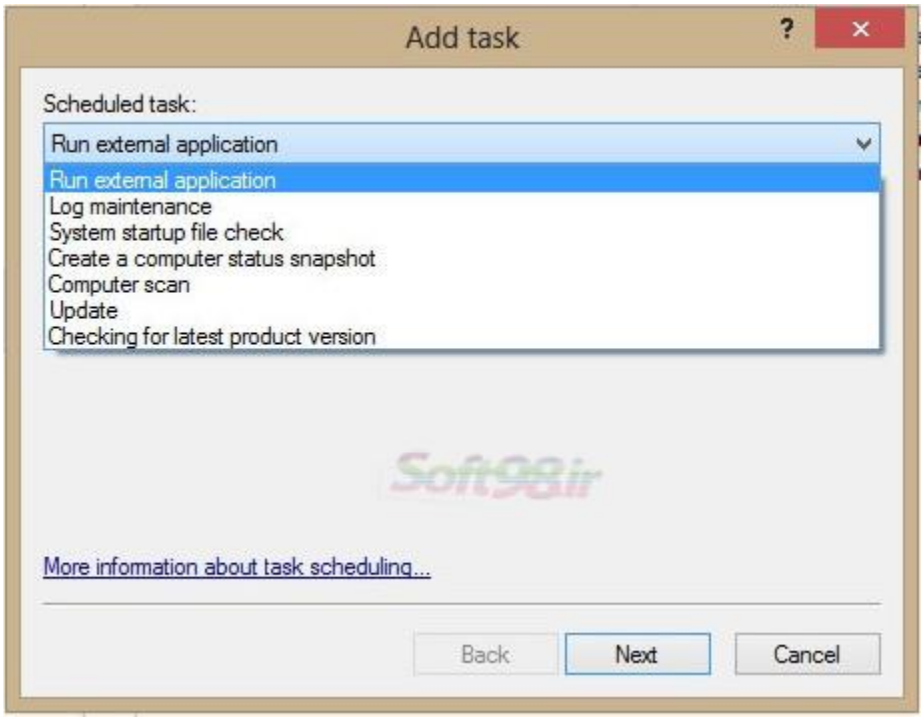


Scheduler -2

وظیفه Scheduler مدیریت و راه اندازی وظایف برنامه ریزی شده با تنظیمات از پیش تعریف شده است.

با استفاده از گزینه Add بصورت دستی میتوانید یک برنامه زمانبندی شده بسازید.

www.ParsBook.org



۱- اجرای برنامه کاربردی خارجی

۲- ثبت و نگهداری رخدادها

۳- بررسی فایلهای "startup"

۴- ذخیره وضعیت کامپیوتر وجمع آوری اطلاعات دقیق در مورد اجزای سیستم (drivers, applications) و بررسی سطح خطر هر کدام

۵- اسکن کامپیوتر

۶- بروزرسانی دیتابیس

۷-بررسی برای آخرین نسخه نرم افزار

www.ParsBook.org

Statistics -3

برای مشاهده یک گراف از داده های آماری مربوط به ماژول های ESET Smart Security باید از منوی کشویی یک گزینه را انتخاب کنید .

تو ضیحات در اسکرین شات

www.ParsBook.org

Quarantine -4

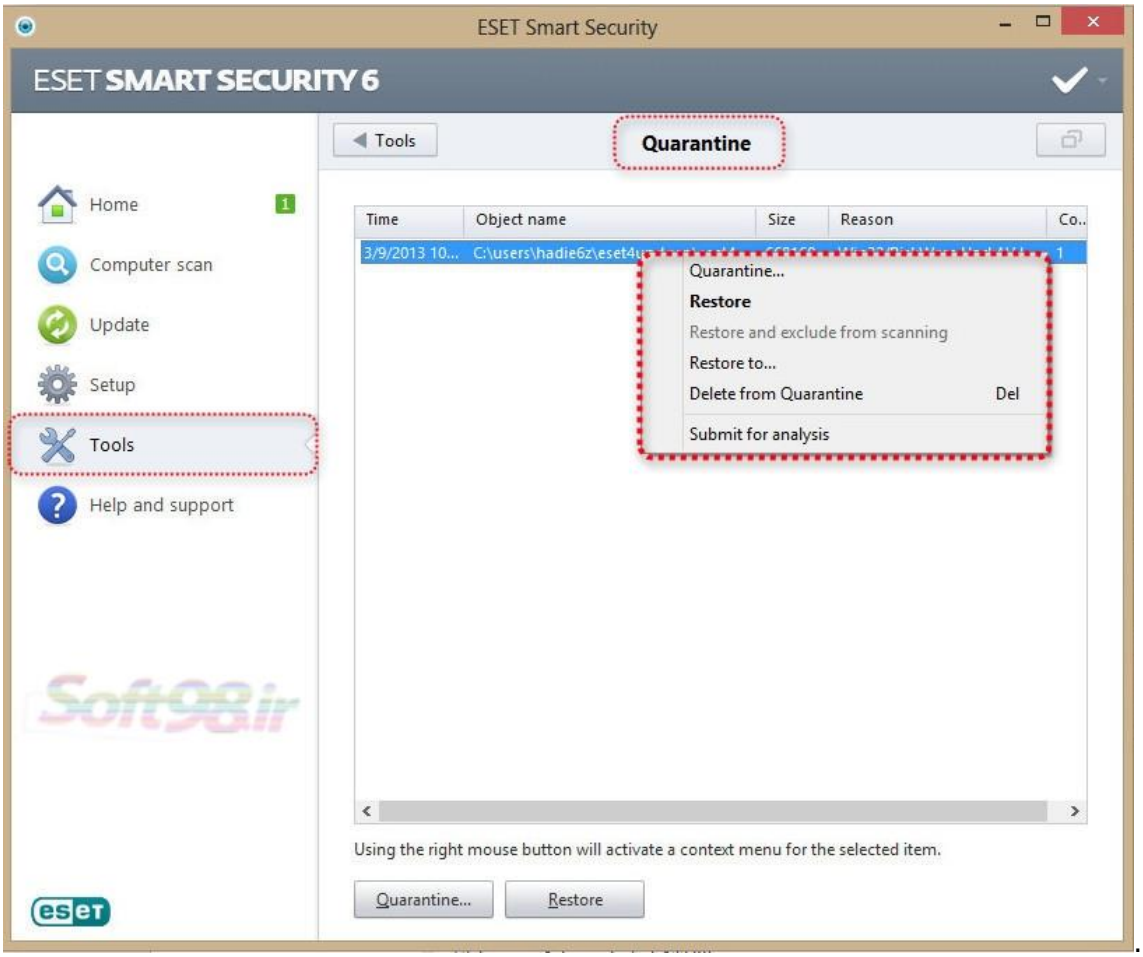
وظیفه اصلی پوشه قرنطینه نگهداری از فایلهای آلوده به روشی ایمن است . فایلهای آلوده را در شرائط خاص لازم است قرنطینه نمود .

این شرائط عبارتند از:

۱-زمانی که نتوان این فایلها را پاکسازی نمود.

۲- زمانی که پاک کردن فایل آلوده ایمن و یا منطقی نباشد.

۳-زمانی که فایل آلوده به صورت اشتباه آلوده شناخته شده باشد.



Quarantine : زمانی که بخواهیم فایلی را بصورت دستی قرنطینه کنیم.

Restore : برگرداندن فایل از قرنطینه به محل اولیه خود

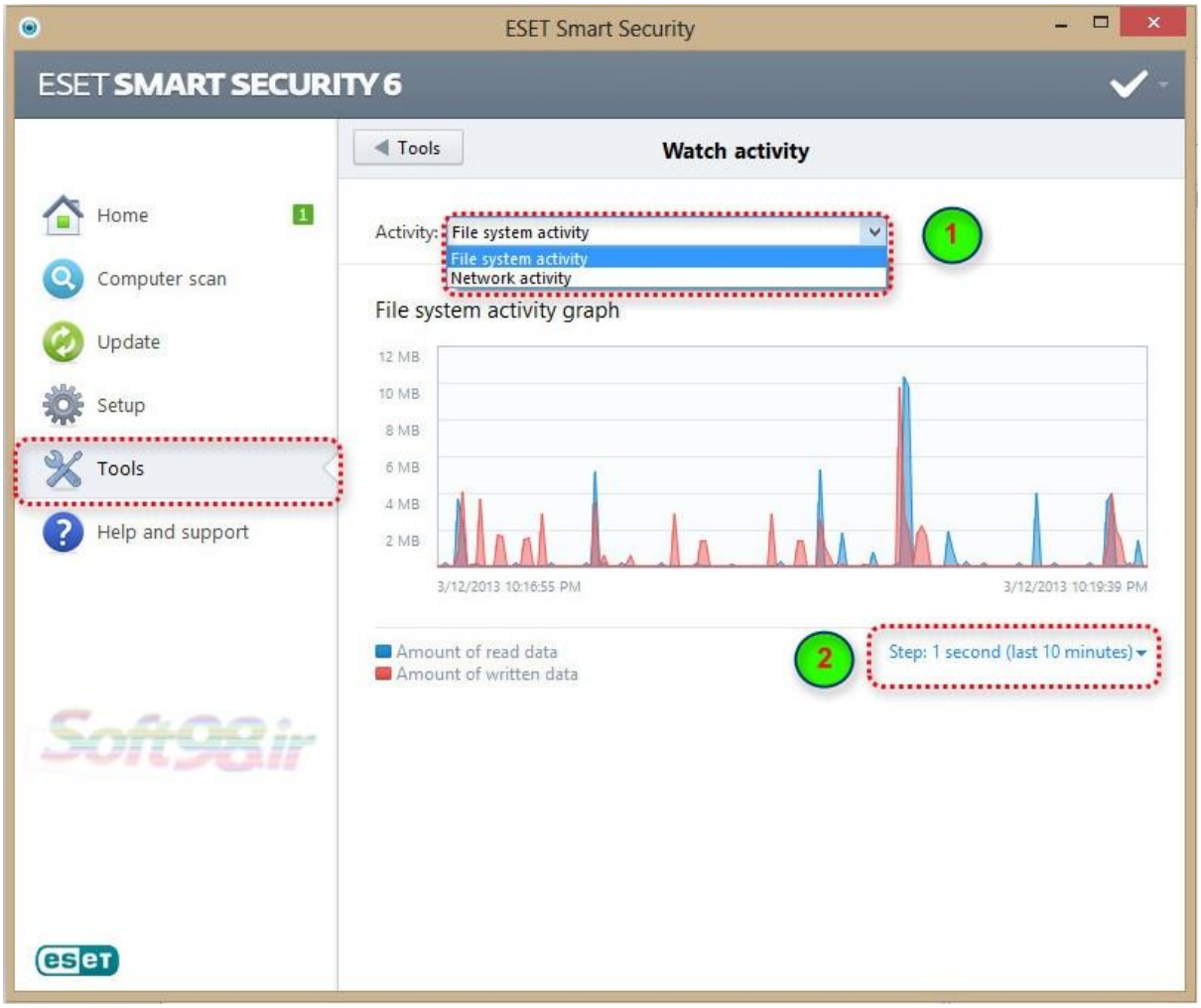
Restore to : برگرداندن فایل از قرنطینه به محل مورد نظر

Delete from Quarantine : حذف کامل فایل از قرنطینه

Submit for analysis : فرستادن فایل برای بررسی و تجزیه و تحلیل به لابراتوارهای ضدویروس شرکت"ESET"

www.ParsBook.org

Watch activity -5



۱-مشاهده فعالیت شامل دو حالت میشود:

File system activity : مشاهده فعالیتهای فایلهای سیستمی

Network activity : مشاهده فعالیتهای شبکه

۲-تعیین میزان نمایش فعالیتها

حالت اول : نمایش یک ثانیه (در ۱۰ دقیقه آخر)

حالت دوم : نمایش یک دقیقه (در ۲۴ساعت آخر)

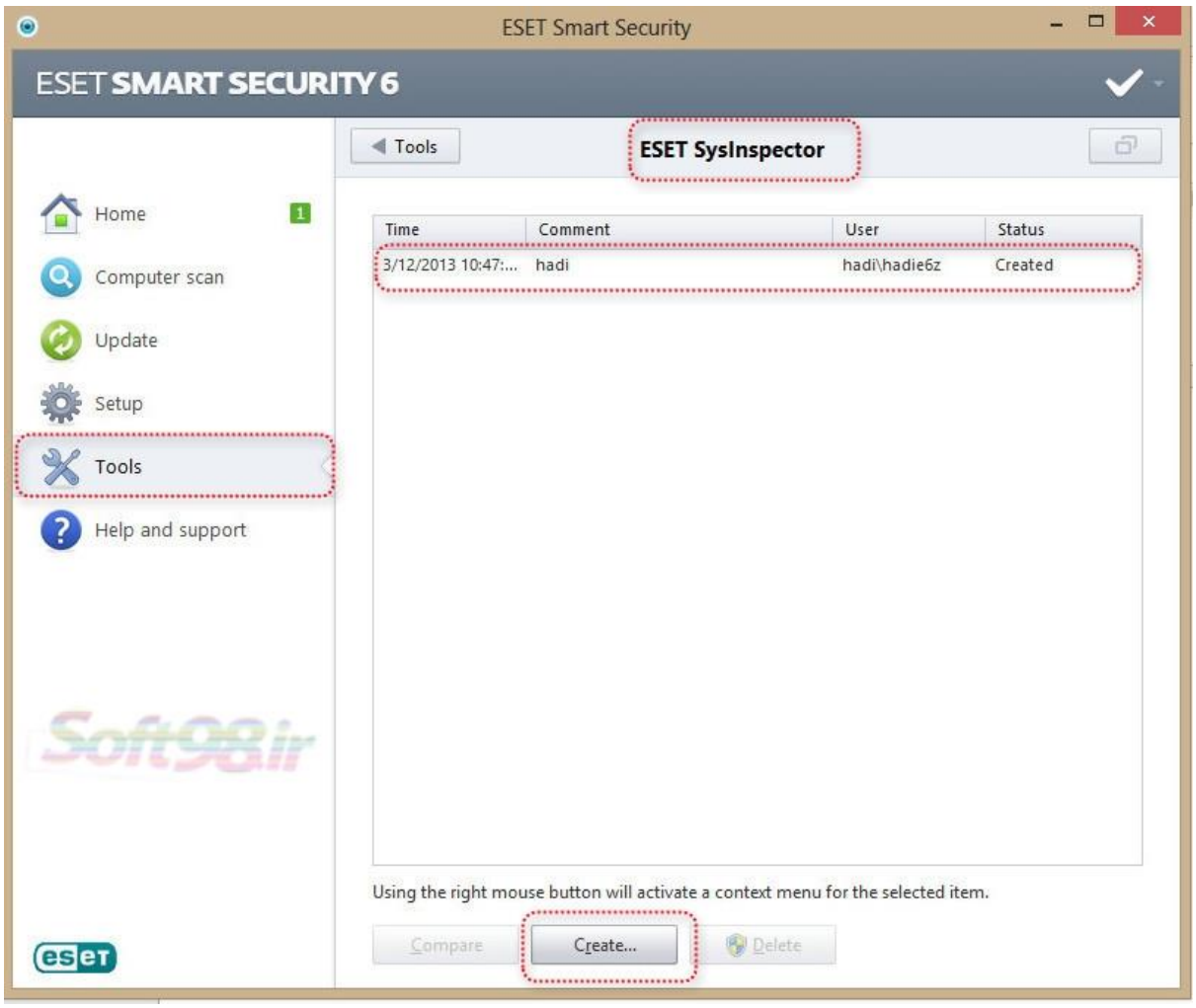
حالت سوم : نمایش یک ساعت (در ۱ ماه آخر)

حالت چهارم : نمایش یک ساعت (با انتخاب یک ماه)

www.ParsBook.org

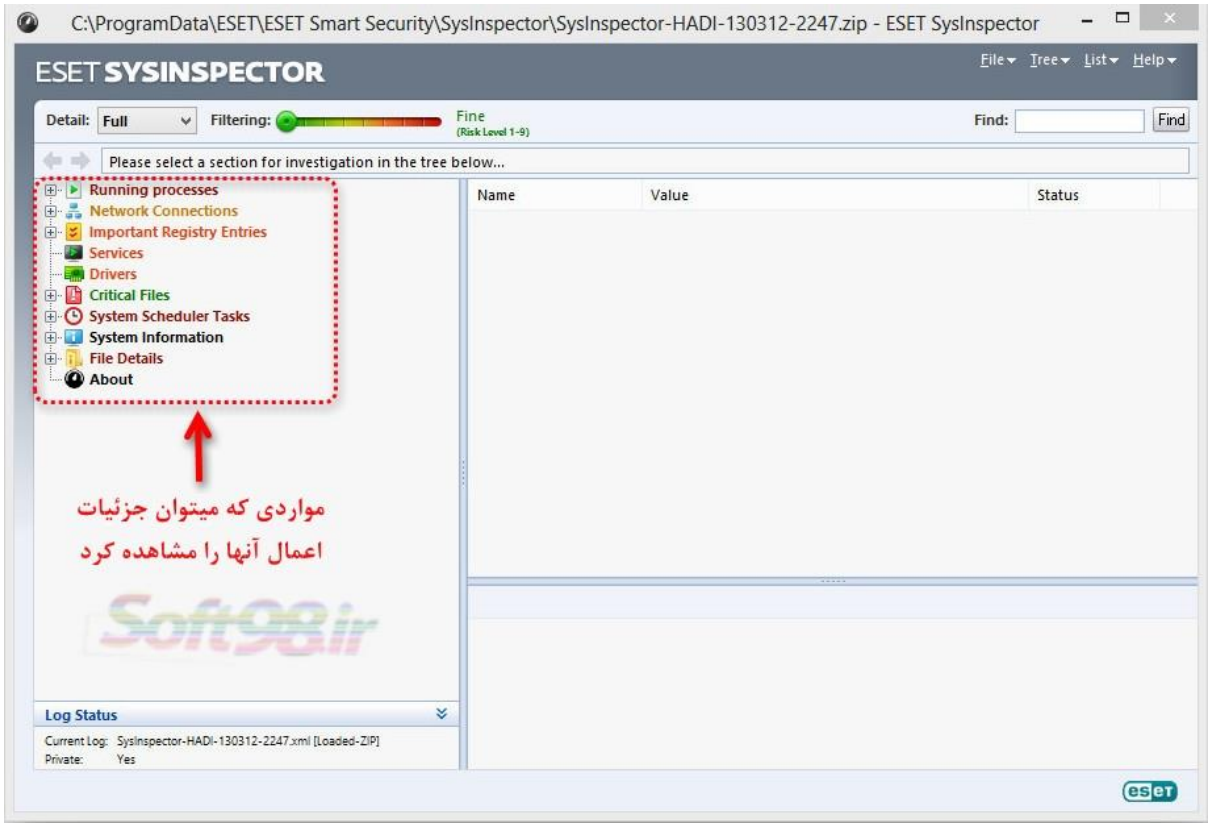
ESET SysInspector-6

ESET SysInspector برنامه ای است که به طور کامل به بازرسی کامپیوتر شما و جمع آوری اطلاعات دقیق در مورد اجزای سیستم از قبیل درایورهای نصب شده ، برنامه های کاربردی، اتصالات شبکه ، ورودی های رجیستری و ارزیابی سطح خطر هر جزء می پردازد .این اطلاعات می تواند به تعیین علت رفتار مشکوک سیستم که شاید در اثر ناسازگاری نرم افزار یا سخت افزار و یا ابتلا به تروجان کمک کند.(ویروسها و برنامه های مخرب معمولا پروسه مخفی دارند که با این قابلیت میتوان آنها را ردگیری کرد.)



برای ایجاد بر روی گزینه Create باید کلیک کرده و یک comment را باید وارد کرد. پس از آن نرم افزار شروع به جستجو میکند .پس تکمیل پروسه بروی گزینه ایجادشده توسط خودتان کلیک کنید.

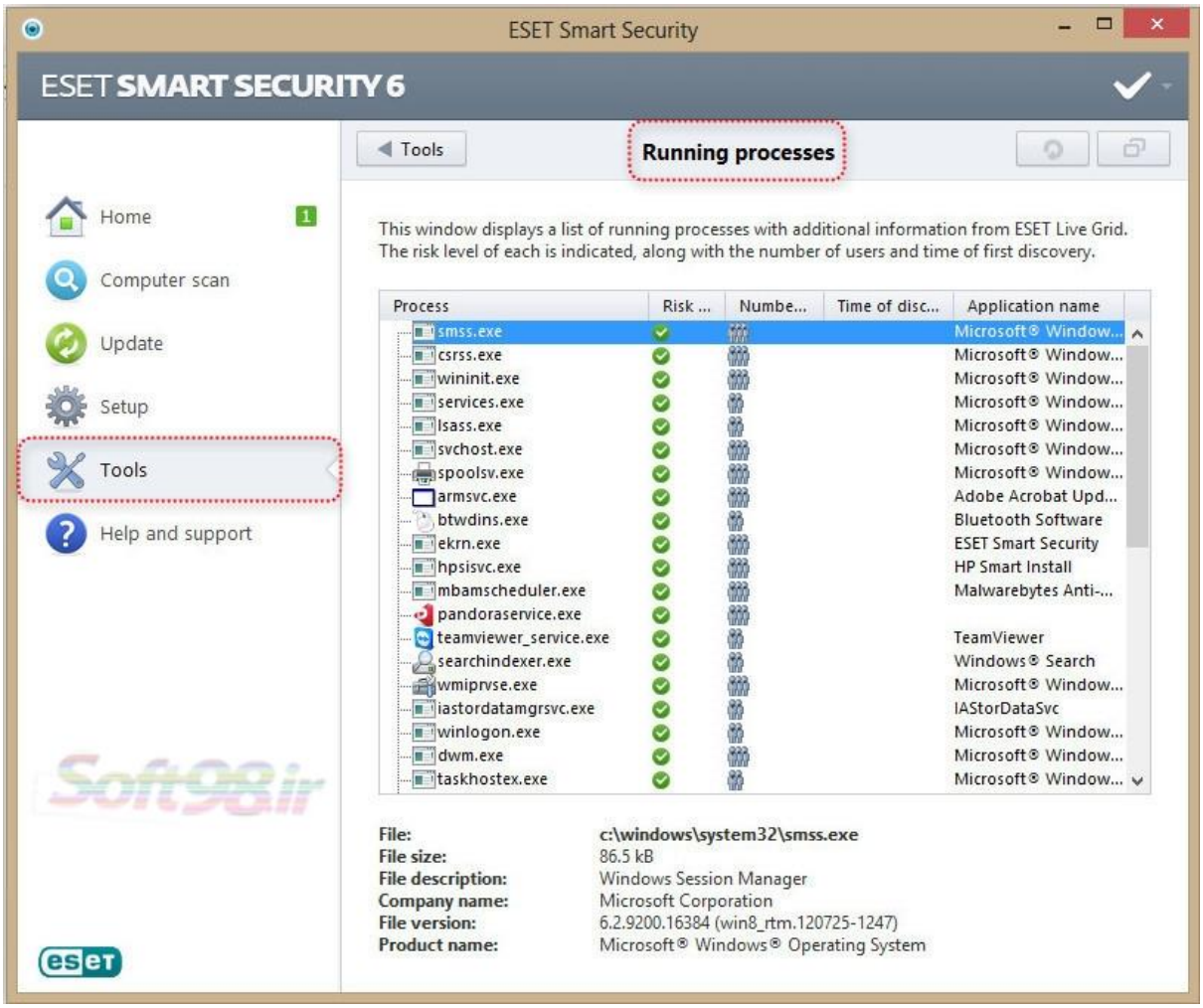
در صفحه باز شده می توانید کلیه موارد درایور ، اتصالات شبکه و .... را بصورت کامل مشاهده کنید.



www.ParsBook.org

Runnig processes –7

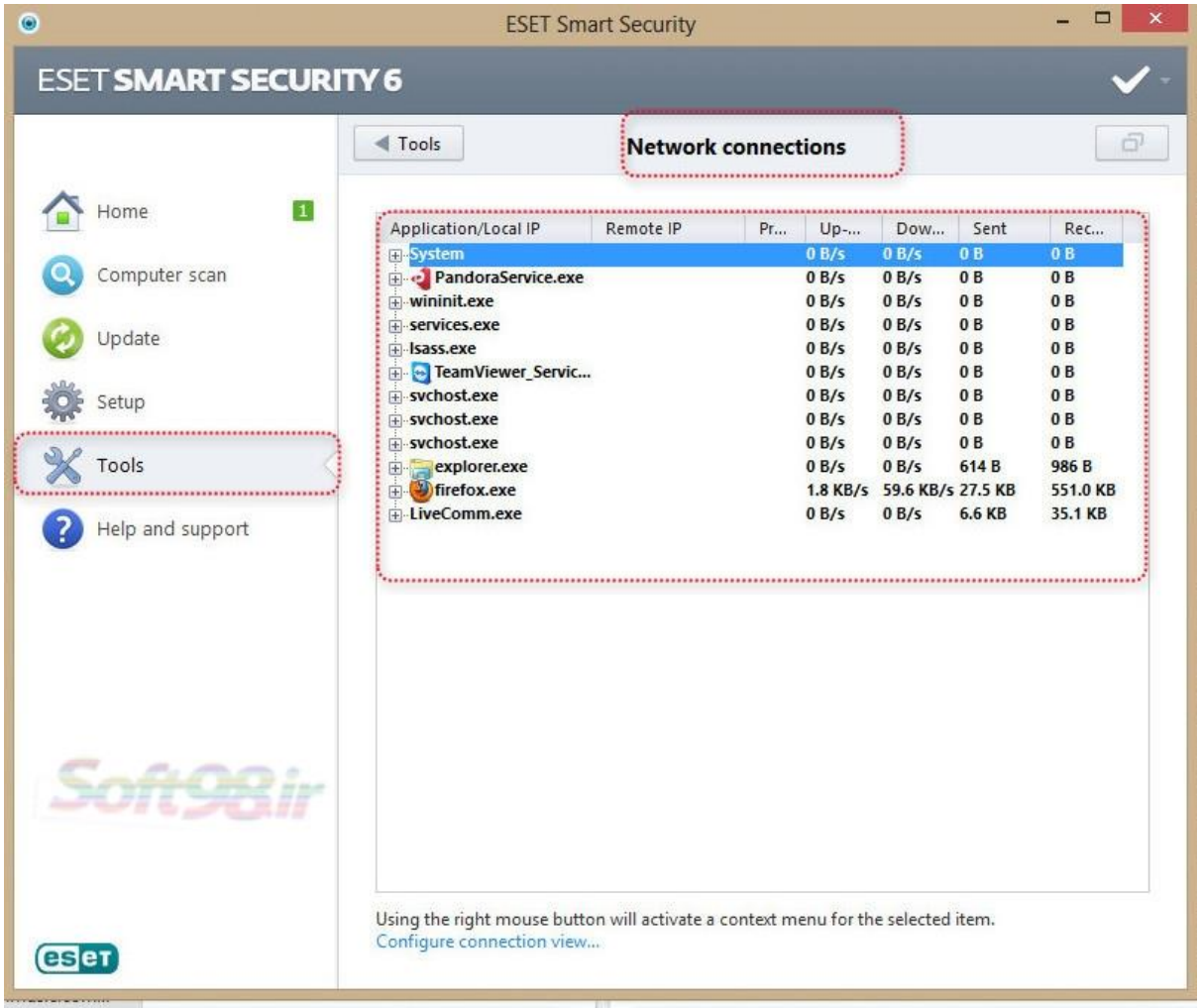
Running processes برنامه های در حال اجرا و پروسه های روی کامپیوتر را نمایش می دهد و ESET به طور مداوم اطلاعات انواع آلودگی های جدید را روی خود نگاه میدارد.ESET Smart Security برای محافظت از کاربران ،اطلاعات دقیق در مورد فرآیندهای در حال اجرا را با فن آوری ESET Live Grid فراهم می کند.



www.ParsBook.org

Network Connections –8

در بخش Network connections ، شما می توانید لیستی از اتصالات فعال و در انتظار را ببینید . با این ویژگی می توان برقراری ارتباط خروجی تمام برنامه های کاربردی را کنترل کنید.



www.ParsBook.org

Submit file for analysis -9

اگر در نظر دارید که فایل مشکوکی به لابراتوارهای"ESET" ارسال کنید باید از این گزینه استفاده کنید.
هنگام ارسال از شما یک آدرس ایمیل خواسته میشود که در کنار فایلهای مشکوک به"ESET" ارسال می گردد تا اگر شرکت"ESET" نیاز به جزئیات بیشتری جهت تجزیه و تحلیل آیتم های دریافتی داشت، از طریق این آدرس بتواند با کاربر ارتباط برقرار نماید . توجه داشته باشید که صرفا این آدرس در زمان نیاز به اطلاعات بیشتر از طرف"ESET" مورد استفاده قرار می گیرد و لذا در شرائط معمول جوابی در پاسخ اطلاعات فرستاده شده برای کاربر ارسال نخواهد گردید چون روزانه فایلهای متعددی به "ESET" ارسال میشود و آنها قادر به پاسخگوئی به تمامی کاربران نیستند.

Eset Social Media Scaner -10

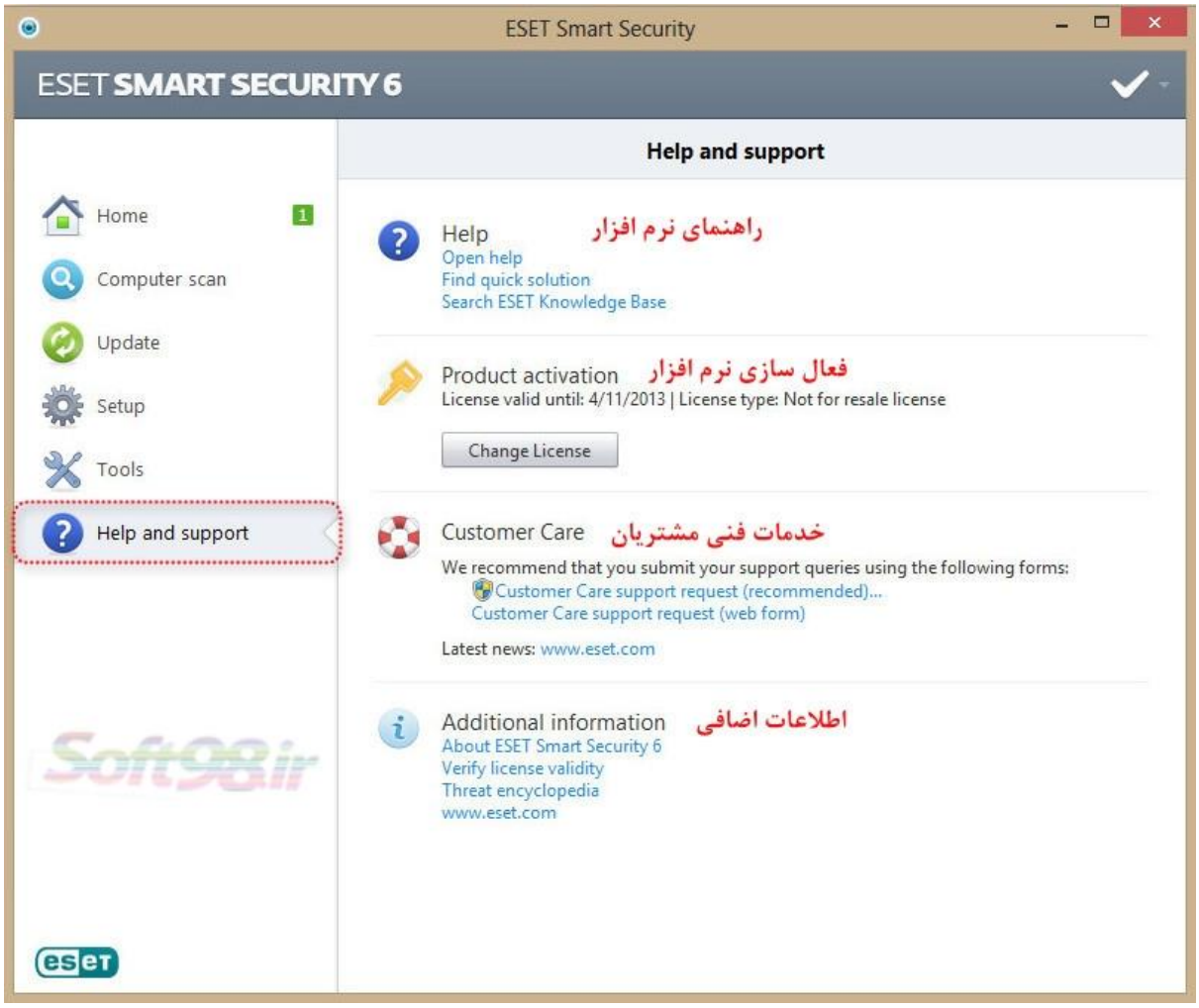
ESET Social Media Scanner لینک به یک برنامه ی رسانه های اجتماعی (مانند فیس بوک) داده شده است و برای محافظت کاربران رسانه های اجتماعی در برابر تهدیدات می باشد .این برنامه مستقل از دیگر محصولات امنیتی ESET است .

Eset SysRescue -11

در مواقعی که سیستم شدیدا آلوده است و آنتی ویروس بخوبی نمیتواند عمل اسکن و پاکسازی را انجام دهد بهترین گزینه اقدام به پاکسازی سیستم از ویروسها در حالت Boot است.پس از ساخت آن هم میتوان دیسک را آپدیت نمود.
برای ساخت دیسک نجات بخش Rescue Disk باید .Windows Automated Installation Kit (Windows AIK) نصب باشد که در لینک زیر قابل دانلود می باشد.

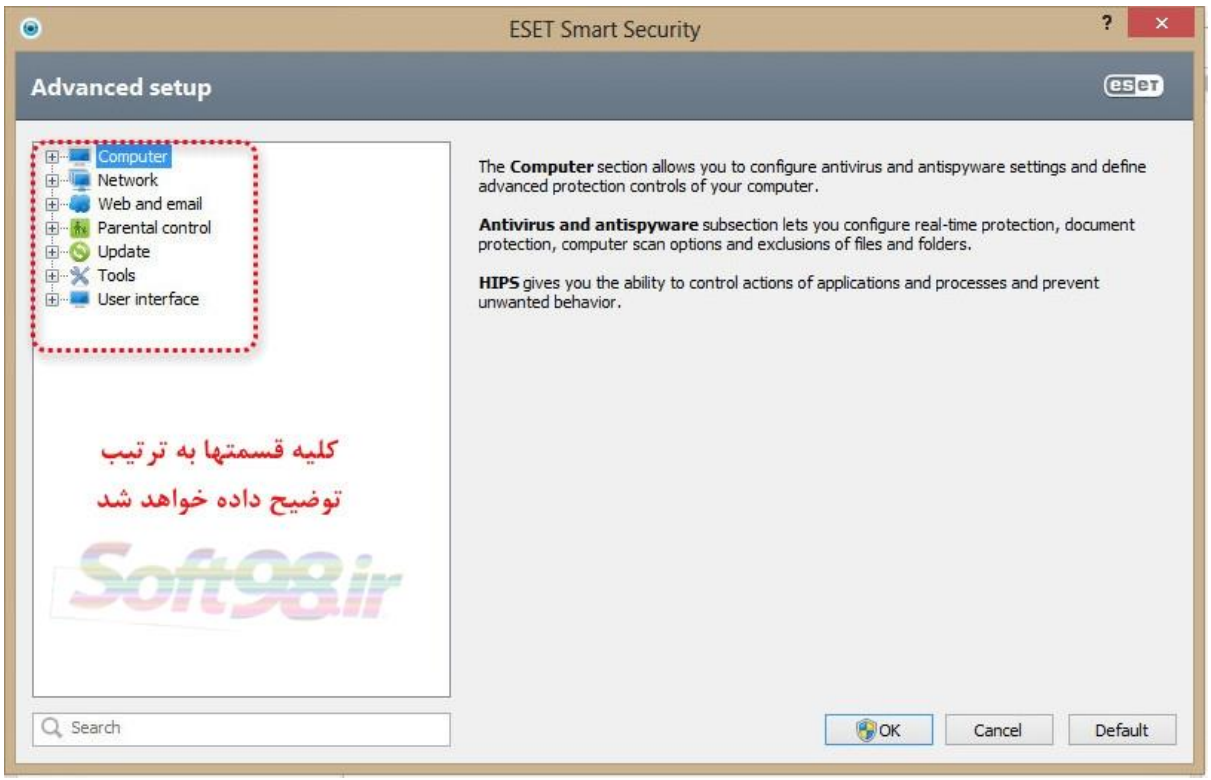
http://go.eset.eu/AIK

نکته: این قابلیت در ویندوز ۸ فعال نمی باشد و قرار است در آپدیتهای بعدی اضافه شود.


ESET Smart Security
ESET SMART SECURITY 6
Home
1
Computer scan
Update
Setup
Tools
Help and support
Help and support
Help
راهنمای نرم افزار
Open help
Find quick solution
Search ESET Knowledge Base
Product activation
فعال سازی نرم افزار
License valid until: 4/11/2013 | License type: Not for resale license
Change License
Customer Care
خدمات فنی مشتریان
We recommend that you submit your support queries using the following forms:
Customer Care support request (recommended)...
Customer Care support request (web form)
Latest news: www.eset.com
Additional information
اطلاعات اضافی
About ESET Smart Security 6
Verify license validity
Threat encyclopedia
www.eset.com
Soft98.ir
eset

تنظیمات پیشرفته Advanced Setup

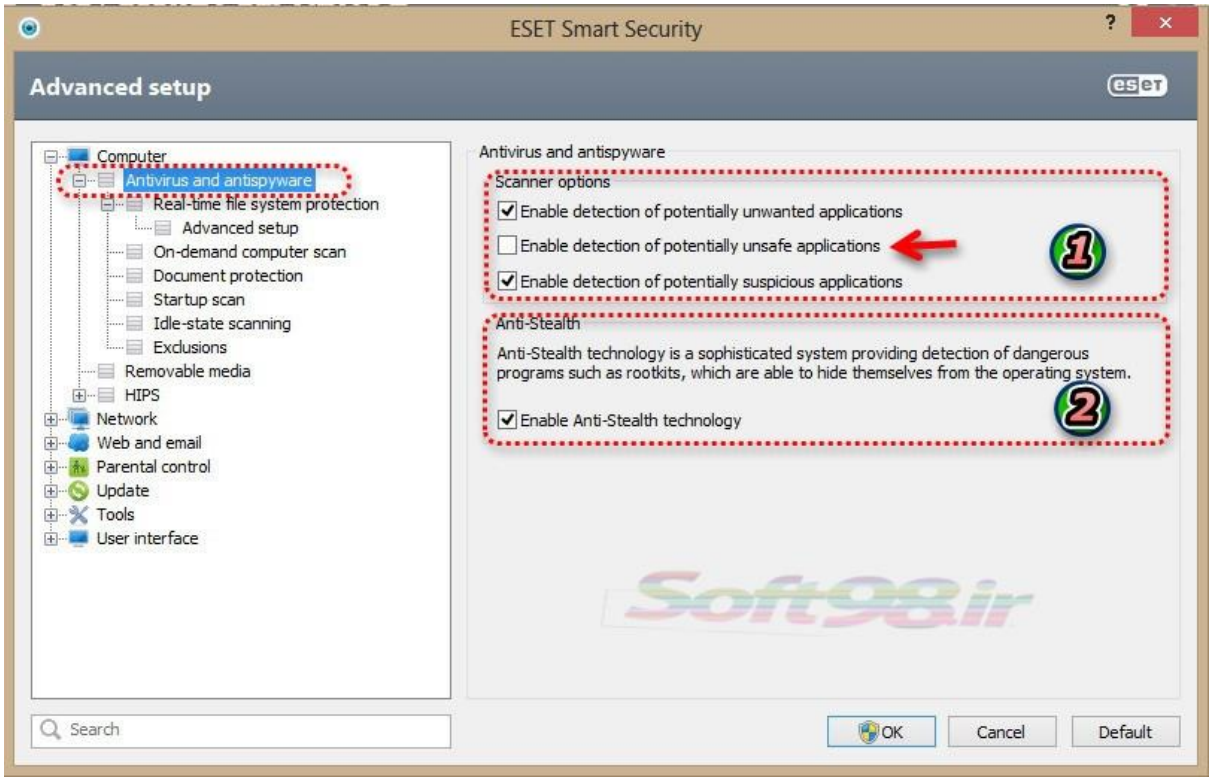
برای ورود به صفحه تنظیمات پیشرفته کلید F5 را بزنید.



www.ParsBook.org

تنظیمات مربوط به قسمت Computer

Antivirus and Antispyware



۱- گزینه های اسکنر(scanner options)

۱-۱-برنامه های بالقوه ناخواسته

بخشی ازگارد آنتی ویروس را فعال می کند که وظیفه آن مقابله با برنامه هائی است که برای مقاصد تجاری و غیرقانونی سعی در کسب اطلاعات شخصی و سیستمی کاربر میکند از جمله معروفترین این مخربها Keyloggerها هستند.

-۱

۱-۲- برنامه های بالقوه ناامن

گزینه Enable detection of potentially unsafe application که با فلش قرمز مشخص شده است منظور برنامه هایی که به صورت بالقوه ناامن هستند. منظور از نرم افزارهای به صورت بالقوه ناامن عبارت از نرم افزارهایی است که جزء کدهای مخرب محسوب نمی شوند ولی وجود آنها می تواند ناامن باشد . به عنوان مثال می توان به نرم افزارهای دسترسی از راه دور اشاره کرد.

۱-۳-برنامه های مشکوک

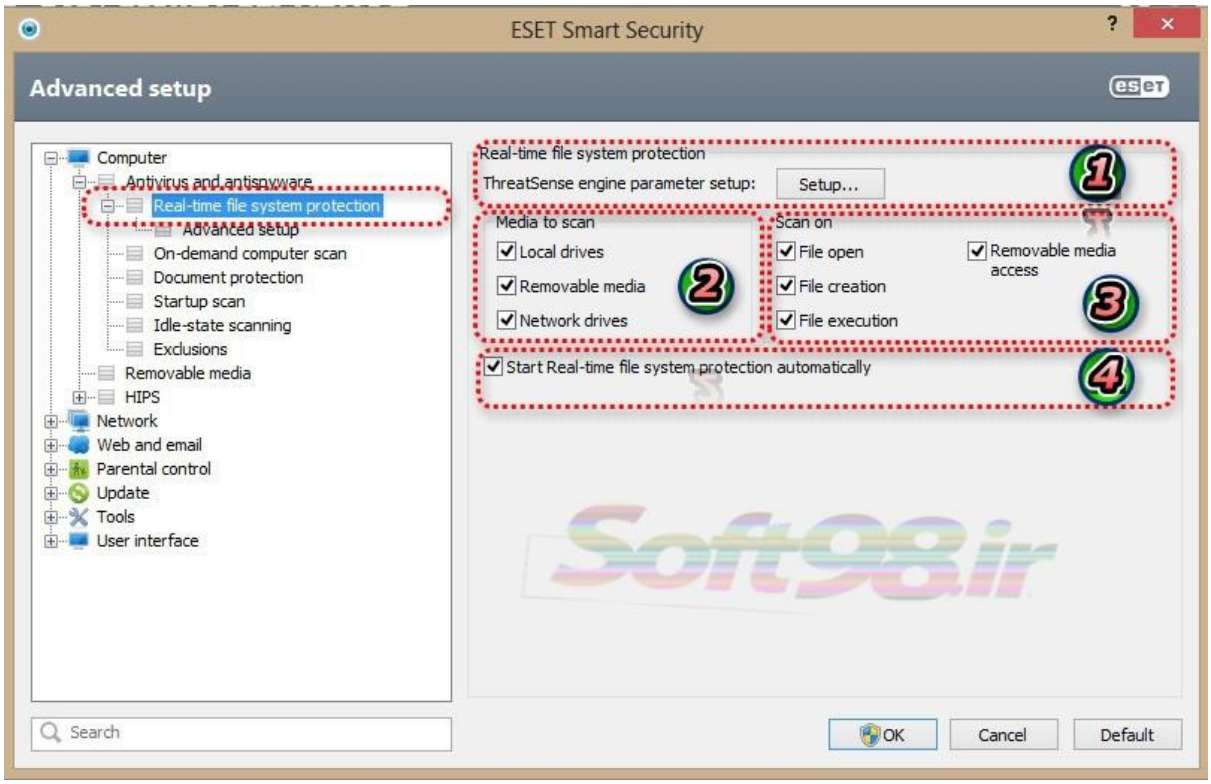
۲- ضد خفا (Anti-stealth)

تکنولوژی ضد مخفیکاری یک سیستم پیچیده تشخیص برنامه های خطرناک مانند روت کیت ها است، که می توانند خود را از سیستم عامل پنهان کنند که تشخیص آنها با استفاده از تکنیک های تست معمولی امکان پذیر نیست.

www.ParsBook.org

Real-time file system Protection

حفاظت"real–time" از سیستم فایلها به معنی کنترل تمامی رخدادهایی در رایانه است که با ماژول ضدویروس ارتباط دارند حفاظت"real–time" ، از سیستم فایلها (گارد نرم افزار) تمامی واحدهای حافظه (فلش و هاردهای اکسترنال و...) را به لحاظ وجود آلودگی ویروسی مورد بررسی قرار می دهد و رخدادهای گوناگون مرتبط با تهدیدات رایانه ای بر نوع این کنترل تاثیر می گذارند .سیستم کنترل نرم افزار از روش های شناسایی مربوط به فناوری"ThreatSense"بهره می جوید .ضمن اینکه رفتار سیستم کنترلی می تواند در مواجه با فایلهای موجود و فایلهایی که اخیرا ایجاد گردیده اند، متفاوت باشد.



توضیحات مربوط به شکل:

۱- توضیحی مختصر در مورد فناوری "ThreatSense" :

"ThreatSense" نام فناوری ای است که از مجموعه ای از روش های شناسایی تهدیدات رایانه ای تشکیل یافته است . این فناوری از نوع حفاظت پیش گیرانه است . به بیان دیگر با استفاده از این فناوری در ساعات اولیه شیوع یک تهدید رایانه ای نیز کاربران دارای نوعی حفاظت پیش گیرانه (با استفاده از ابزار هوش مصنوعی) خواهند بود.

همانطور که عنوان گردید در این فناوری از روشهای متعددی نظیر روش بررسی کدها، نمونه سازی کدها، شناسه های "generic"یا نوعی و همچنین بانک اطلاعاتی شناسه ویروسهای رایانه ای استفاده به عمل آمده است تا بتوان با استفاده از این روشها در کنار یکدیگربه یک سطح حفاظت رایانه ای بالا دست یافت . ضمن اینکه موتور این فناوری قادر است به طور همزمان چندین رشته از اطلاعات راکنترل نماید و این موضوع باعث افزایش نرخ آشکارسازی تهدیدات رایانه ای و تاثیرگذاری می گردد . نکته دیگر اینکه می توان از فناوری"ThreatSense" جهت مقابله با "rootkit" ها نیز بهره جست.

از این سیستم همچنین جهت ارسال تهدیدات جدید به لابراتوار شرکت"ESET" استفاده به عمل می آید .در این لابراتوار تهدیدات جدید مورد تحلیل و پردازش قرار گرفته و سپس به بانک اطلاعاتی شناسه ویروسهای رایانه ای نرم افزارهای شرکت "ESET" افزوده می گردند.

جهت دسترسی به تنظیمات پیشرفته این سیستم به منظور ارسال فایلهای مشکوک به آلودگی به سایت شرکت"ESET" می توانید بر روی گزینه setup کلیک کنید.

www.ParsBook.org

۲- آیتمهای مورد نظر جهت اسکن(Media to scan)

۱-هارد دیسک کامپیوتر

۲- حافظه های قابل حمل نظیر فلش ها،هاردهای اکسترنال و حافظه های دارای پورتUSB و ...

۳- درایوهای شبکه ای(Network drives)

۳- اسکن در زمان بروز یک رخداد(scan on)

به صورت پیش فرض تمامی فایلها در زمان باز شدن(file open) و ایجاد(file creation)و اجرا(file execution) و (removeable media access) مورد اسکن قرار می گیرند .توصیه می شود از تنظیمات پیش فرض مربوطه استفاده شود .زیرا حداکثر سطح حفاظتی را برای رایانه تضمین خواهد کرد.

۴- فعال شدن "real–time" از هنگام system startup

تمامی فایلها در زمان ایجاد و یا اجرا به لحاظ وجود آلودگی ویروسی مورد اسکن قرار می گیرند.

حفاظت "real–time" از سیستم، از زمان راه اندازی رایانه(system startup) اجرا میشود.

پارامترهای موتور ThreatSense

Objects

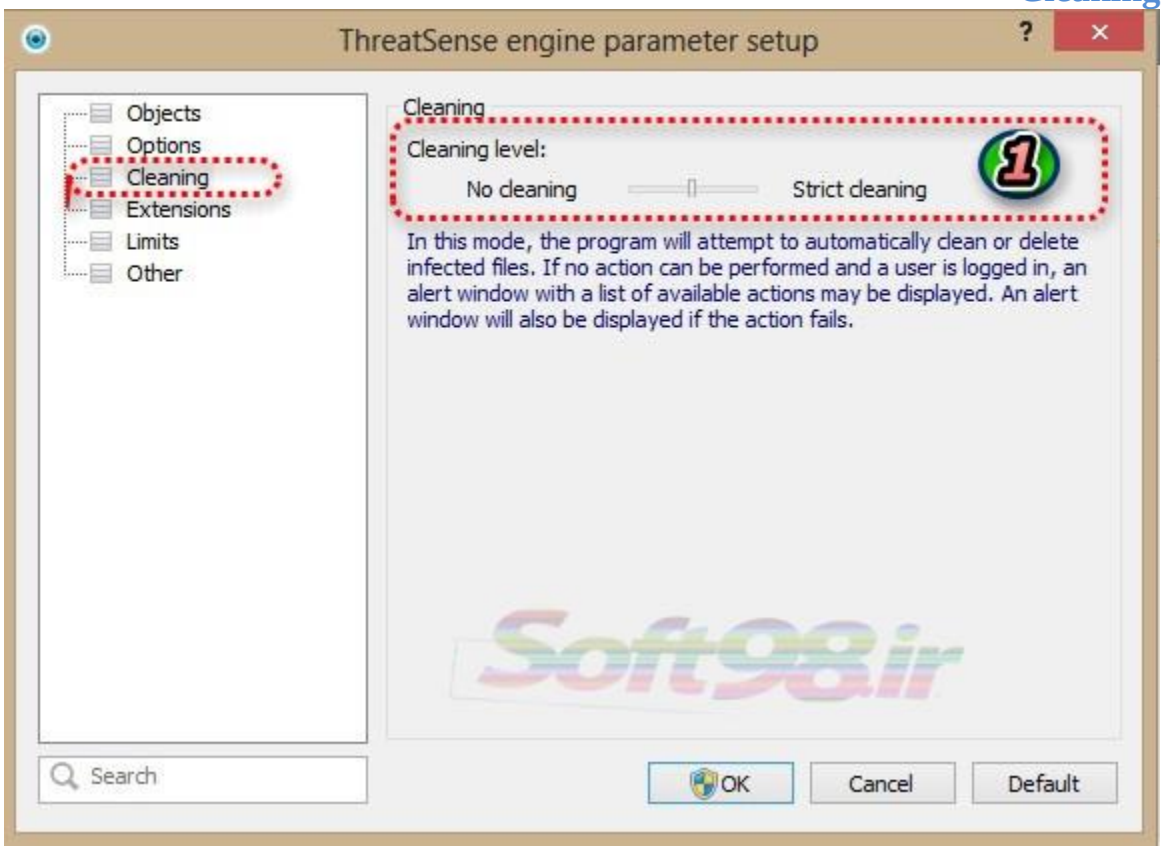
www.ParsBook.org

Option

سطوح پاکسازی آیتم های دارای آلودگی ویروسی

حفاظت"real–time" دارای سه سطح پاکسازی است . برای مشاهده و دسترسی به این سطوح می توان پس از کلیک بر روی گزینه"setup…" در قسمت"real–time file system protection" ، به قسمت"cleaning" مراجعه کنید.

Cleaning



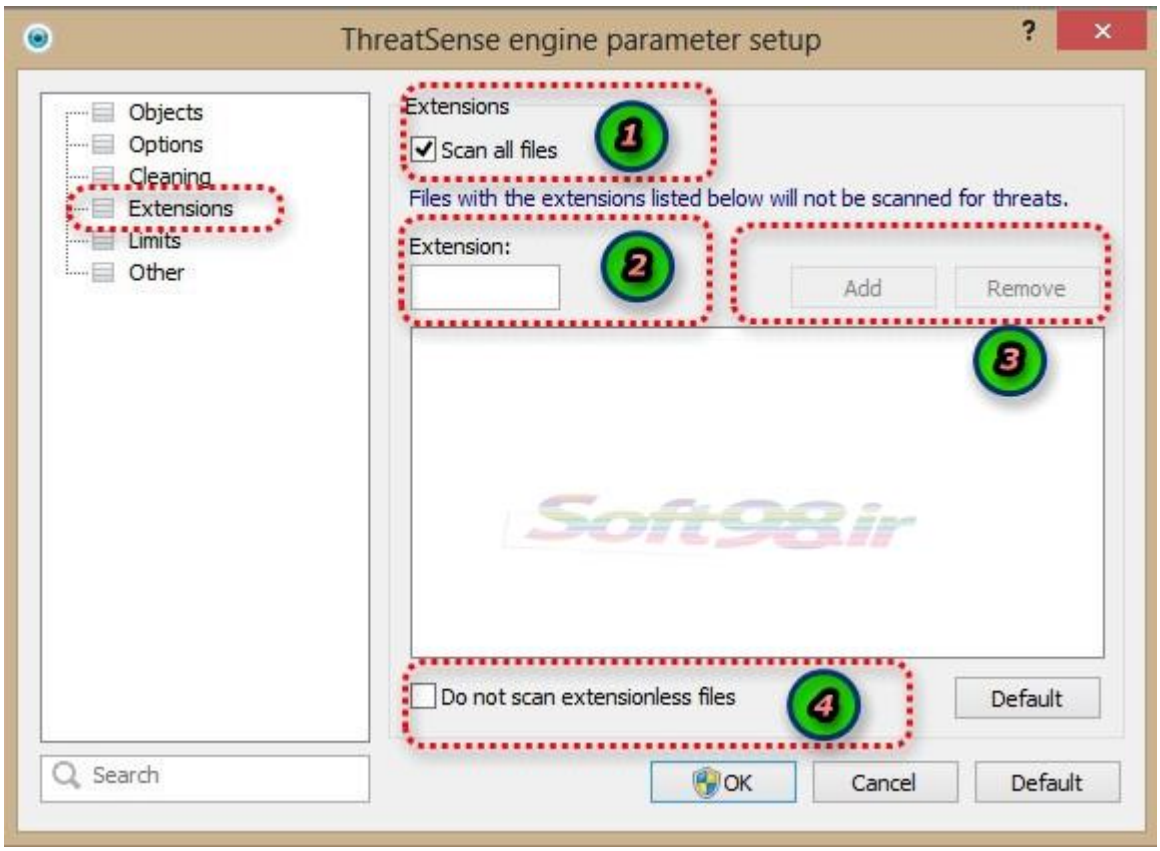
www.ParsBook.org

اولین سطح عبارت از نمایش پنجره هشدار به همراه دیگر گزینه ها جهت مقابله با تهدید شناسایی شده است . لذا کاربر باید یکی از روش های مقابله ای ارائه شده را برای هر یک از تهدیدات شناسایی شده برگزیند . این گزینه مناسب کاربران حرفه ای است که با گام های مختلف مبارزه با تهدید رایان های آشنایی کامل دارند.

سطح دوم، سطح پیش فرض نرم افزار است . در این حالت نرم افزار روش مقابله ی از پیش تعیین شده را، در مورد تهدید شناسایی شده به صورت خودکار اعمال می کند .شناسایی و پاک نمودن فایل آلوده نیز طی یک پنجره کوچک که در گوشه پائین سمت راست صفحه نمایش قابل رویت خواهد بودو به اطلاع کاربر میرسد.با این حال توجه داشته باشید که اگر تهدید شناسایی شده در یک فایل آرشیو دارای فایلهای غیر آلوده باشد و یا روش از پیش تعیین شده ای برای مقابله با آن تهدید تعیین نگردیده باشد، مقابله خودکار با آن تهدید انجام نخواهد پذیرفت.

سطح سوم سطح تهاجمی تری است . در این سطح تمامی آیتم های دارای آلودگی ویروسی مورد پاکسازی قرار خواهند گرفت . لذا از آنجا که ممکن است به صورت بالقوه در این سطح اطلاعات معتبر کاربر نیز از بین برود،توصیه می شود از سطح مورد نظر در شرایط بسیار ویژه استفاده گردد.

Extensions



همانطور که می دانیم هر فایل رایانه ای دارای یک پسوند خاص است که این پسوند بیانگر نوع و محتو ای آن فایل میباشد.

۱-در صورتی که "scan all files" تیک داشته باشد تمامی فایلها با تمامی پسوندها، مورد اسکن قرار میگیرد ولی در صورتی که"scan all files" تیک نخورده باشد ،پسوندهاي موجود در فهرست زیر آن ،تبدیل به گزینه هایي میشوند که توسط نرم افزارمورد اسکن قرار خواهد گرفت.

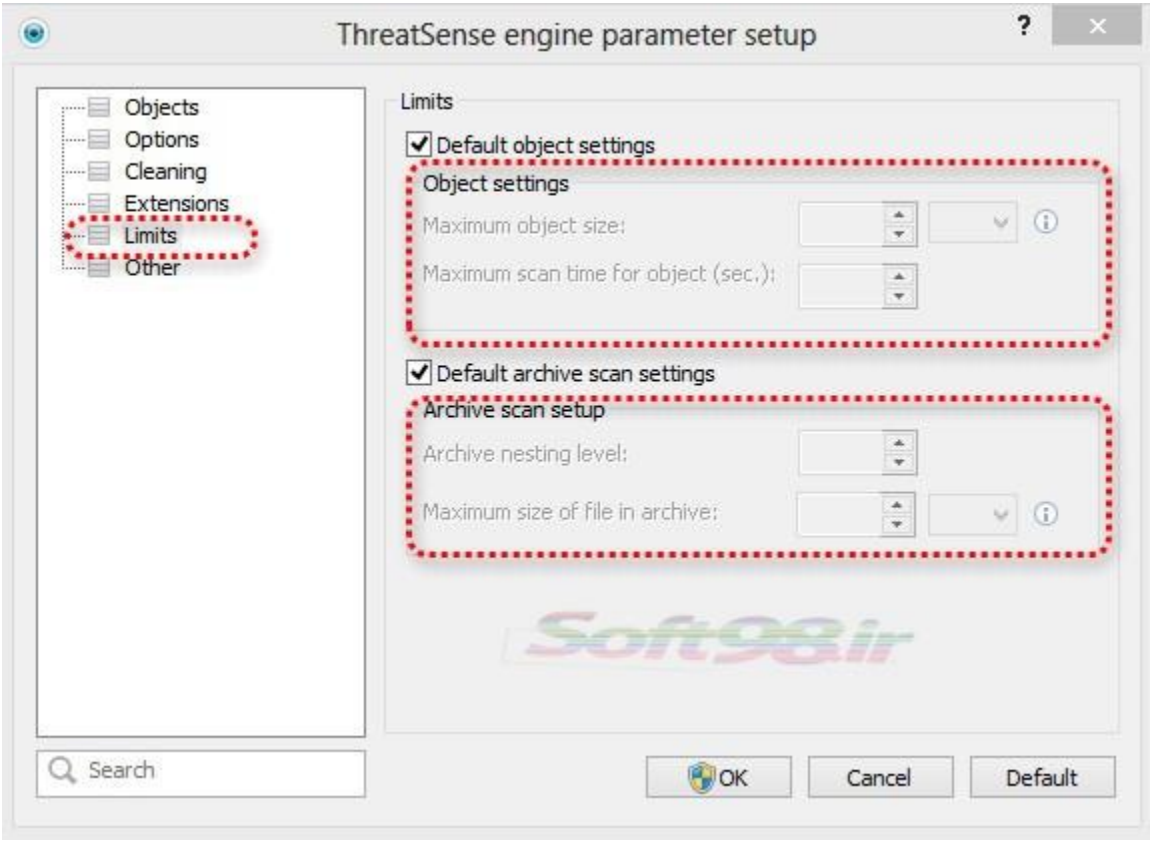
۲-محل وارد کردن پسوند

۳- کاربر با استفاده از دکمه هاي "remove" و"add" میتواند پسوندهاي مورد نظر خود را جهت اسکن و یا عدم اسکن مشخص کند.

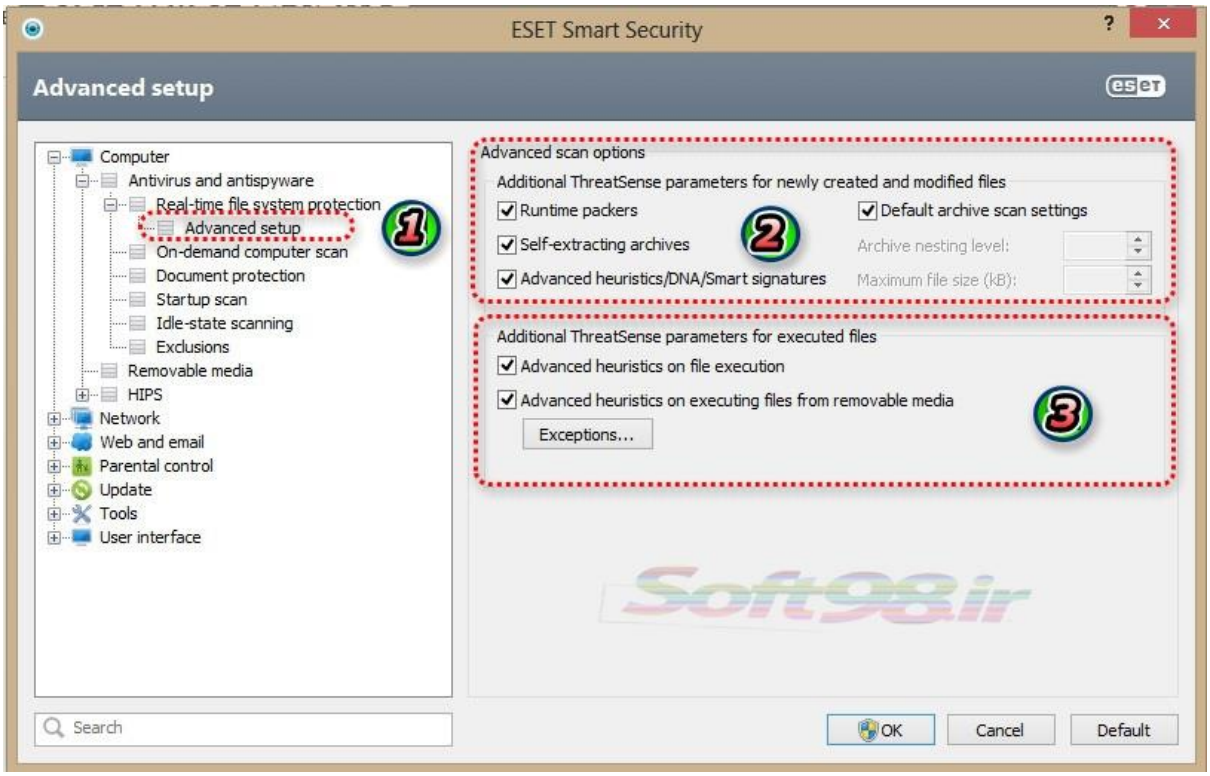
۴-با زدن تیک این قسمت فایلهای با پسوند لیست مورد اسکن قرار نمیگیرند.

www.ParsBook.org

Limits



جهت ایجاد محدودیت در فایهائی که مورد اسکن قرار می گیرند.



۱- Advanced setup:

تنظیمات پیشرفته

www.ParsBook.org

۲- گزینه های اسکن پیشرفته

همانگونه که می دانید احتمال آلودگی فایلهای که اخیرا ایجاد شده اند در مقایسه با فایلهای موجود دیگر بسیار بیشتر است لذا دلیل اصلی اینکه این فایلها با پارامترهای اسکن بیشتری کنترل می شوند نیز همین مسئله است . در نتیجه علاوه بر روشهای اسکن مبتنی بر بانک اطلاعاتی شناسه ویروسها از روشهای پیشگیرانه هوش مصنوعی نیز استفاده به عمل می آید تا نرخ آشکار سازی این قبیل تهدیدات نیز افزایش یابد.

علاوه بر فایلهایی که اخیرا ایجاد گردیده اند، اسکن فایل های آرشیو شده خود اجرا(self–extracting files) و همچنین "runtime packer"وAdvanced heuistics/DNA/Smart signatures نیز انجام میشود.

با بر داشتن تیک گزینه Default archive scan setting میتوان تنظیمات دستی جهت اسکن فایلهای آرشیو اعمال کرد.

(از جمله ایجاد محدودیت حجم فایلهای که مورد اسکن)

۳- پارامترهای تکمیلی "ThreatSense" برای فایلهای اجراشده:

advanced heuristics on file execution

با تیک دار بودن این گزینه تمامی فایلهای در حال اجرا را زیر نظر میگیرد.

این هوش مصنوعی از الگوریتم شناسائی خاصی جهت شناسائی مخربهای جدید و ناشناخته است.

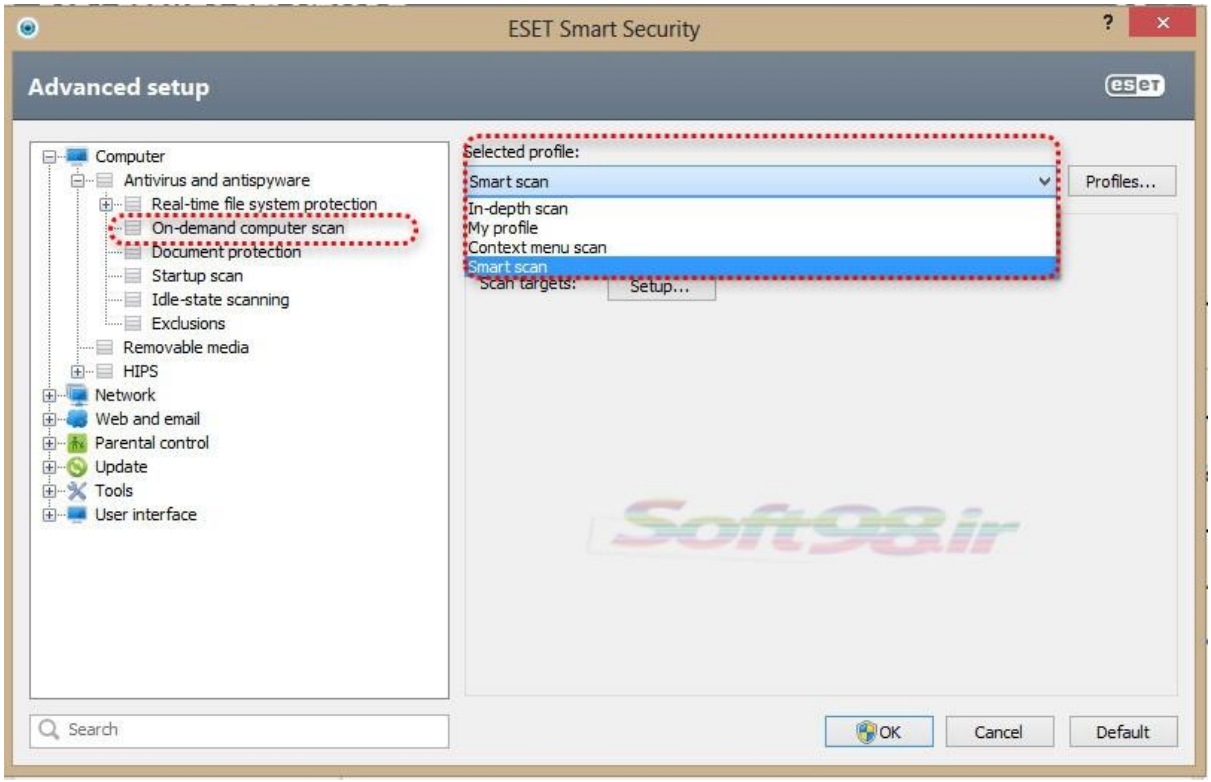
advanced heuristics on executing file from removable media

با تیک دار بودن این گزینه تمامی فایلهای در حال اجرا را در وسایل removable زیر نظر میگیرد. در ضمن میتوان هر پورت را سفارشی کرد.

تیک داربودن این گزینه ها باعث افزایش قدرت آنتی ویروس میشود.

On-demand computer scan

www.ParsBook.org



۱- **In-depth scane** اسکن عمیق و دقیق

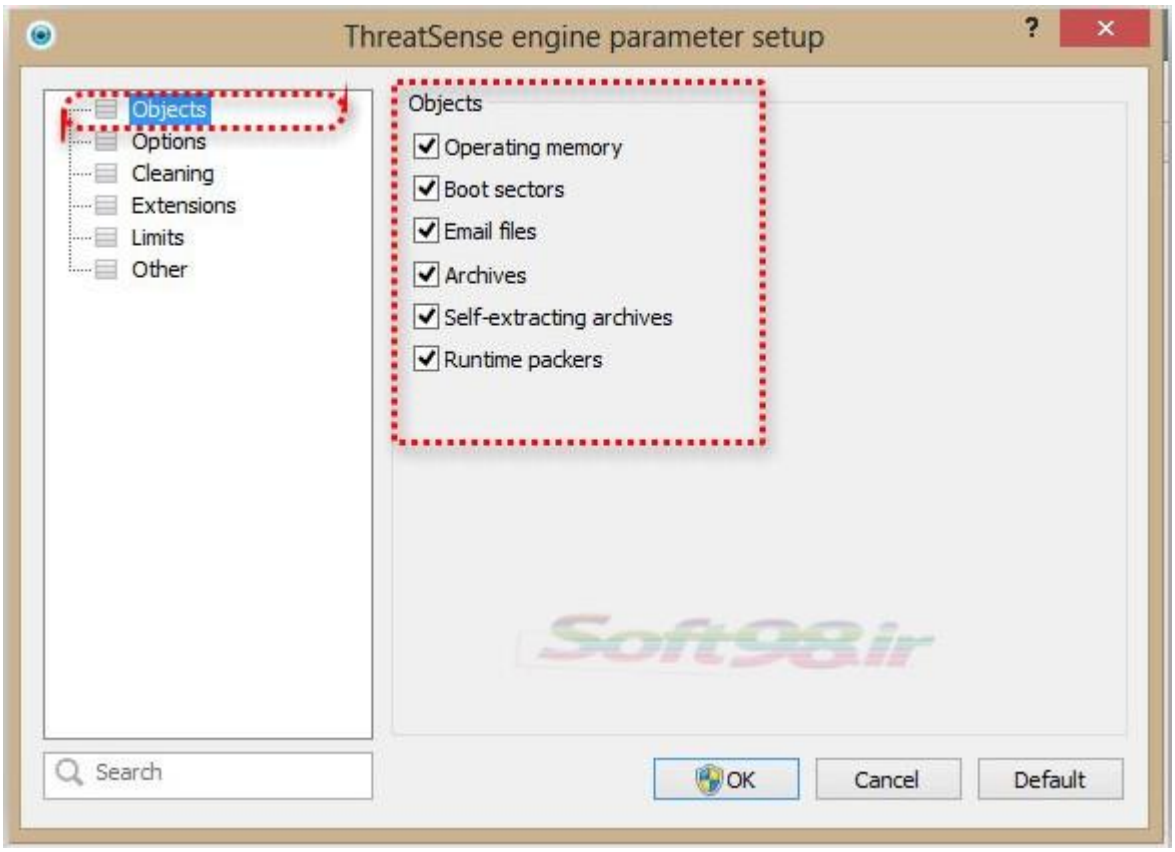
۲- **My profile** اسکن بصورت تنظیمات پروفایل شخصی

۳-**Context menu scan** تنظیمات درجه اسکن قرار گرفته در راست کلیک

۴- **Smart scan** اسکن سریع و هوشمند

فایلهای مورد اسکن :

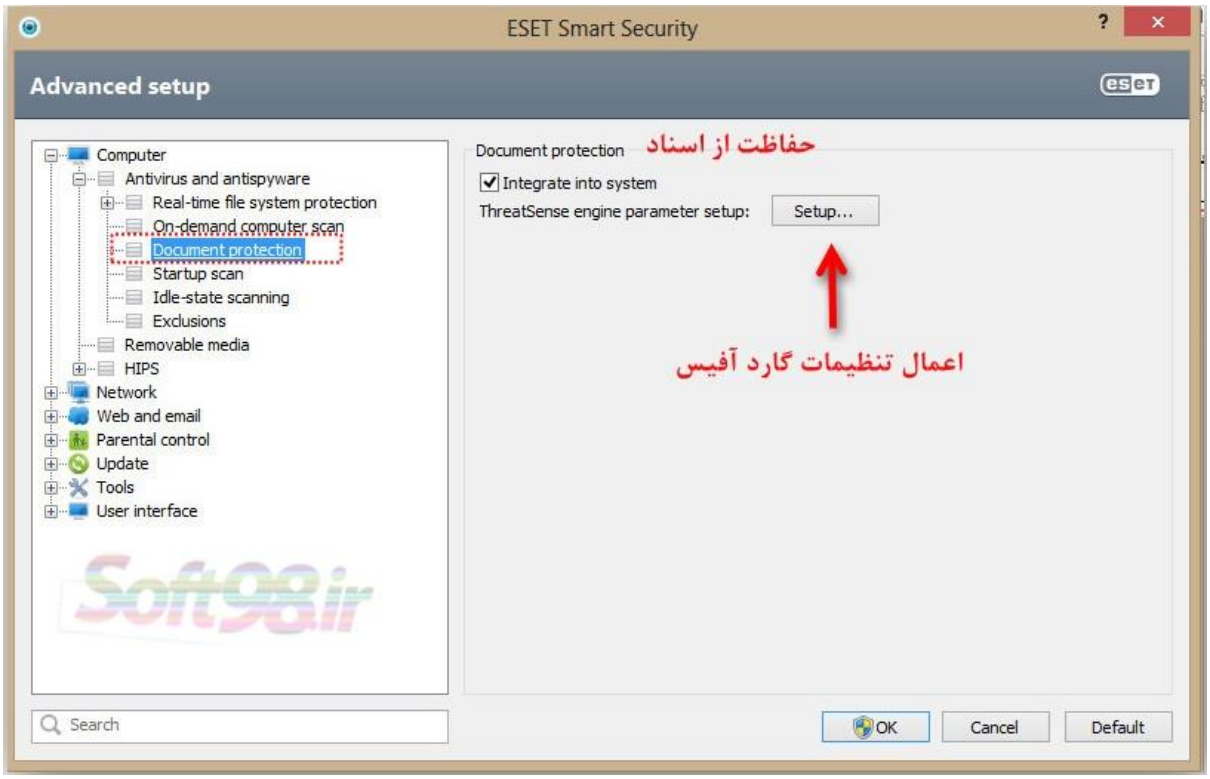
تنظیمات فایلها بر اثرنوع اسکن In-depth scane و My profile و Context menu scan و Smart scan



www.ParsBook.org

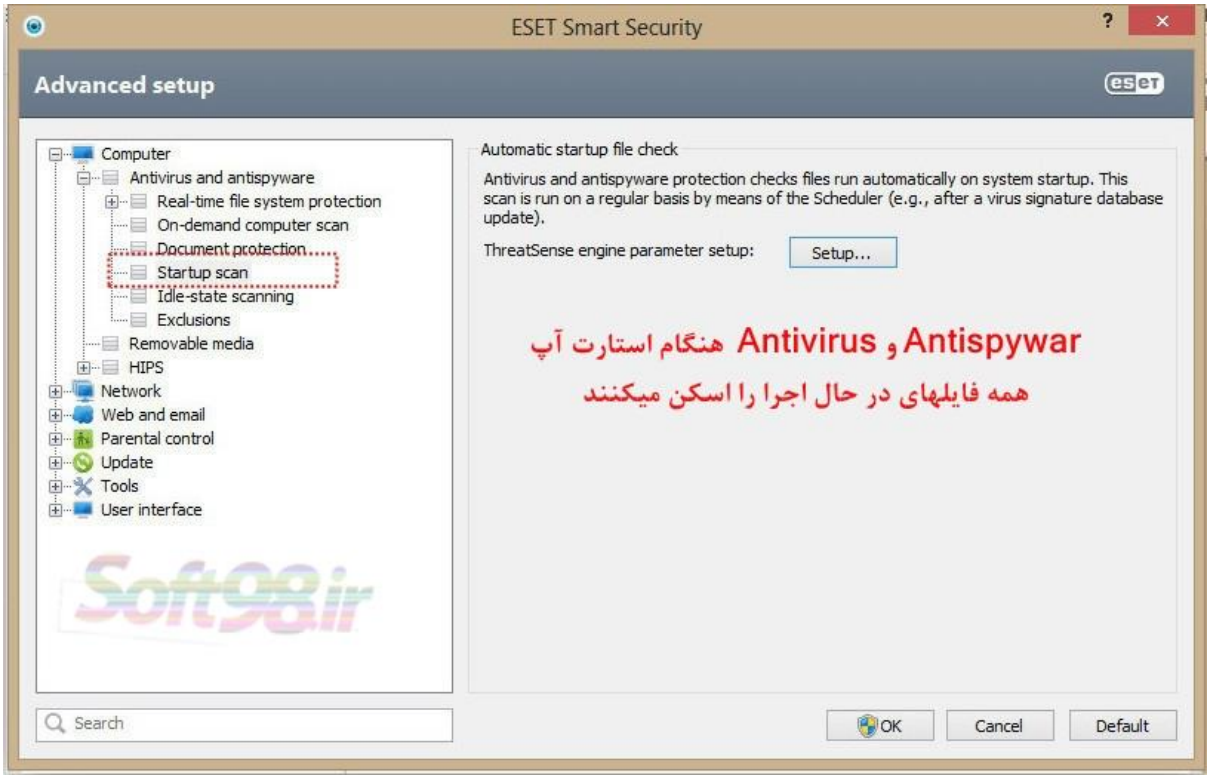
۱-حافظه اصلی(operating memory)
در زمان انتخاب این گزینه حافظه در حال کارکرد (منظورRAM است) سیستم مورد اسکن قرار میگیرد.
۲-سکتورهای راه اندازی (Boot sector)
۳- فایلهای موجود در نامه های الکترونیک
۴-فایلهای آرشیو
۵- فایلهای آرشیو شده خود اجرا
۶-"runtime packer"
اهدافی که باید مورد اسکن قرار بگیرند.

Document protection

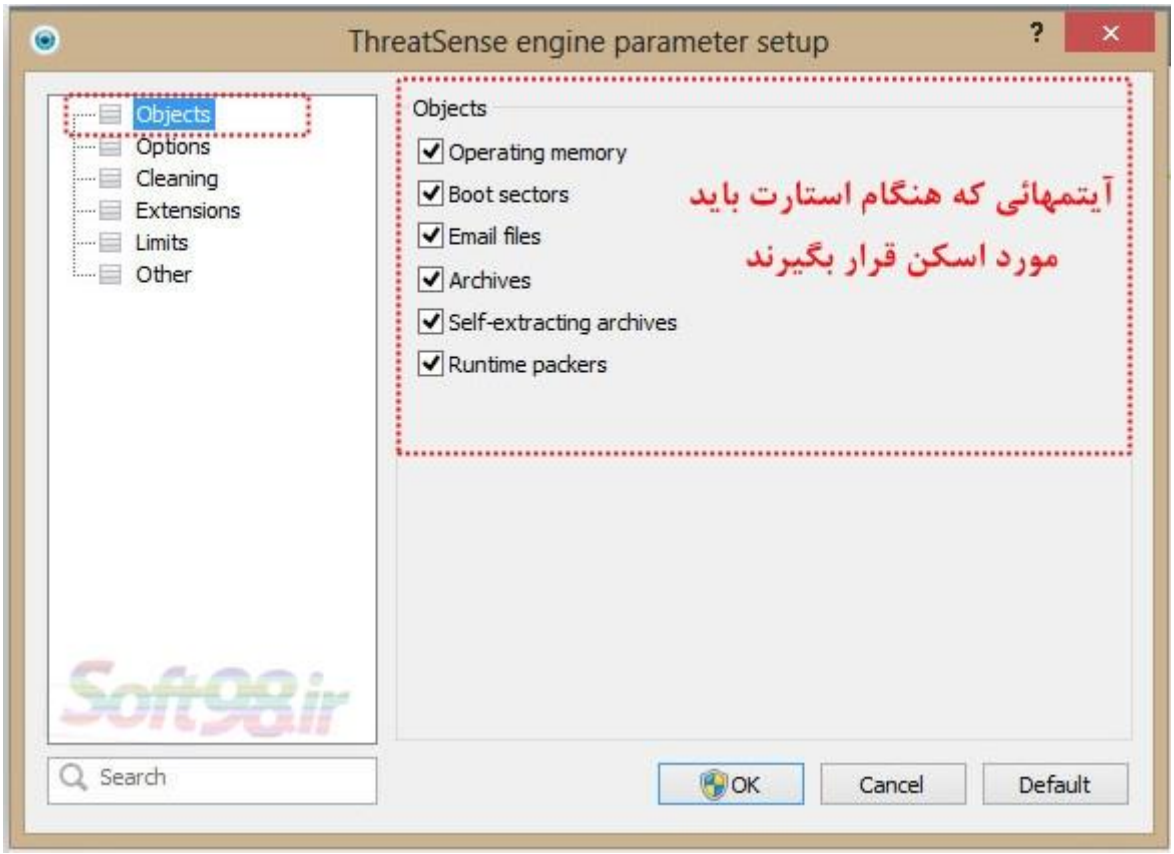


www.ParsBook.org

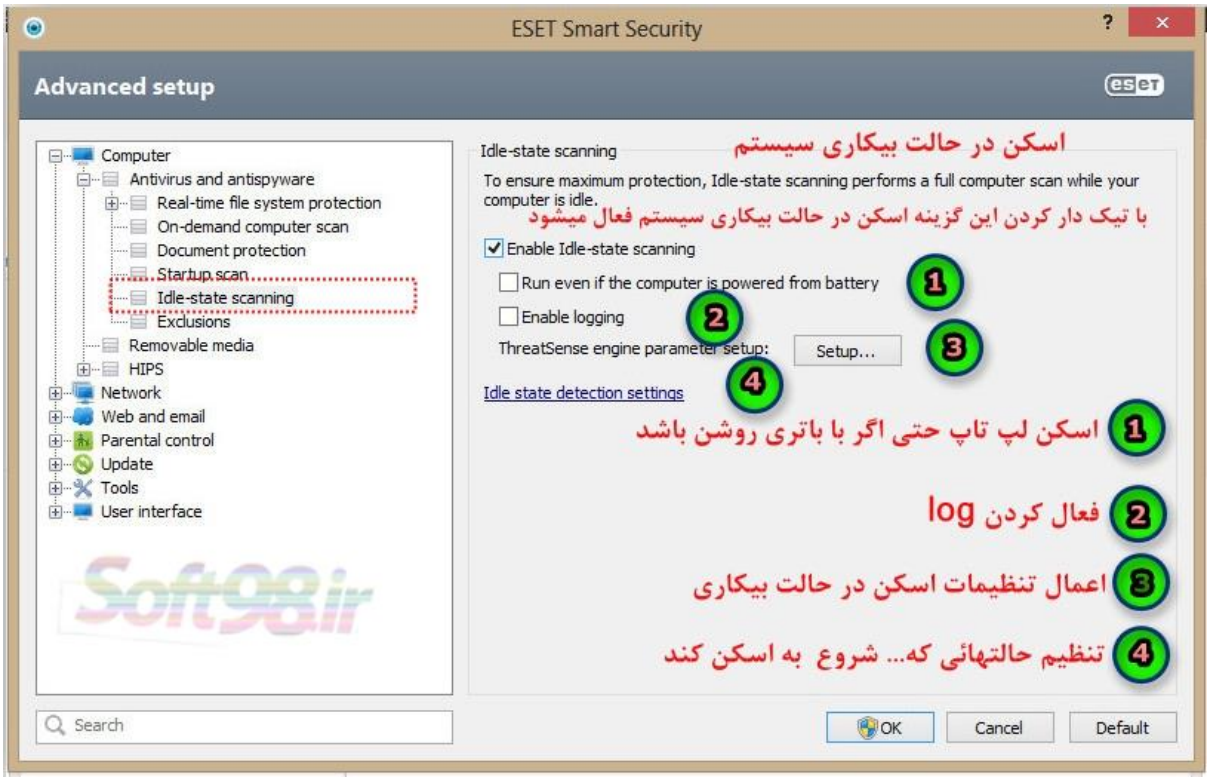
Startup scan



www.ParsBook.org



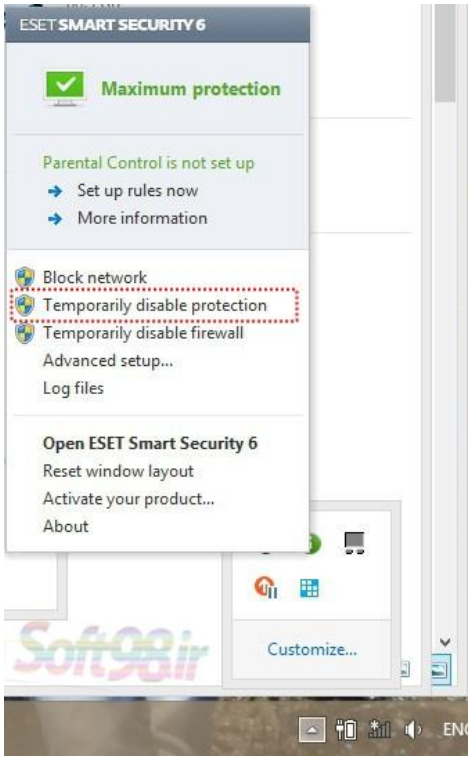
Idle-state scanning



www.ParsBook.org

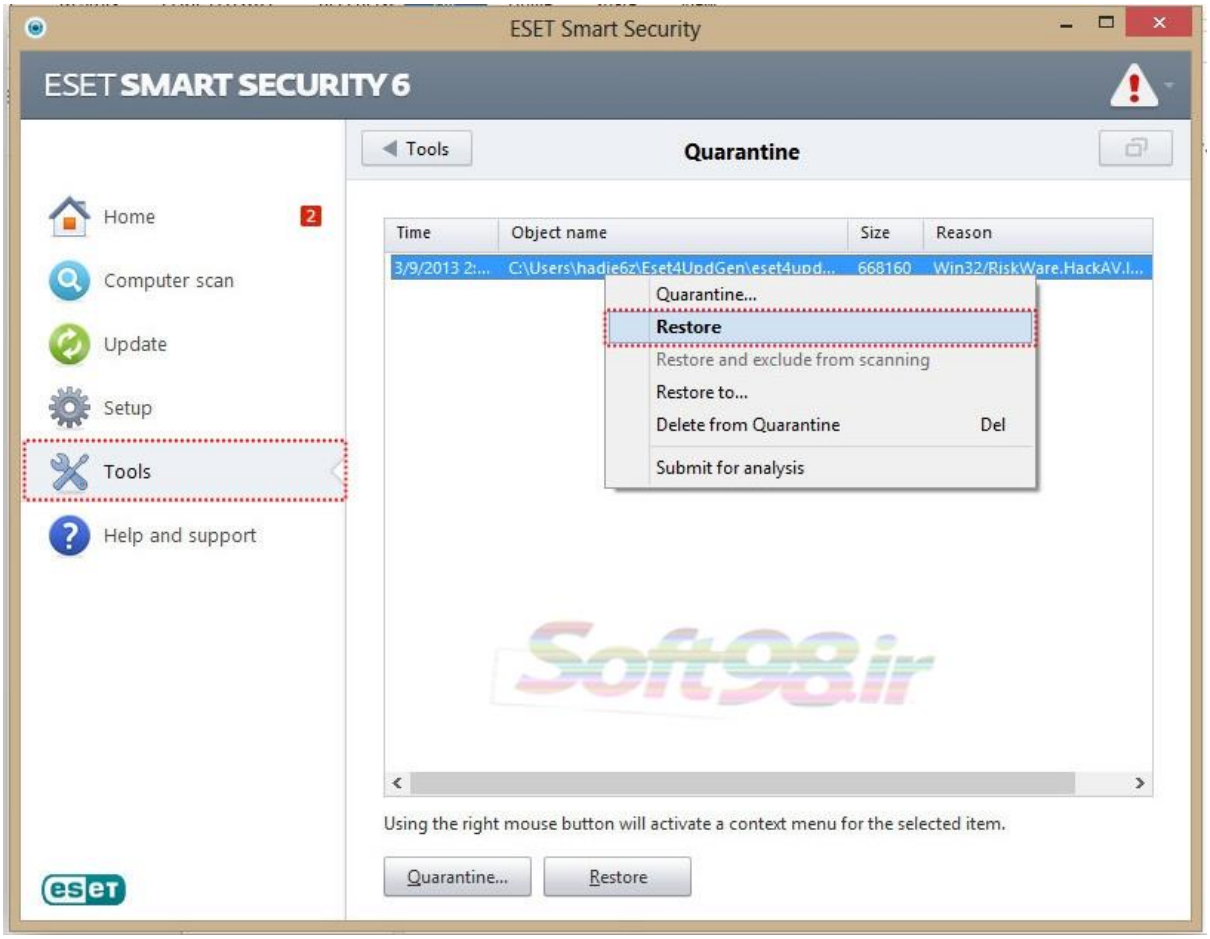
اعتماد سازی یک فایل به آنتی ویروس

آنتی ویروس معمولا با کرک و پچ ها میانه خوبی ندارد به همین جهت اقدام به پاکسازی و حذف آنها میکند. برای معرفی کردن یه 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 می باشد. برای این کار باید طبق اسکرین شات زیر عمل گردد.

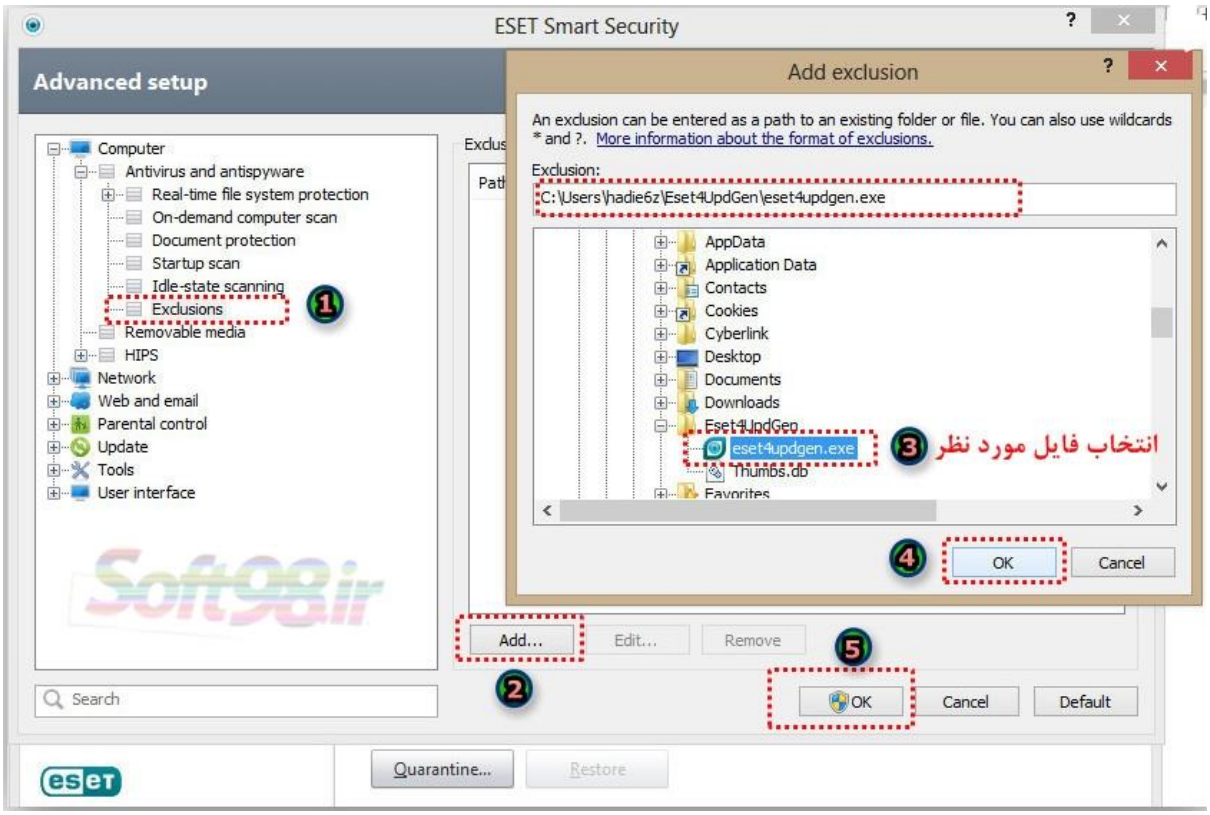


www.ParsBook.org

در مرحله بعدی اقدام به بازیابی فایل از قرینطینه میکنیم.

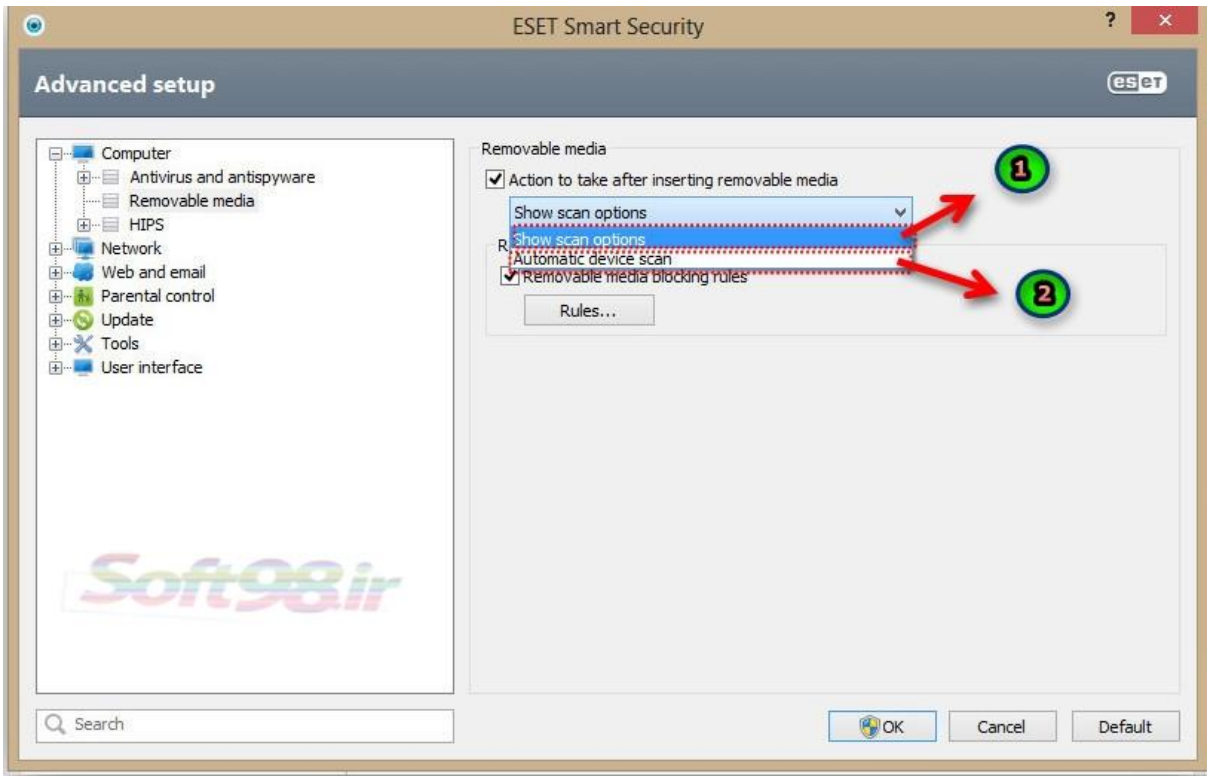


گام بعدی معرفی فایل به آنتی ویروس است.



www.ParsBook.org

Removable media

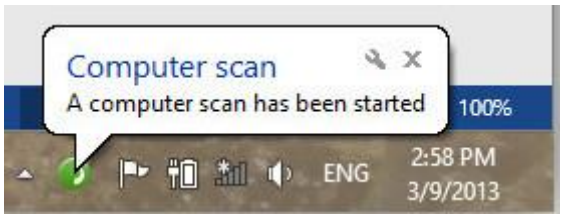


www.ParsBook.org

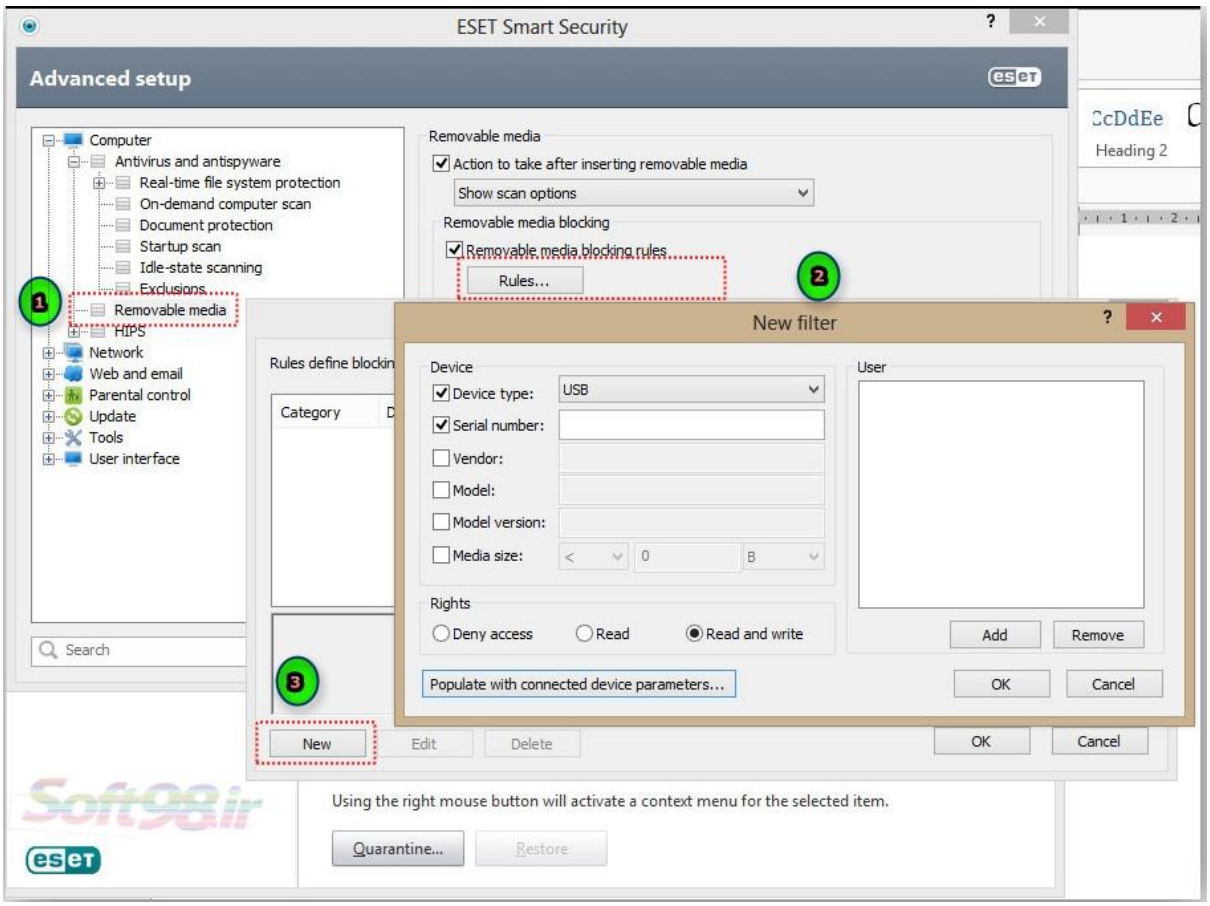
۱-پس از وصل وسایل Removable گزینه های اسکن را نشان میدهد.

البته گزینه ها بقدری واضح هستند که نیازی به توضیح نمی باشد.

۲-پس از وصل وسایل Removable آنتی ویروس بطور اتوماتیک شروع به اسکن میکند.

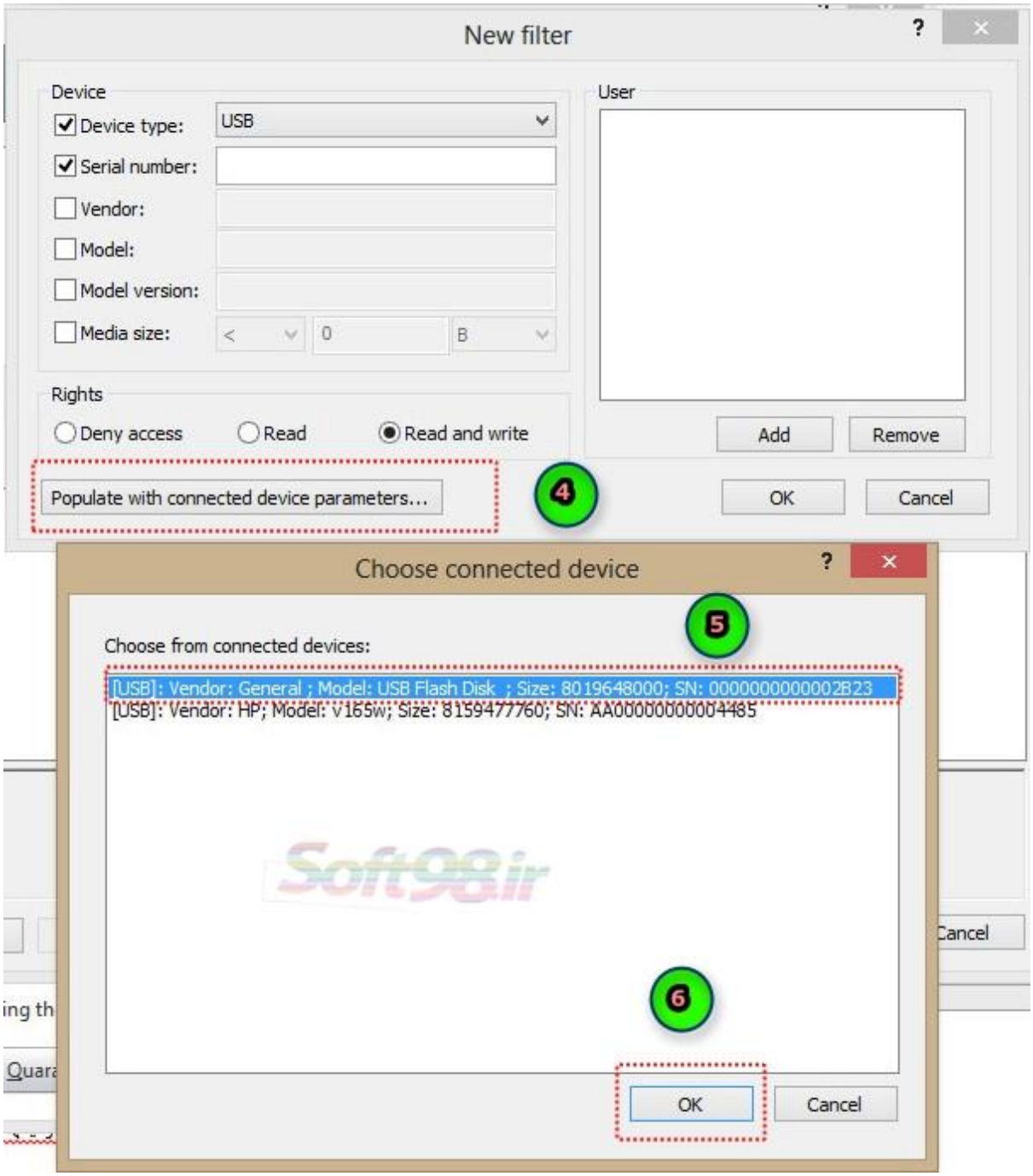


طریقه قفل کردن Removable media



www.ParsBook.org

در مرحله بعدی اگر وسیله ای وصل باشد(درحال حاضر دو فلش به سیستم خودم وصل است) میتوان وسایل را به آنتی ویروس معرفی کرد.



۷-در مرحله بعدی میتوان محدودیتهای لازم را به وسیله مورد نظر اعمال کرد.

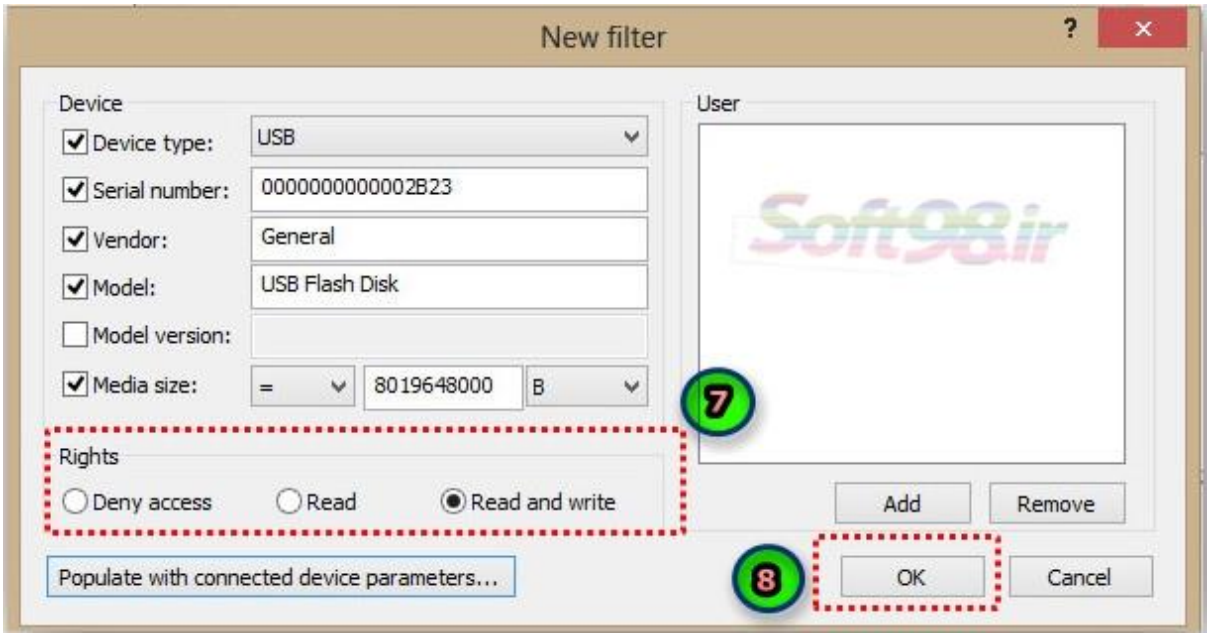
گزینه ها شامل موارد زیر میشود.:

منع دسترسی

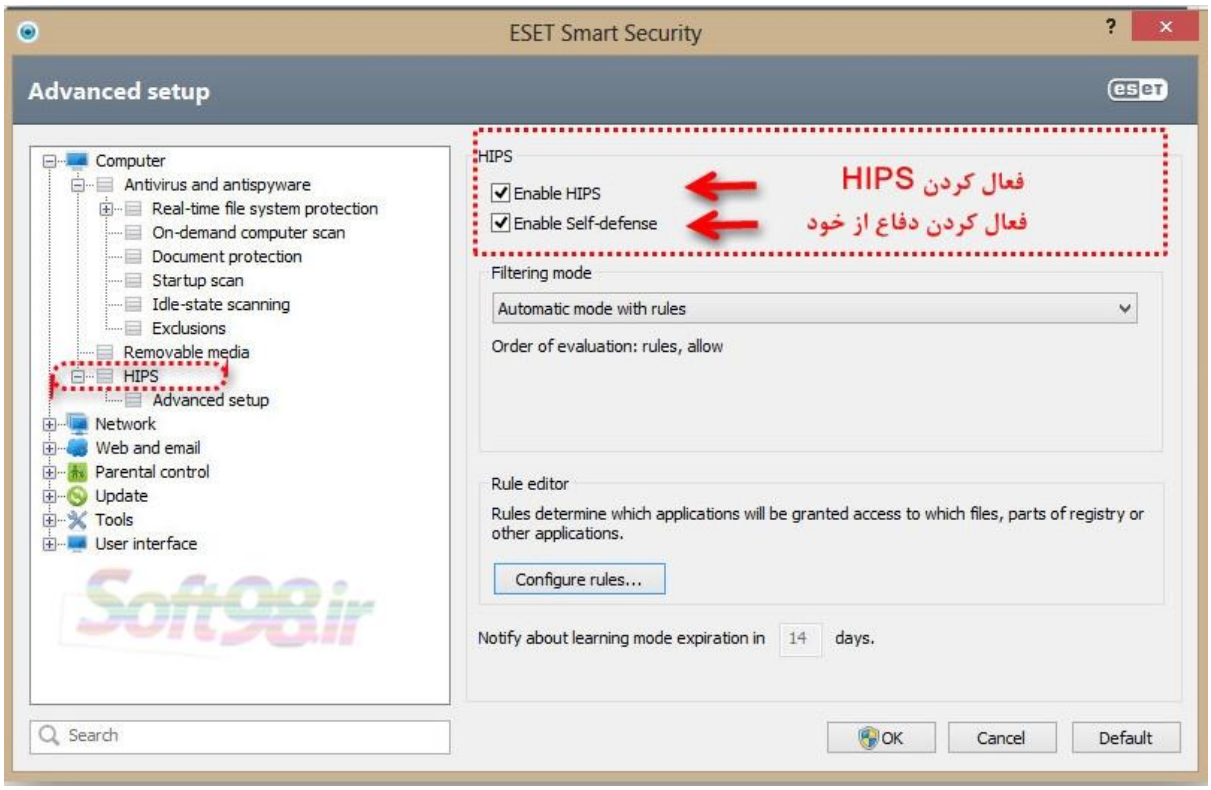
فقط خواندن

خواندن و نوشتن

www.ParsBook.org



(Host-based Intrusion Prevention System) HIPS



سیستم پیشگیری از نفوذ مبتنی بر میزبان (HIPS)

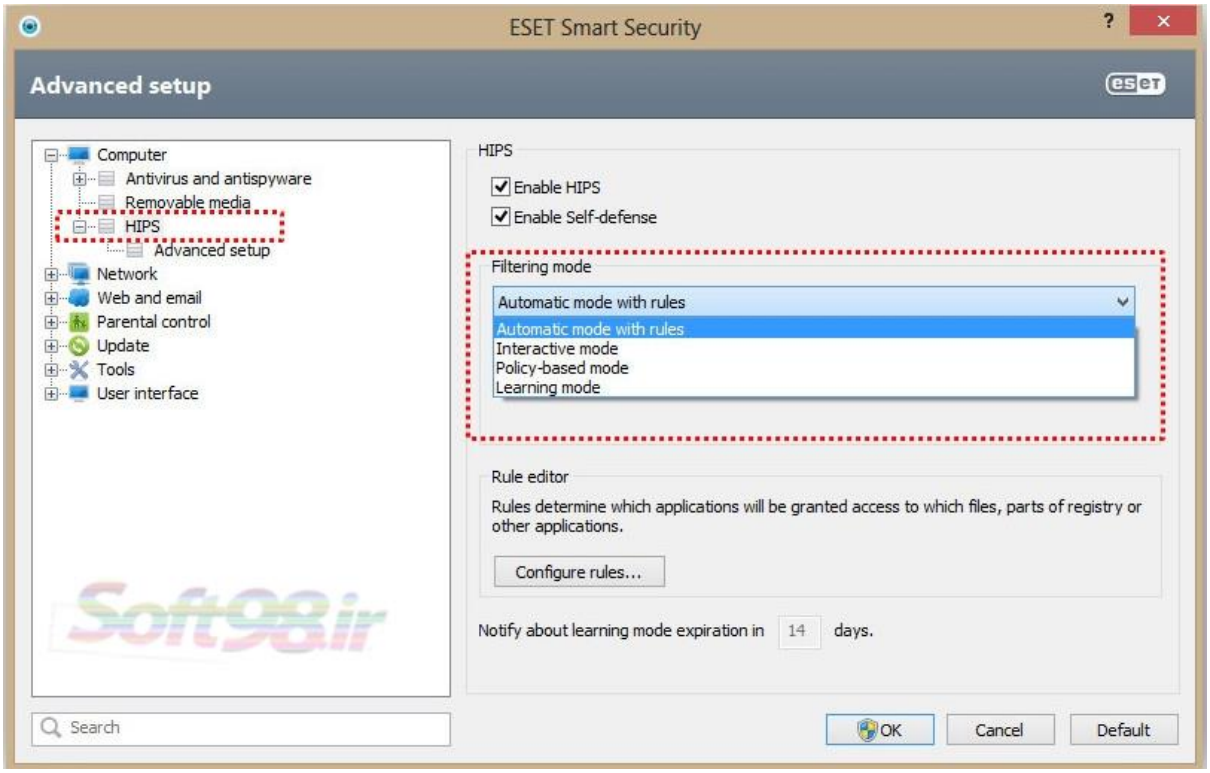
HIPS برای محافظت از سیستم شما در برابر فعالیت نرم افزارهای مخرب و ناخواسته ای که سعی دارند تاثیر مخرب و منفی از خود باقی بگذارند می باشد. HIPS با بهره گیری از پیشرفته تجزیه و تحلیل رفتاری همراه با قابلیت تشخیص شبکه فیلتر برای نظارت بر فرایندهای در حال اجرا و فایل ها و کلید های رجیستری است. HIPS جدا از حفاظت Real time ازیک فایل سیستمی ، یک فایروال نیست و نظارت تنها فرایندهای در حال اجرا در سیستم عامل را بر عهده دارد.

هشدار: تغییرات تنظیمات HIPS باید فقط توسط یک کاربر با تجربه باید انجام شود.

توجه: تغییرات فعال کردن HIPS و فعال کردن تنظیمات دفاع از خود پس از راه اندازی مجدد سیستم عامل ویندوز عمل خواهد کرد. غیر فعال کردن کل سیستم HIPS نیز نیاز به راه اندازی مجدد کامپیوتر دارد.

www.ParsBook.org

مهم : غیر فعال کردن مکانیسم دفاع از خود باعث می شود که HIPS در برابر تهدیدات بالقوه نتواند کاری انجام دهد بنابراین این کار توصیه نمی شود.



فیلتر را می توان در یکی از چهار حالت زیر انجام داد :

Automatic mode with rules : دراین حالت بجز موارد از پیش تعریف شده که محافظت از سیستم شما است، همه عملیاتها فعال هستند.

Interactive mode : در این حالت تمامی کارها با نظارت کاربر انجام میشود و برای هر فرایندی از او اجازه گرفته میشود.

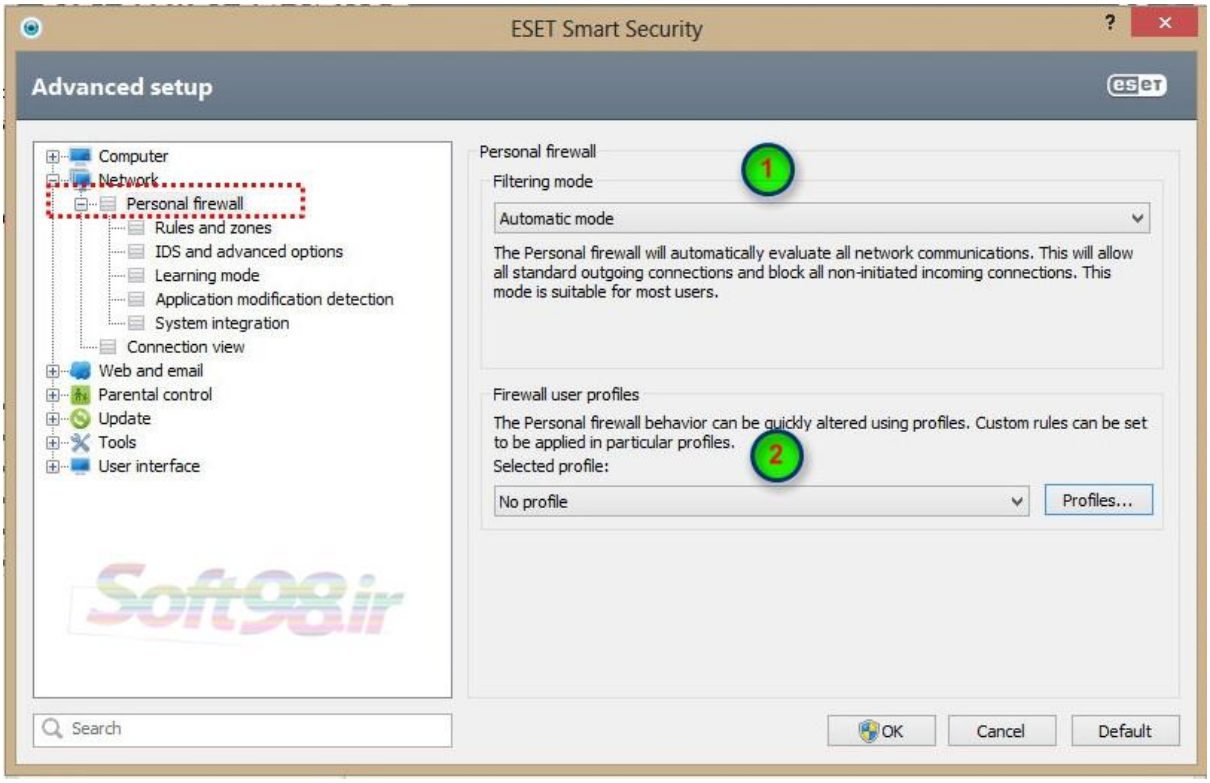
Policy-based mode : عملیاتی را توسط یک قانون تعریف نشده است را می توان مسدود کرد.

Learning mode : در حالت یادگیری، عملیاتها فعال و یک قاعده است که بعد از هر عمل ایجاد شده است .قوانین ایجاد شده در این حالت می تواند در ویرایشگر قاعده ویرایش شود، اما اولویت خود را پایین تر از اولویت قوانین که بصورت دستی و یا قوانین مورد استفاده در حالت اتوماتیک ایجاد شده اند میدهد.

با انتخاب حالت یادگیری ، چک باکس بعدی که تعداد روزهای یادگیری است را فعال می کند. .پس از گذشت زمان خاص دوره، حالت یادگیری غیر فعال است.مدت زمان حداکثر ۱۴روز است .پس از اینکه دوره زمانی تمام شد، می توان قوانین و فیلتر کردن حالت های مختلف را ویرایش کرد.

www.ParsBook.org

تنظیمات مربوط به قسمت Network



توضیحات مربوط به شماره ۱

۵ حالت کاری برای فایروال وجود دارد :

Automatic mode: در این حالت فایروال بصورت اتوماتیک عمل کرده و کاربر دخالتی در آن ندارد. این حالت برای کاربرانی که ترجیح می دهند استفاده آسان و راحت و بدون نیاز به تعریف قوانین از فایروال داشته باشند، مناسب است.

Automatic mode with exceptions (user-defined rules): علاوه بر حالت اتوماتیک، همچنین می توان ، قواعدی جهت سفارشی سازی توسط کاربر اضافه کرد.

Interactive mode : این گزینه به کاربر اجازه می دهد تا فایروال را بصورت سفارشی پیکربندی کند. این به معنای کنترل کامل فایروال بصورت دستی می باشد. در این حالت برای هر برقراری ارتباط از کاربر سوال می شود. همچنین هنگامی که یک ارتباط بدون قانون شناسایی شود یک پنجره محاوره ای مبنی بر ارتباط ناشناخته نمایش داده خواهد شد .پنجره محاوره ای گزینه هایی جهت اجازه یا رد ارتباط را می دهد. همچنین تصمیم گیری اجازه یا رد ارتباط را می توان به عنوان یک قانون جدید برای فایروال تعریف نمود که تمامی ارتباطات در آینده از این نوع مجاز یا مسدود خواهد شد.

Policy-based mode : بلوکه کردن تمام ارتباطات بجز ارتباطاتی که توسط کاربر با یک قانون جدید به آنها اجازه برقراری ارتباط داده خواهد شد .این حالت به کاربران حرفه ای اجازه می دهد تا با تعریف قوانین ،تنها به ارتباطات امن اجازه برقراری دهند و تمامی ارتباطات دیگر نامشخص تشخیص داده شده و توسط فایروال مسدود خواهد شد.

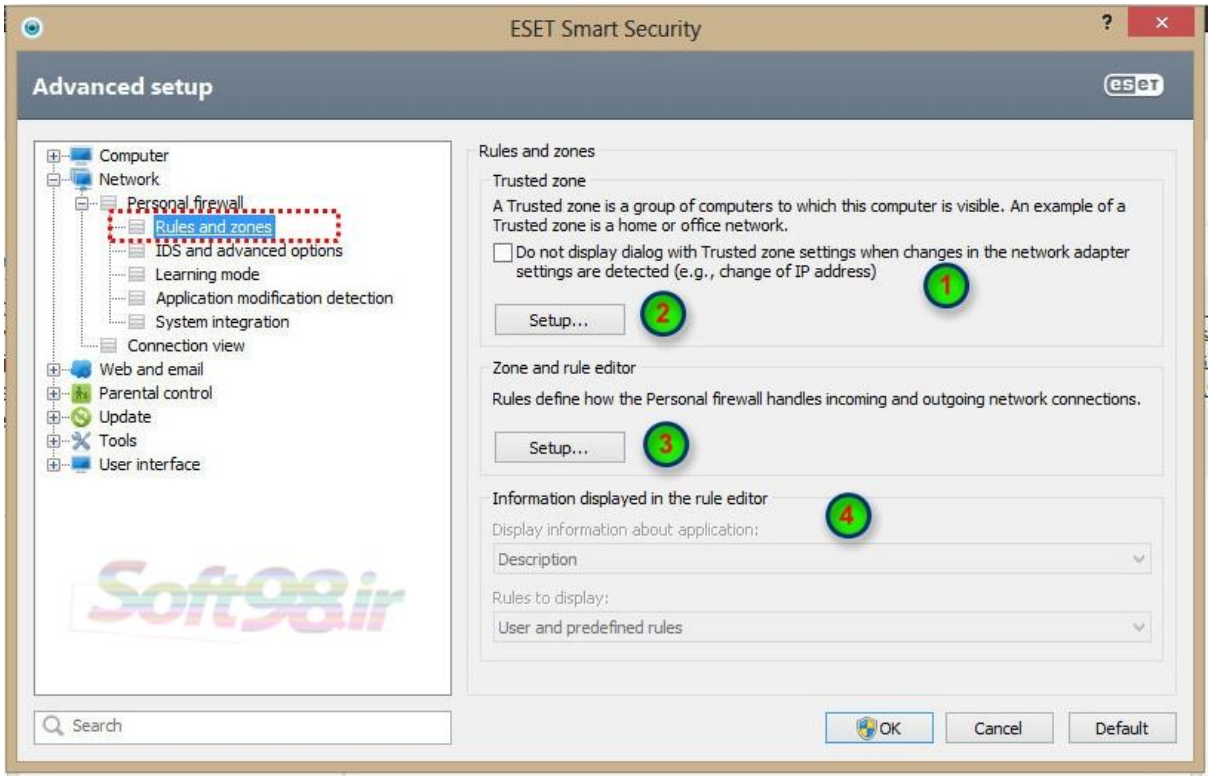
Learning mode : تمامی ارتباطات به صورت اتوماتیک توسط فایروال رسیدگی می شود و برای هر ارتباط به کاربر درباره نوع و پورت مورد استفاده توضیح داده می شود.

هشدار: در این حالت کاری تمامی ارتباطات ورودی و خروجی باز است و فقط پیغامی به کاربر مبنی بر برقرای این نوع ارتباط داده می شود.

www.ParsBook.org

۲-پروفایل ها به منظور کنترل رفتار فایروال می تواند مورد استفاده قرار بگیرد.

Rules and zones



توجه : اگر فایروال در حالت Automatic mode تنظیم شده باشد، برخی از تنظیمات فعال نیستند.

۱-عدم نمایش کادر محاوره ای با تنظیمات زون مورد اعتماد زمانی که تغییراتی در تنظیمات آداپتور شبکه تشخیص داده شود(به عنوان مثال تغییر آی پی)

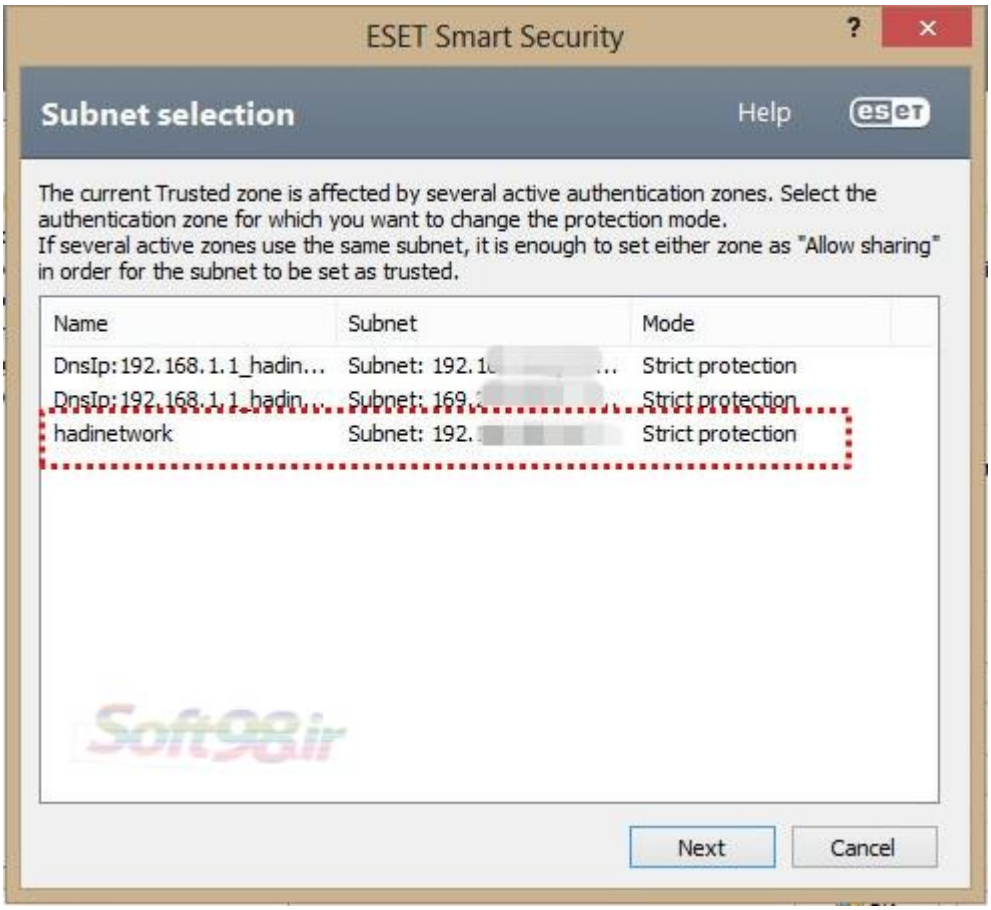
۲-معرفی یک شبکه به عنوان شبکه امن جهت برقراری با سایر کامپیوترها(مثلا معرفی یک شبکه خانگی یا اداری)

۳-بخش تنظیمات فایروال برای باز و بسته ارتباطات اینترنتی برنامه های مختلف

۴- نمایش اطلاعات در ویرایشگر Rule

www.ParsBook.org

معرفی یک شبکه به عنوان شبکه امن جهت برقراری با سایر کامپیوترها(مثلا معرفی یک شبکه خانگی یا اداری)

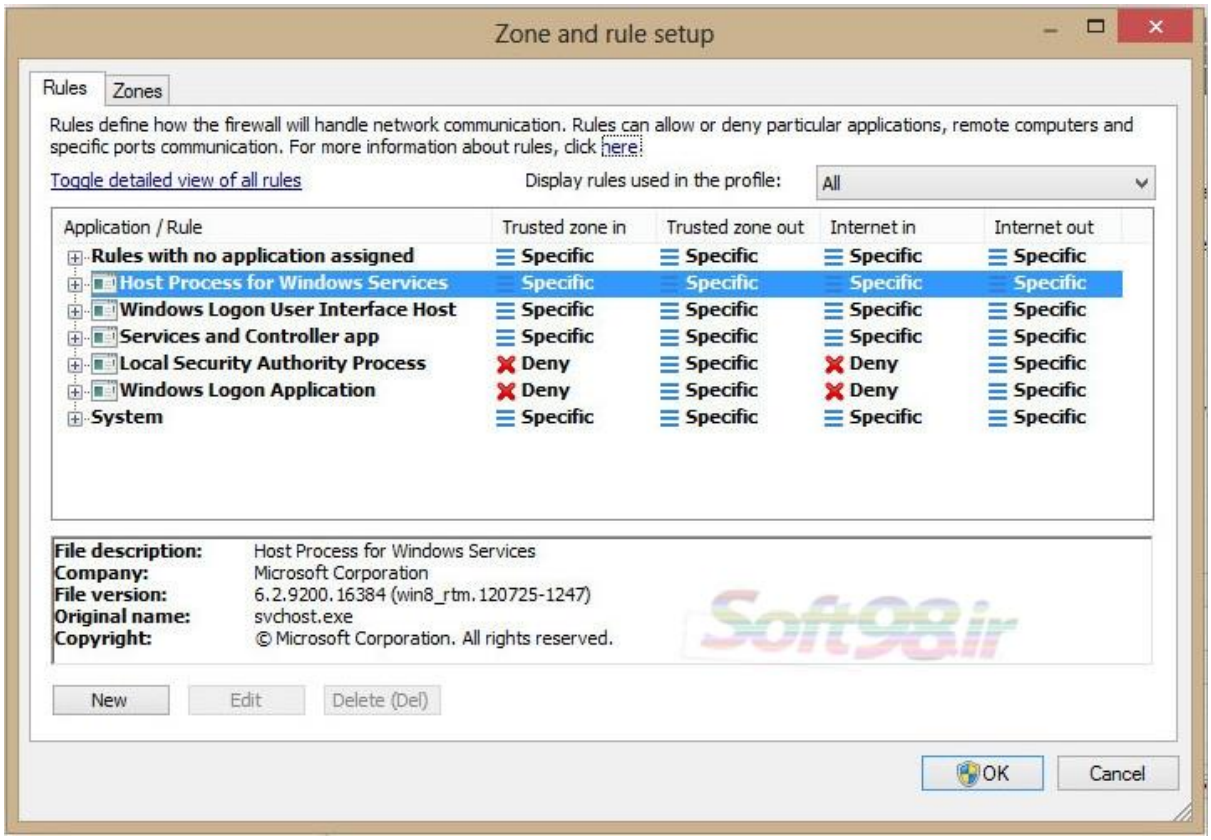


www.ParsBook.org

نحوه ساختن یک قانون

هشدار: برای ساختن یک قانون باید فایروال رو از حالت Automatic Mode خارج کنید.

ابتدا بر روی New کلیک کنید تا پنجره New Rule باز شود.



www.ParsBook.org

Direction : جهت محدود کردن اصلاعات ورودی یا خرو جی یا محدود کردن هر دو

(in : ورودی ، out : خروجی ، Both : هر دو) که معمولا بهتر است هر دو ارتباط محدود شود.

Action : جهت انتخاب نوع محدودیت اعمالی که شامل گزینه ای زیر می شود :

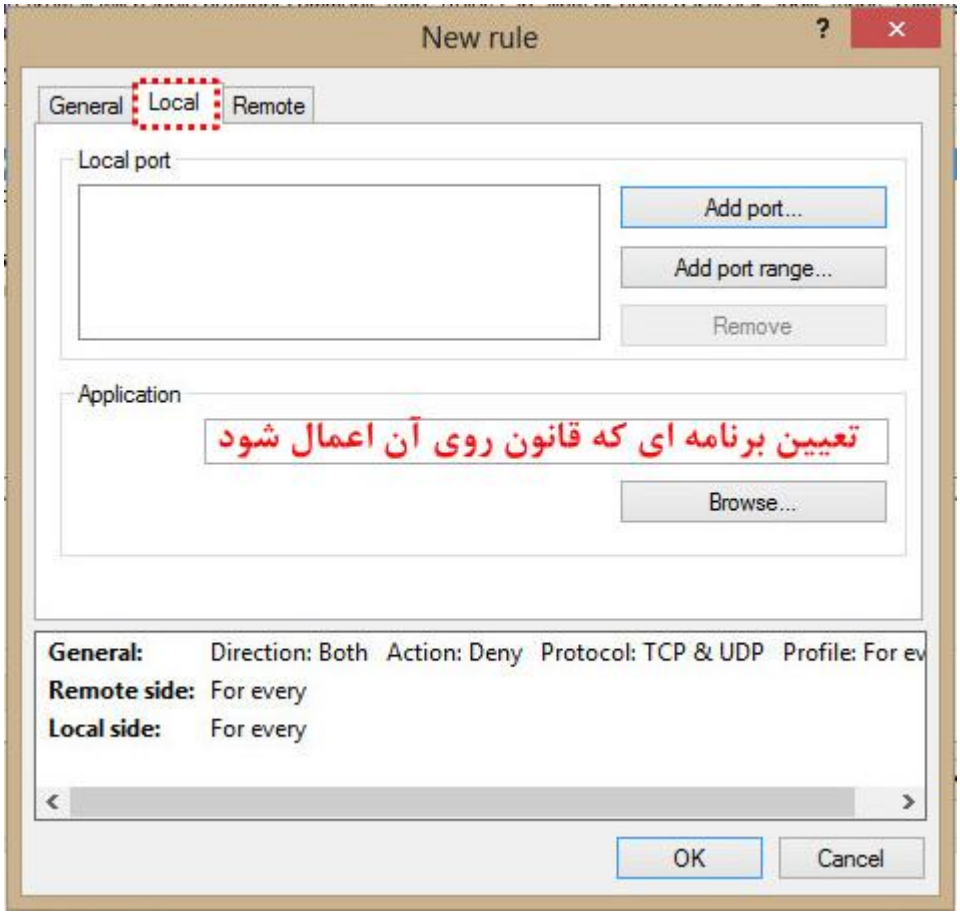
بلوکه شدن برنامه (Deny) یا اجازه دادن(Allow) یا سوال کردن(Ask)

Protocol : تعیین نوع انتقال داده ها

Profile : انتخاب پروفایلی که قانون در آن اجرا شود (for every انتخاب برای همه پروفایلها)

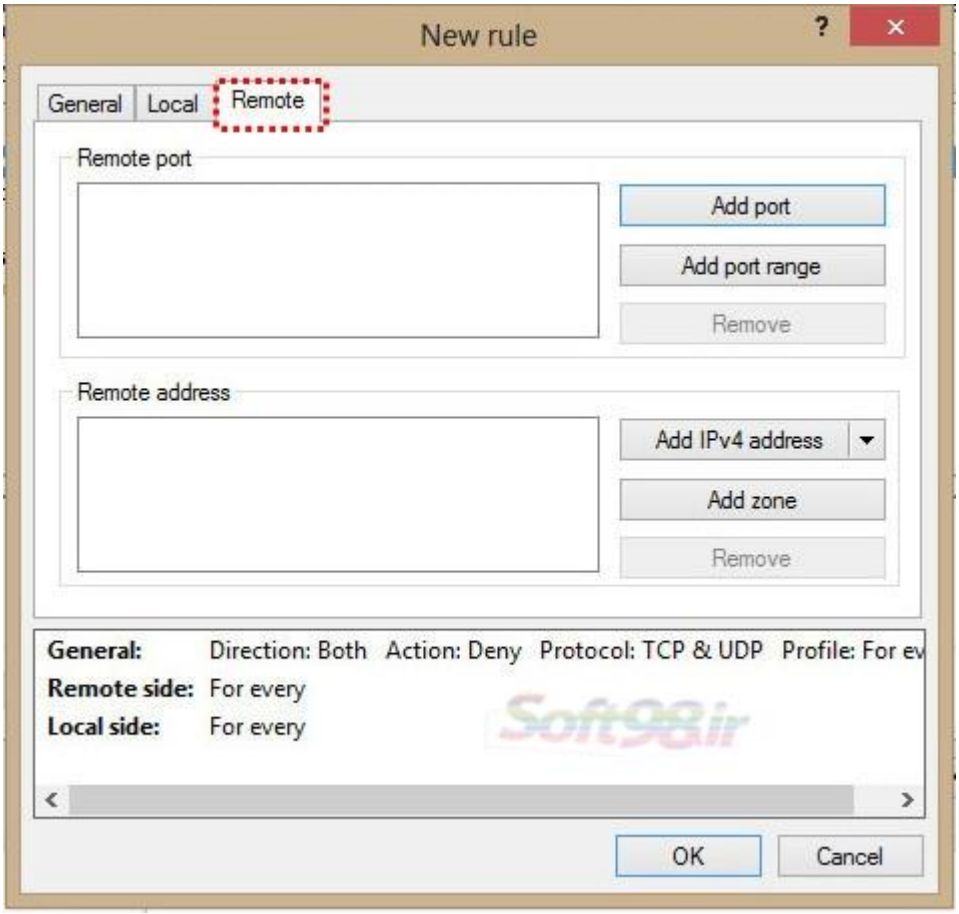
Notify usr : اعلام به کاربر

Log : رخداد



Local Port : تعیین پورتهایی که توسط برنامه انتخاب شده مورد استفاده قرار می گیرد(در صورت اضافه نکردن پورت همه پورتها اعمال می شود)

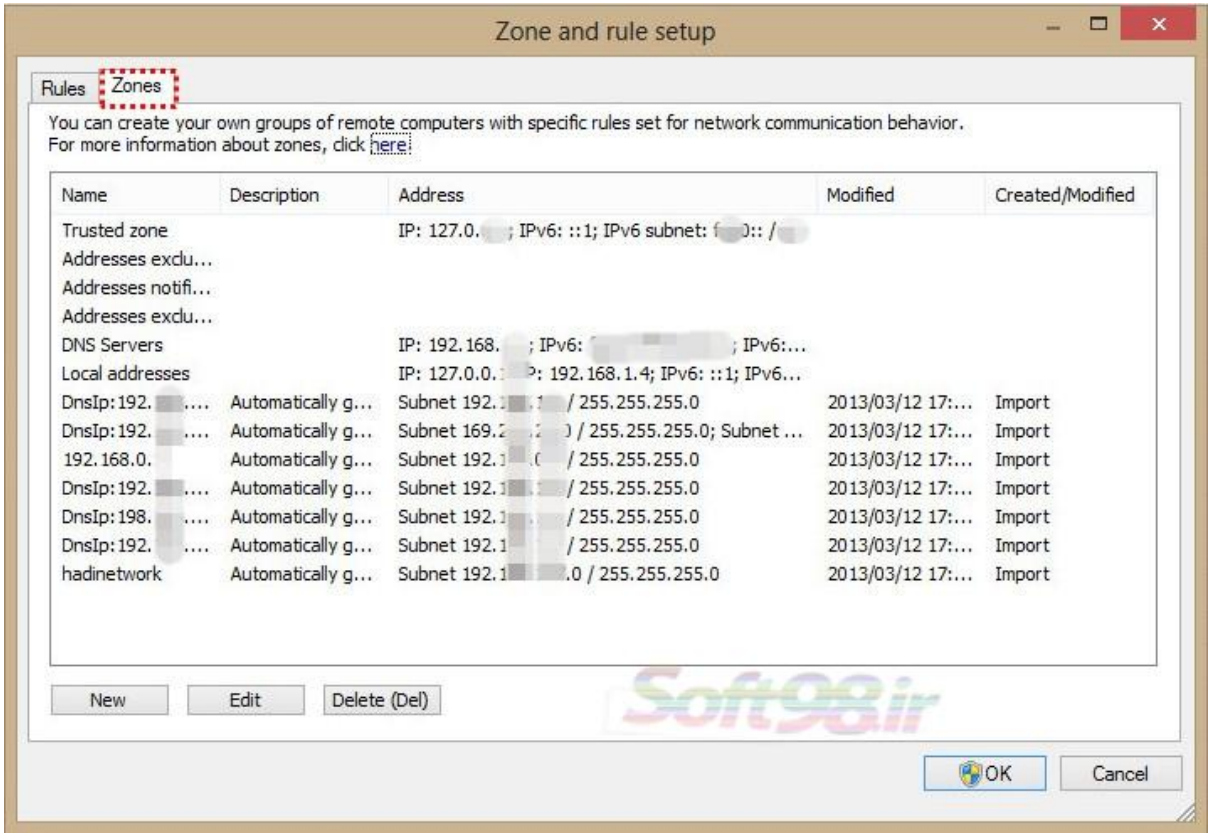
www.ParsBook.org



این برگه حاوی اطلاعاتی در مورد کنترل از راه دور پورت می باشد. همچنین می توان یک لیست از آدرس های IP برای کنترل از راه دور تعریف نمود .

www.ParsBook.org

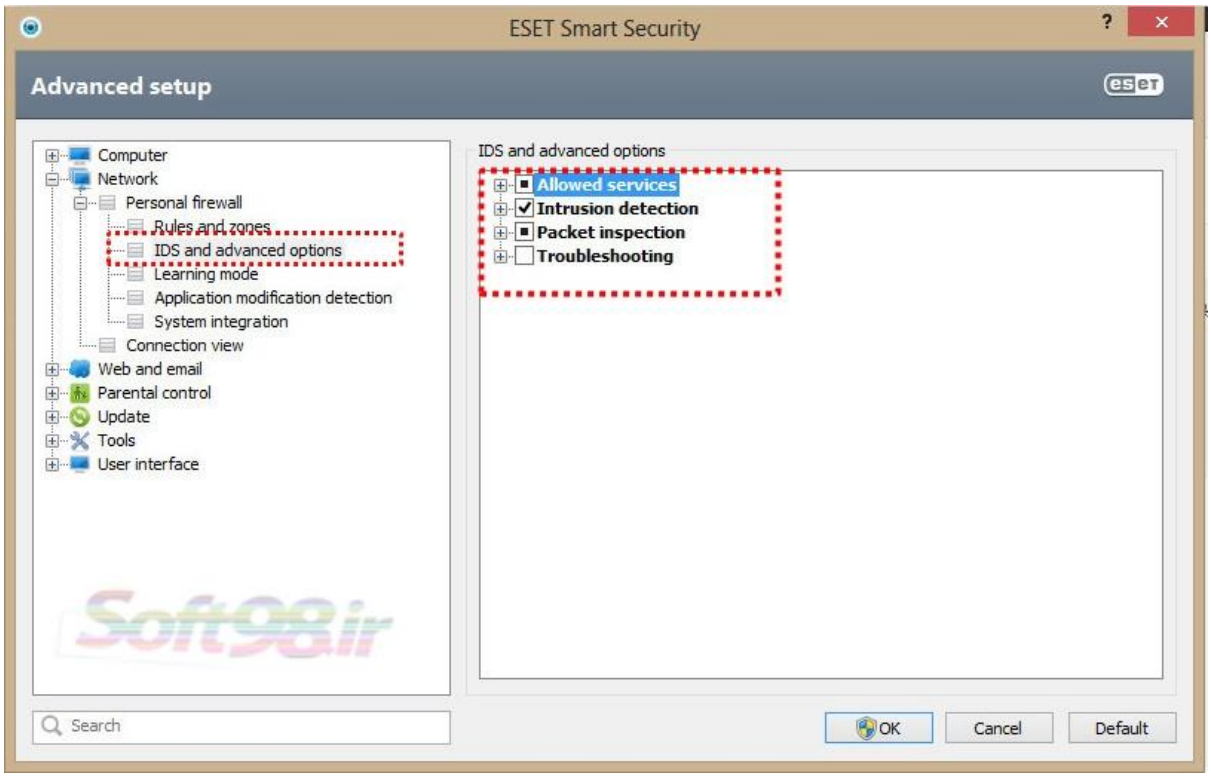
Zones



در پنجره تنظیمات منطقه(Zones) می توانید نام منطقه، توضیحات، لیست آدرس شبکه و تصدیق هویت منطقه را مشخص کنید.

www.ParsBook.org

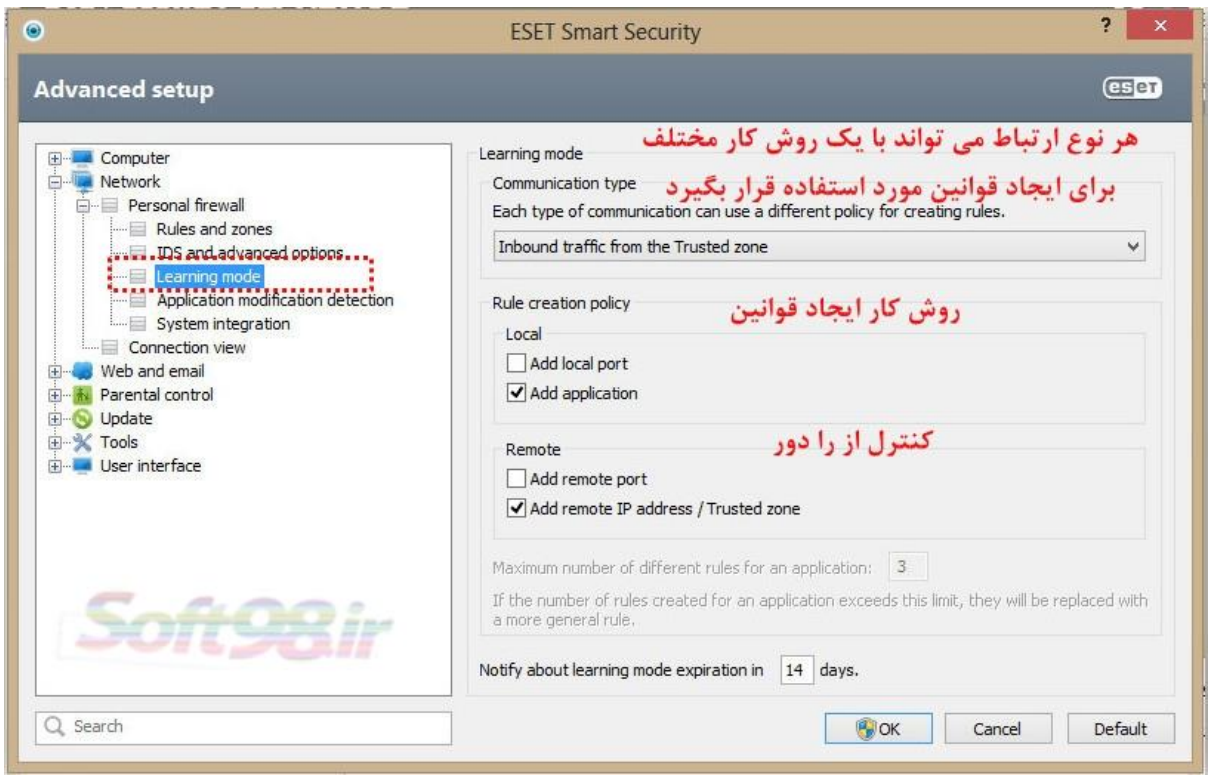
IDS and advanced option



IDS and advanced options به شما اجازه ی پیکربندی گزینه های فیلترینگ پیشرفته را می دهد که برای تشخیص انواع مختلفی از حملات به کامپیوتر مفید می باشد.

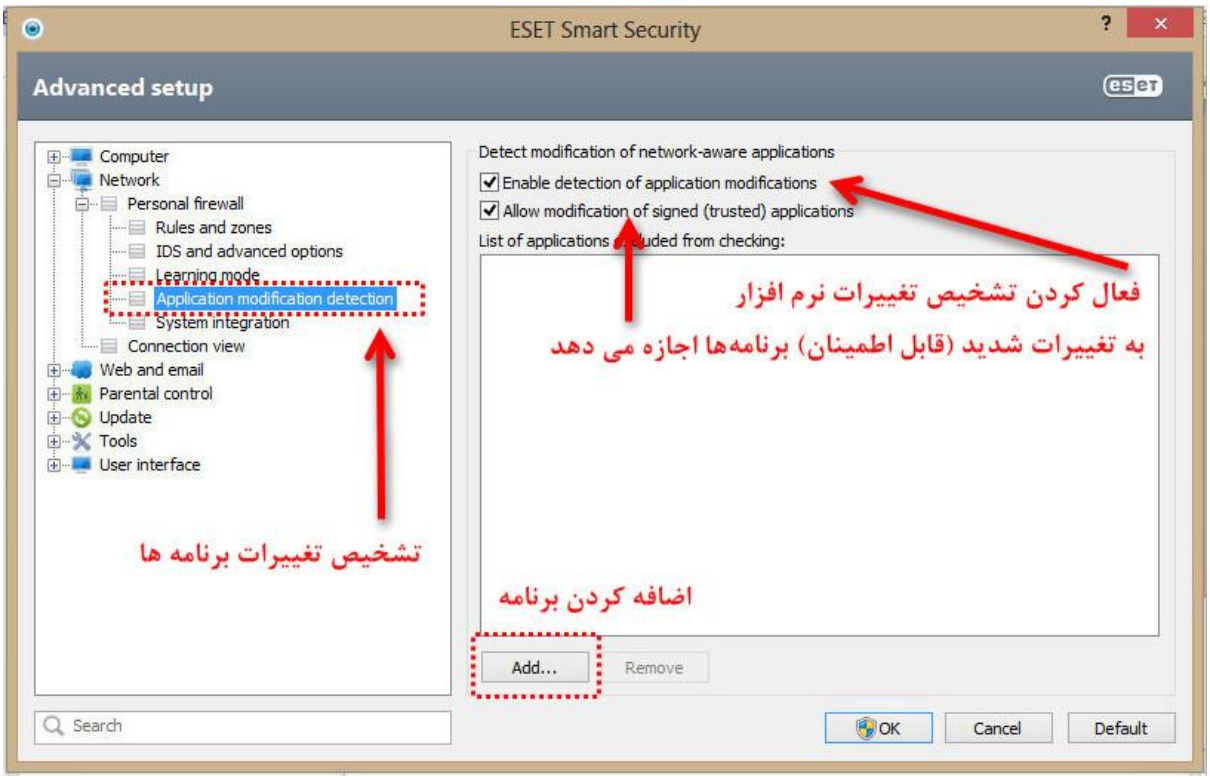
Learning mode

هشدار: برای فعال بودن گزینه ها باید فایروال در حالت Learning Mode باشد.

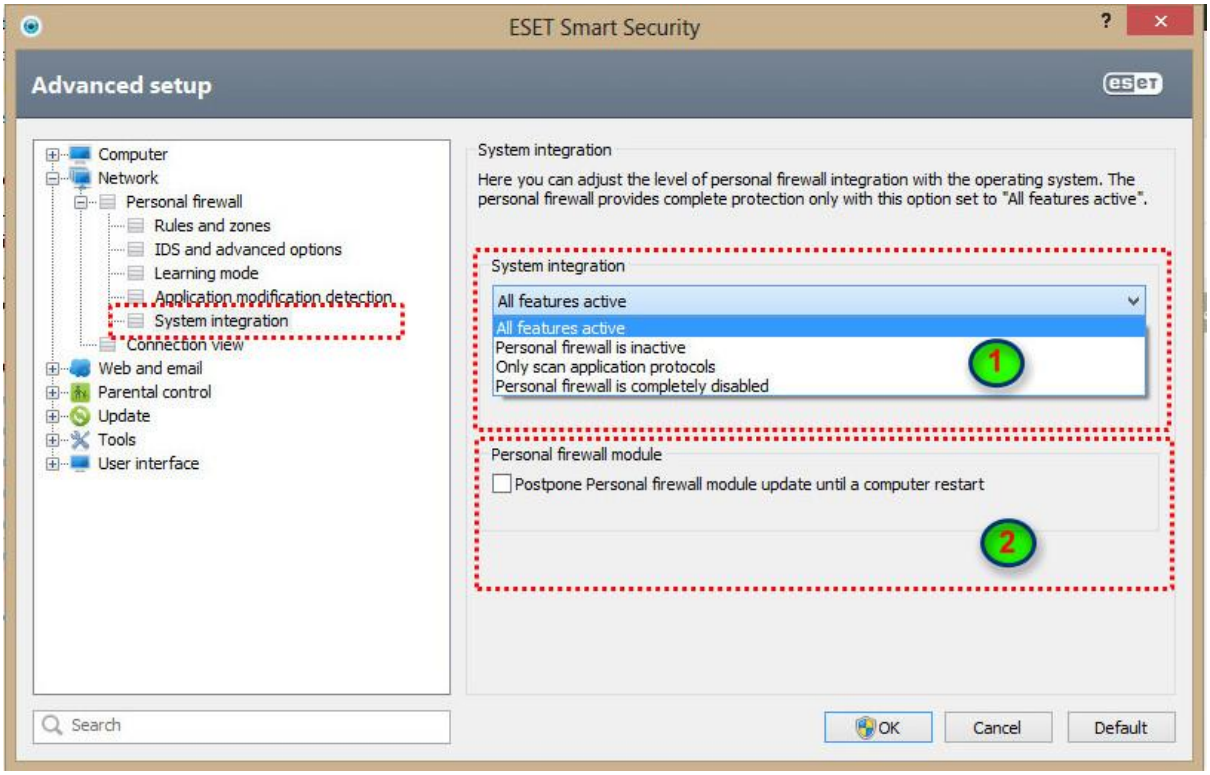


www.ParsBook.org

Application modification detection



System integration



۱-فایروال ESET Smart Security می تواند در سطوح مختلف بکارگیری شود:

All features active : در این حالت فایروال کاملا یکپارچه است و اجزای آن به طور پیش فرض فعال هستند. اگر کامپیوتر شما قرار است به یک شبکه بزرگ یا به اینترنت متصل شود توصیه می شود که این گزینه را فعال کنید. این گزینه امن ترین تنظیمات فایروال است و سطح بالایی از حفاظت را ارائه می دهد.

www.ParsBook.org

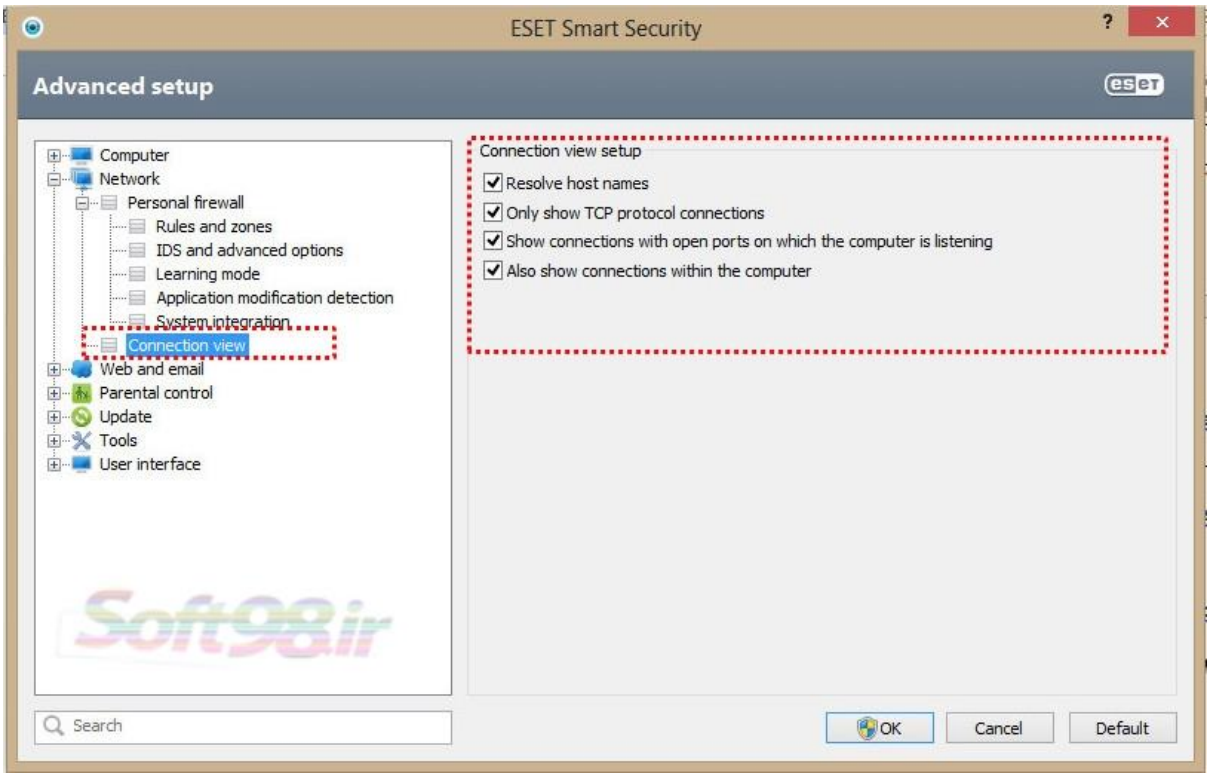
Personal firewall is inactive : فایروال شخصی در سیستم و واسطه ارتباطات شبکه یکپارچه شده است، اما تهدیدات مورد بررسی قرار نمی گیرد.

Only scan application protocols : فقط بخش اسکن پروتکل های نرم افزار (HTTP, HTTPS , POP3, IMAP) فعال است.

Personal firewall is completely disabled : فایروال بطور کامل غیر فعال می شود.

۲- بروزرسانی ماژول فایروال را تا زمانی که کامپیوتر راه اندازی مجدد شود به تعویق می اندازد.

System integration



Resolve host names : در صورت امکان، تمام آدرس های شبکه در قالب DNS، نمایش داده می شود نه در قالب IP

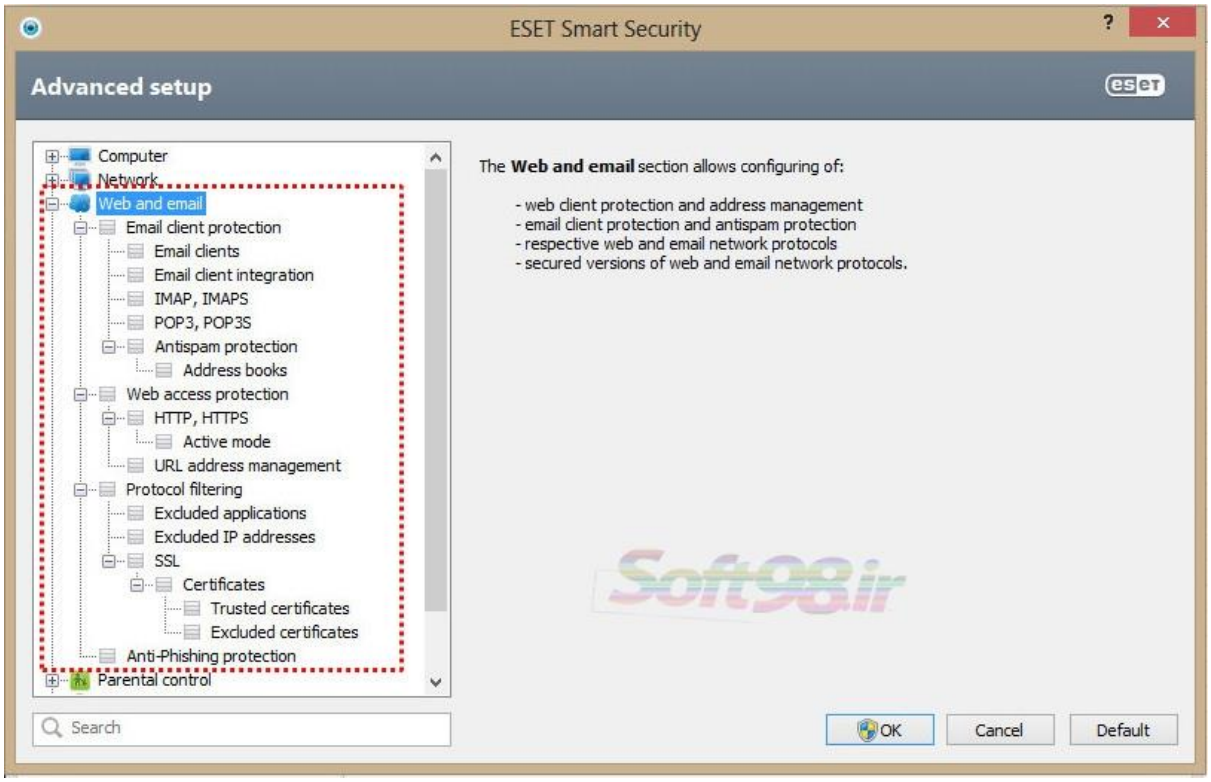
Only show TCP protocol connections : این لیست تنها ارتباطات پروتکل TCPرا نشان می دهد.

Show connections with open ports on which the computer is listening : انتخاب این گزینه فقط ارتباطاتی، که درحال حاضر درآن هیچ ارتباطی وجود ندارد، اما سیستم یک پورت را باز کرده و منتظر برای اتصال است.

Also show connection within the computer : انتخاب این گزینه تنها ارتباطات، کنترل از راه دور یک سیستم محلی را نمایش می دهد که به اصطلاح host local نامیده می شود.

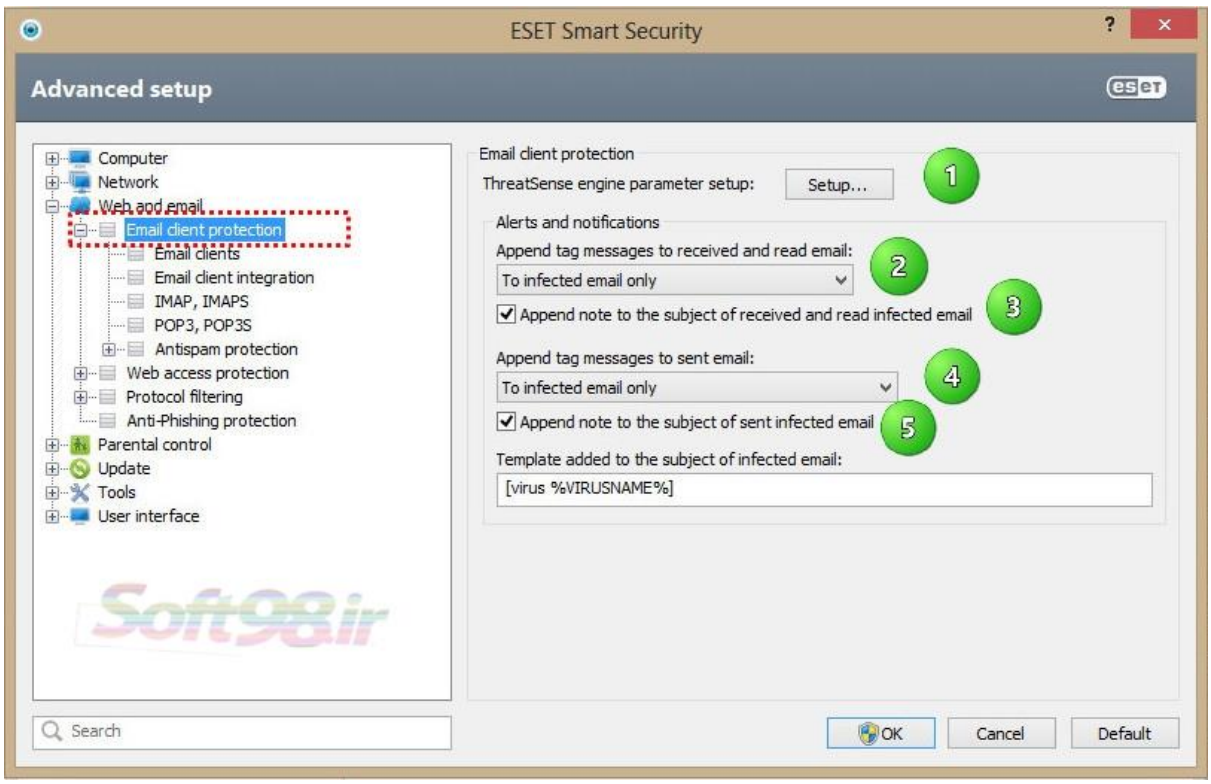
www.ParsBook.org

تنظیمات مربوط به قسمت Web and Email



اتصال به اینترنت از ویژگی های استاندارد برای کامپیوتر های شخصی است .متاسفانه اینترنت، رسانه اصلی برای توزیع کد های مخرب تبدیل شده است به همین دلیل دقت در تنظیمات حفاظت دسترسی به وب ضروری است. این نرم افزار با بهره گیری از متدهای ThreatSense تمامی نامه های ورودی را مورد تجزیه و تحلیل قرار می دهد.

Email client protection



www.ParsBook.org

۱-وارد شدن به تنظیمات پیشرفته ThreatSense برای پیکربندی آن از جمله اهداف اسکن، روش های تشخیص، تعیین سطح پاک کنندگی و غیره

۲- پیوست پیام های برچسب به ایمیلهای دریافتی و خواندنی که شامل سه حالت زیر می شود:

Never : پیامهای برچسب به هیچ ایمیلی اضافه نمی شود.

To infected email only : تنها پیامهای را که به عنوان حاوی نرم افزار مخرب مشخص شده اند ، مورد بررسی قرار میگیرد.

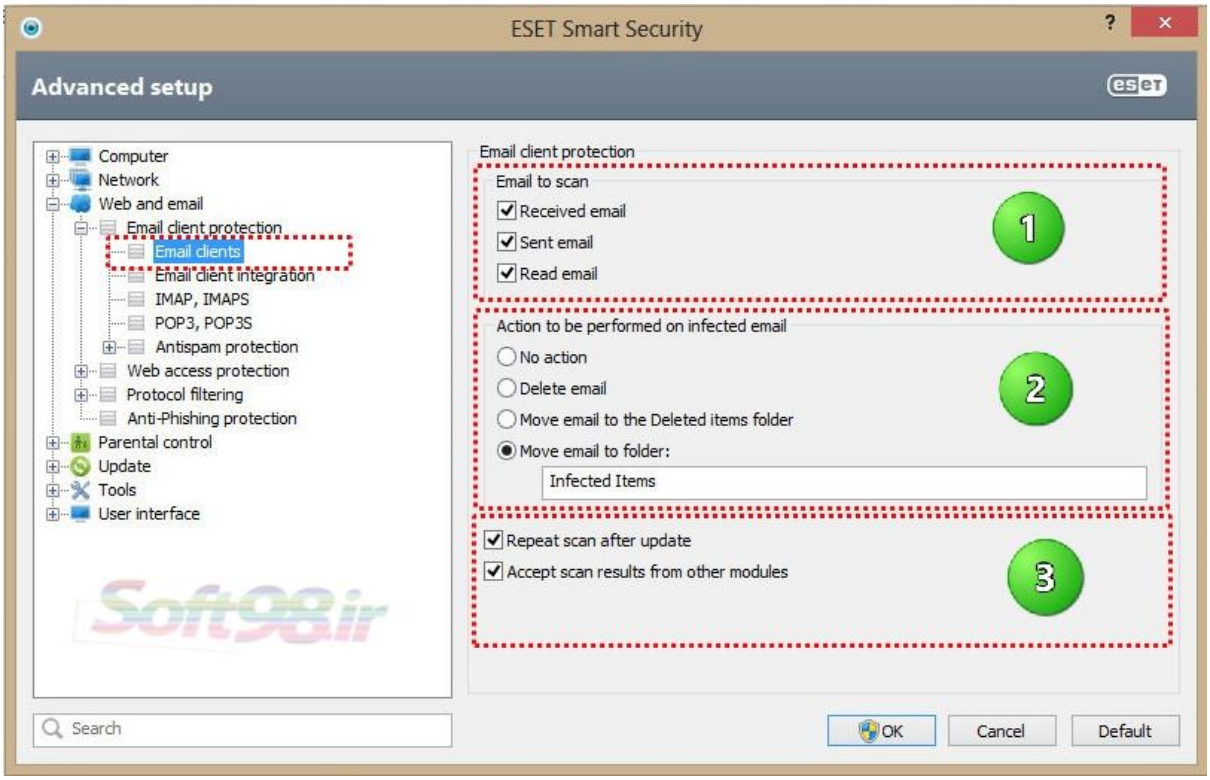
To all scanned email : برنامه پیام های برچسب را به تمام ایمیلهای اسکن شده، اضافه می کند.

۳- اضافه کردن هشدار ایمیل آلوده به موضوع ایمیل های دریافتی وخواندنی

۴-پیوست پیامهای برچسب به ایمیلهای ارسالی

۵- اضافه کردن هشدار ایمیل آلوده به موضوع ایمیل های ارسالی

Email clients



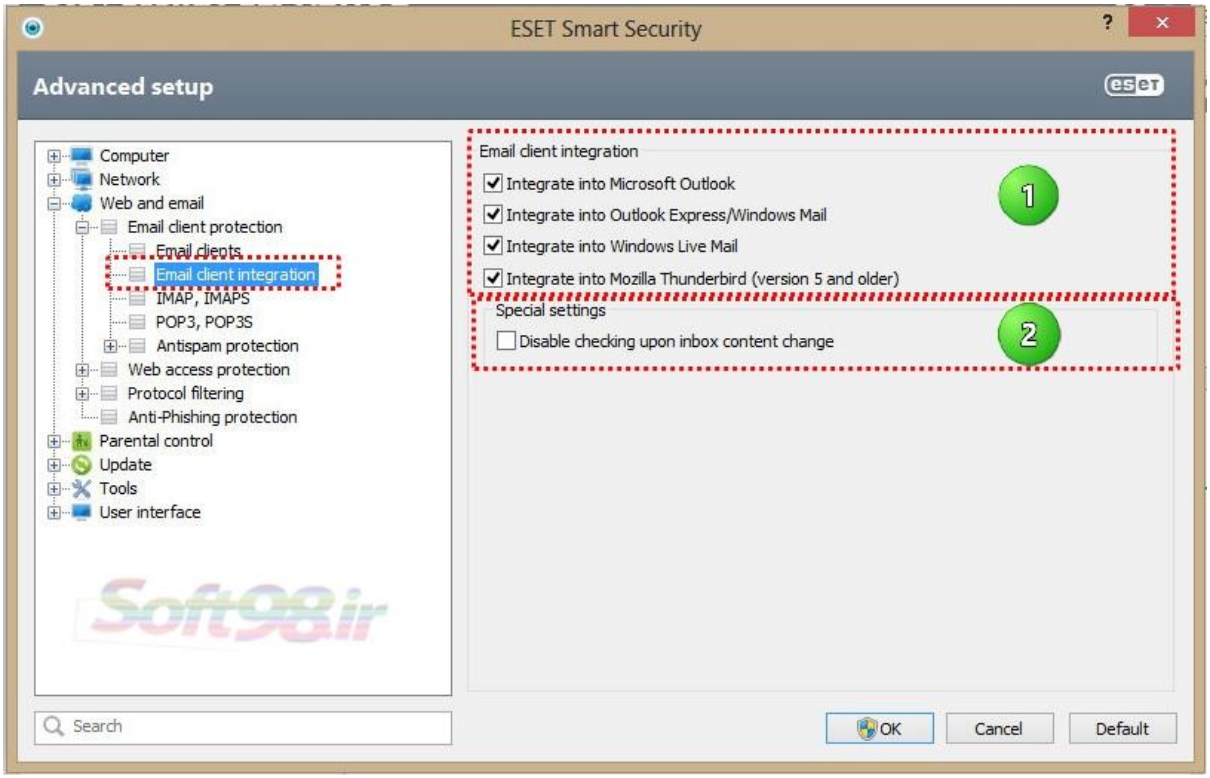
۱- ایمیلهایی که مورد اسکن قرار می گیرند.

۲- اقدامی که بر روی ایمیل آلوده انجام بگیرد.(که شامل ۱-هیچ عملی انجام نگیرد.۲-ایمیل حذف شود.۳-انتقال ایمیل به پوشه آیتمهای حذف شده ۴- انتقال به پوشه آیتمهای آلوده)

۳- گزینه اول (تکرار اسکن بعد از هر بار آپدیت) گزینه دوم (پذیرفتن نتایج اسکن از دیگر ماژول های حفاظت)

www.ParsBook.org

Email client integration

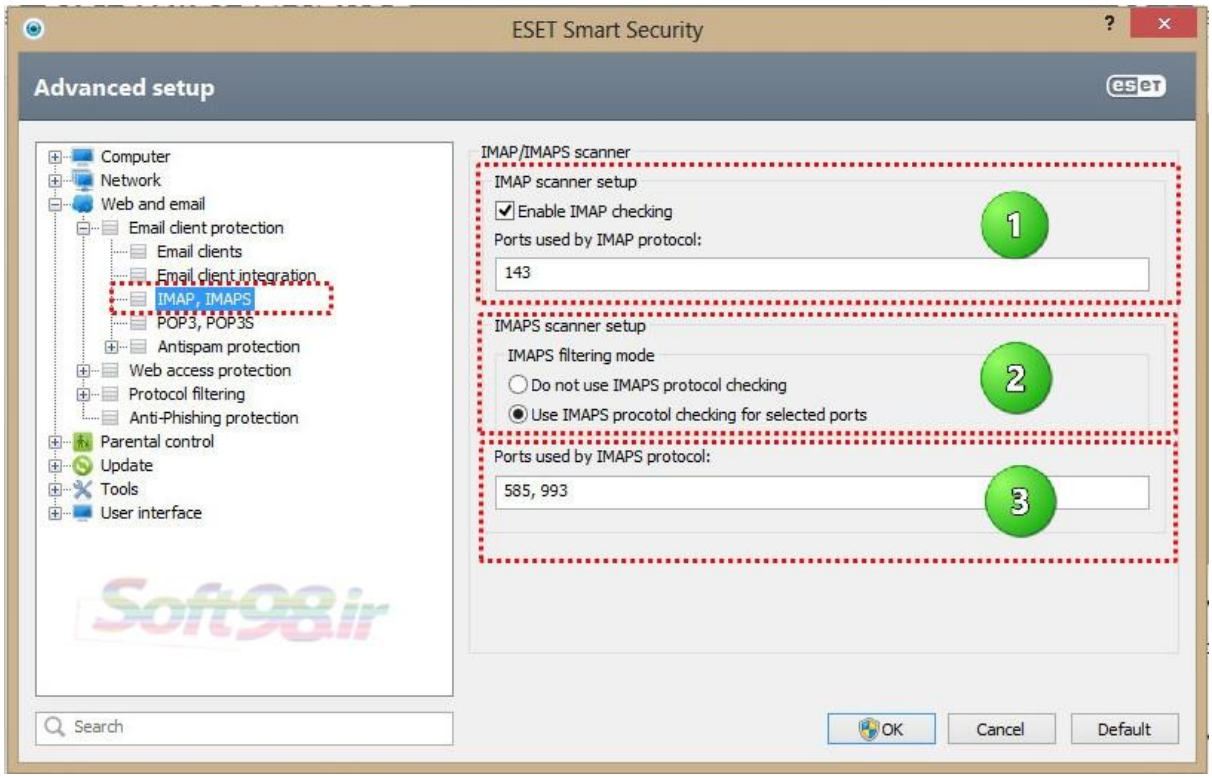


۱- یکپارچه سازی با نرم افزارهای ایمیل Microsoft Outlook, Outlook Express, Windows Mail Windows Live Mail and Mozilla Thunderbird

۲- غیر فعال کردن بررسی برای تغییر مطالب صندوق ورودی ایمیل

این گزینه زمانیکه شما در حال کار با نرم افزار ایمیل با کندی سرعت سیستم مواجه شوید، کارائی دارد.

IMAP , IMAPS

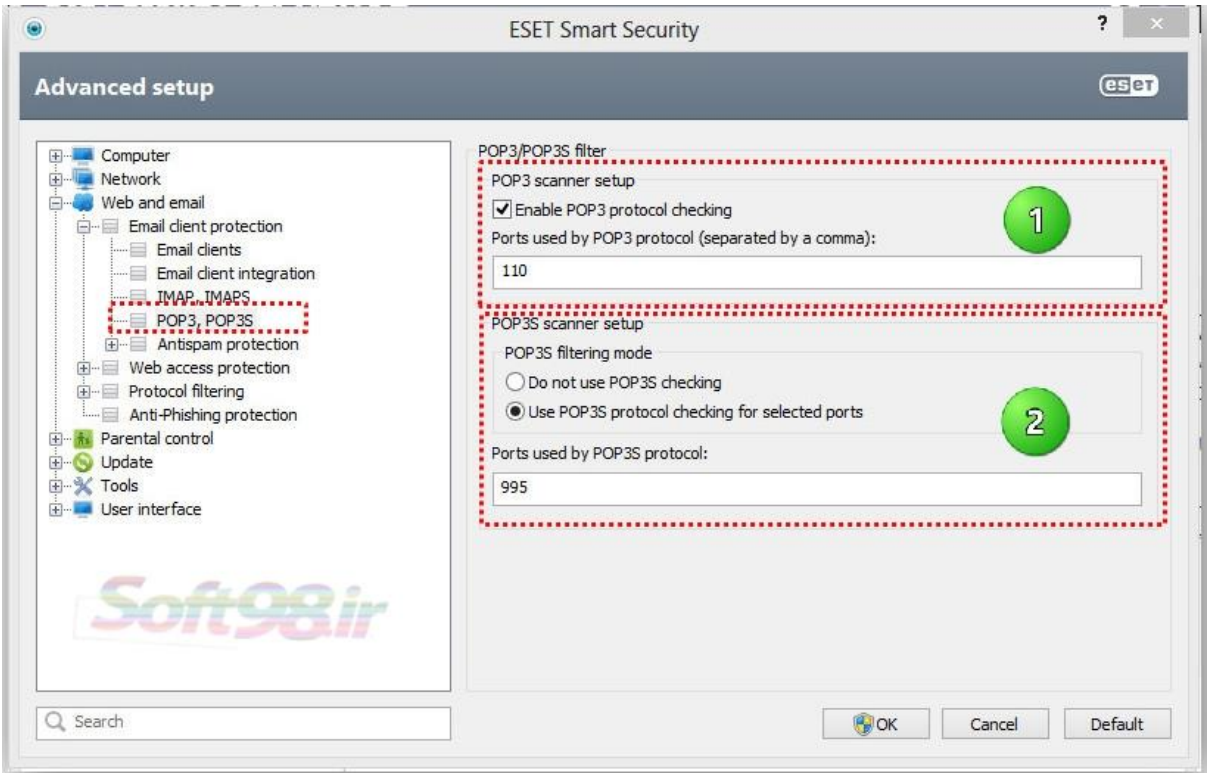


www.ParsBook.org

۱- فعال کردن پروتکل دسترسی به پیام اینترنتی (IMAP) و انتخاب پورت مورد استفاده در پروتکل IMAP

۲- فعال یا غیر فعال کردن اسکنر پروتکل IMAPS و انتخاب پورت مورد استفاده ی پروتکل

POP3 , POP3S

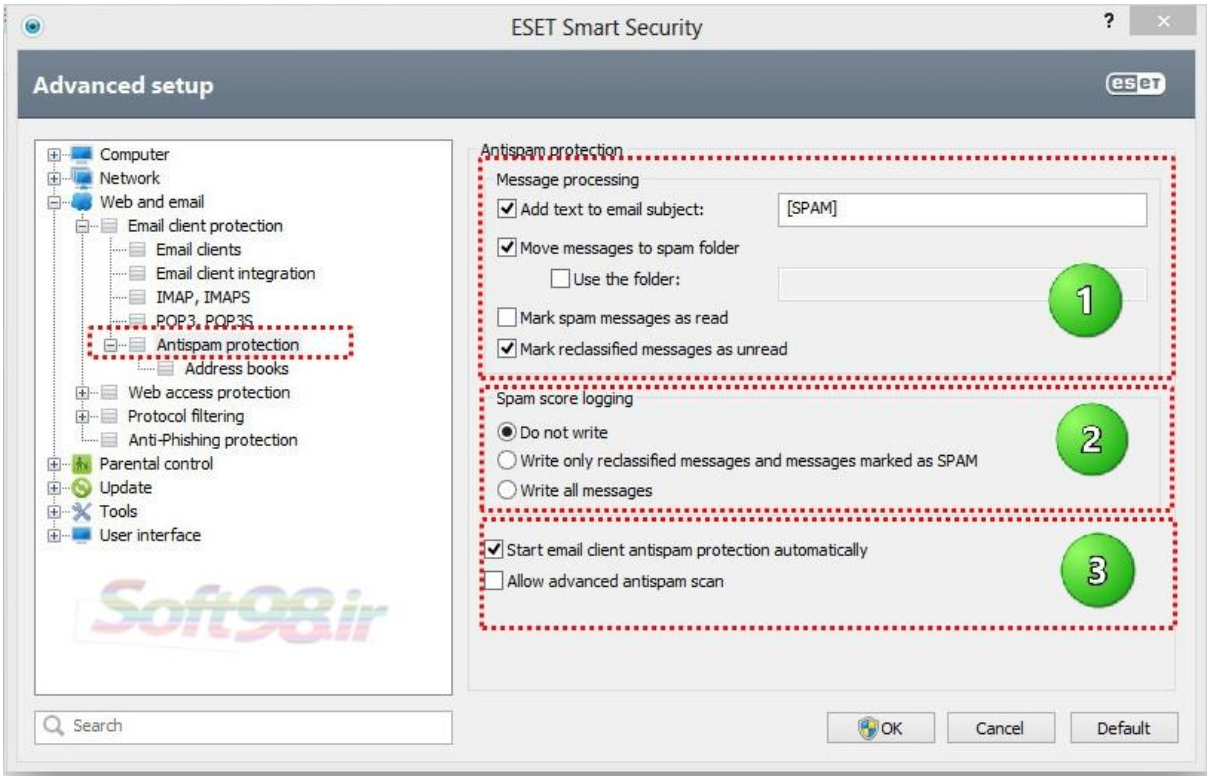


۱- پروتکل POP3 گسترده ترین پروتکل مورد استفاده برای دریافت ارتباطات ایمیل در یک برنامه سرویس گیرنده ایمیل است. ESET Smart Security برای حفاظت از این پروتکل بدون در نظر گرفتن ایمیل سرویس گیرنده استفاده می شود.
این ماژول حفاظت به طور خودکار در هنگام راه اندازی سیستم راه اندازی میشود و پس از آن در حافظه فعال است. چک کردن پروتکل POP3 به طور خودکار و بدون نیاز به پیکربندی مجدد از سرویس گیرنده ایمیل انجام میشود. به طور پیش فرض، همه ارتباطات بر روی پورت ۱۱۰ میباشد ولی میتوان پورت های ارتباطی دیگر را هم اضافه کرد. در صورت لزوم شماره پورت های دیگر را باید به وسیله کاما از هم جدا کرد.

۲- فعال یا غیر فعال کردن اسکنر پروتکل POP3S و انتخاب پورت مورد استفاده ی پروتکل

www.ParsBook.org

Antispam Protection



ایمیل های ناخواسته اسپم نامیده می شود که یکی از بزرگترین مشکلات ارتباطات الکترونیکی است. هرزنامه (اسپم) تا ۸۰ درصد از تمام ارتباطات ایمیل را بخود اختصاص داده است. ESET Smart Security به محافظت در برابر این مشکل کمک میکند. ماژول Antispam به فیلتر کردن صندوق ورودی ایمیل از هرزنامه و تمیز نگه داشتن آن کمک میکند.

یکی از اصول مهم برای تشخیص هرزنامه ها توانایی شناسایی ایمیل های ناخواسته بر اساس آدرس از پیش تعریف شده قابل اعتماد (لیست سفید) و آدرس های اسپم (لیست سیاه) است. تمام آدرس ها ، از لیست تماس شما به صورت خودکار به لیست سفید اضافه میشود.

روش اصلی مورد استفاده برای شناسایی هرزنامه اسکن خواص پیام ایمیل است. پیام های دریافت شده با معیارهای Antispam (تعاریف پیام، فن آوری هوشمند آماری، الگوریتم های تشخیص و دیگر روش های منحصر به فرد) اسکن میشود و ارزش شاخص تعیین می کند که آیا یک پیام هرزنامه است یا نه .

۱-Message processing (پردازش پیام)

Add text to email subject : اضافه کردن یک متن به موضوع ایمیل هایی که به عنوان اسپم طبقه بندی شده اند.

پیش فرض[هرزنامه] می باشد.

Move messages to spam folder : هنگامی که این گزینه فعال باشد، پیامهای هرزنامه به طور پیش فرض به پوشه ایمیل های ناخواسته منتقل خواهد شد.

Use the folder : این گزینه برای انتقال هرزنامه ها به یک پوشه تعریف شده توسط کاربر است.

Mark spam messages as read : علامت گذاری پیام های اسپم به عنوان پیامهای خوانده شده

www.ParsBook.org

Mark reclassified messages as unread : علامت گذاری پیام های خوانده نشده از نو طبقه بندی شده (در این حالت پیامهایی که به عنوان هرزنامه طبقه بندی شده بودند، ولی بعدا به عنوان "پاک" مشخص شده اند آنوقت به عنوان خوانده نشده نمایش داده خواهند شد.)

۲-Spam score logging (شدت ورود به سیستم هرزنامه)

موتور Antispam بعد هر اسکن پیام، شدت هرزنامه به آن اختصاص می دهد.

Do not write : سلول های نمره در رخدادهای حفاظت Antispam خالی خواهد بود.

Write only reclassified messages and messages marked as SPAM : با استفاده از این گزینه شما میتوانید به پیام هایی که به عنوان هرزنامه مشخص شده اند نمره بدهید.

Write all messages : همه پیام ها در رخدادها ،نمره هرزنامه خواهند گرفت.

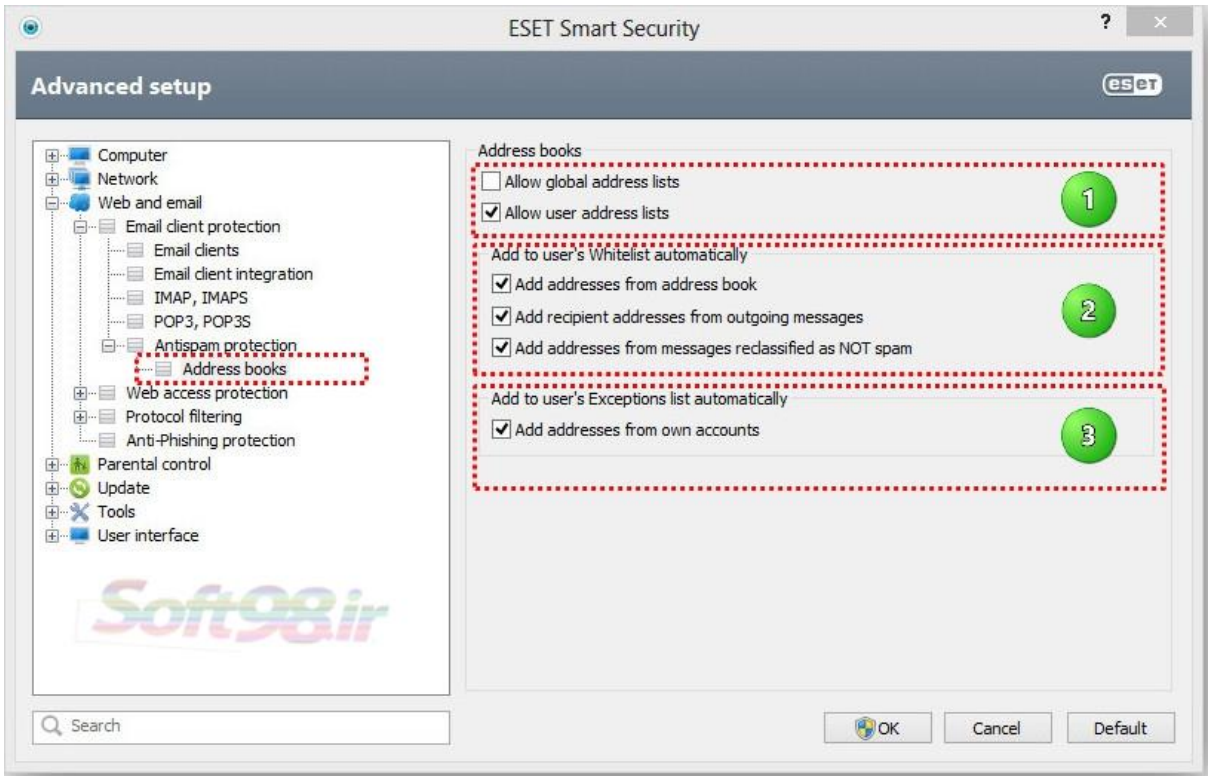
۳-Start email client antispam protection automatically

شروع اتوماتیک حفاظت antispam برای سرویس گیرنده های ایمیل

Allow advanced antispam control : فعال کردن کنترل پیشرفته antispam

با تیک دار کردن این گزینه دیتابیس های antispam دانلود خواهد شد و باعث افزایش قابلیت های antispam و تولید نتایج بهتر خواهد شد.

Address books



allow global address list : اجازه به فهرست آدرسهای جهانی

allow user address list : اجازه به فهرست آدرسهای کاربر

www.ParsBook.org

add addresses from list address book : اضافه کردن آدرسها از دفترچه آدرس

add recipient addresses from outgoing messages : اضافه کردن آدرس گیرنده از پیام های خروجی

add addresses from messages reclassified as not spam : اضافه کردن آدرس از پیامهای طبقه بندی مجدد مانند غیر اسپم

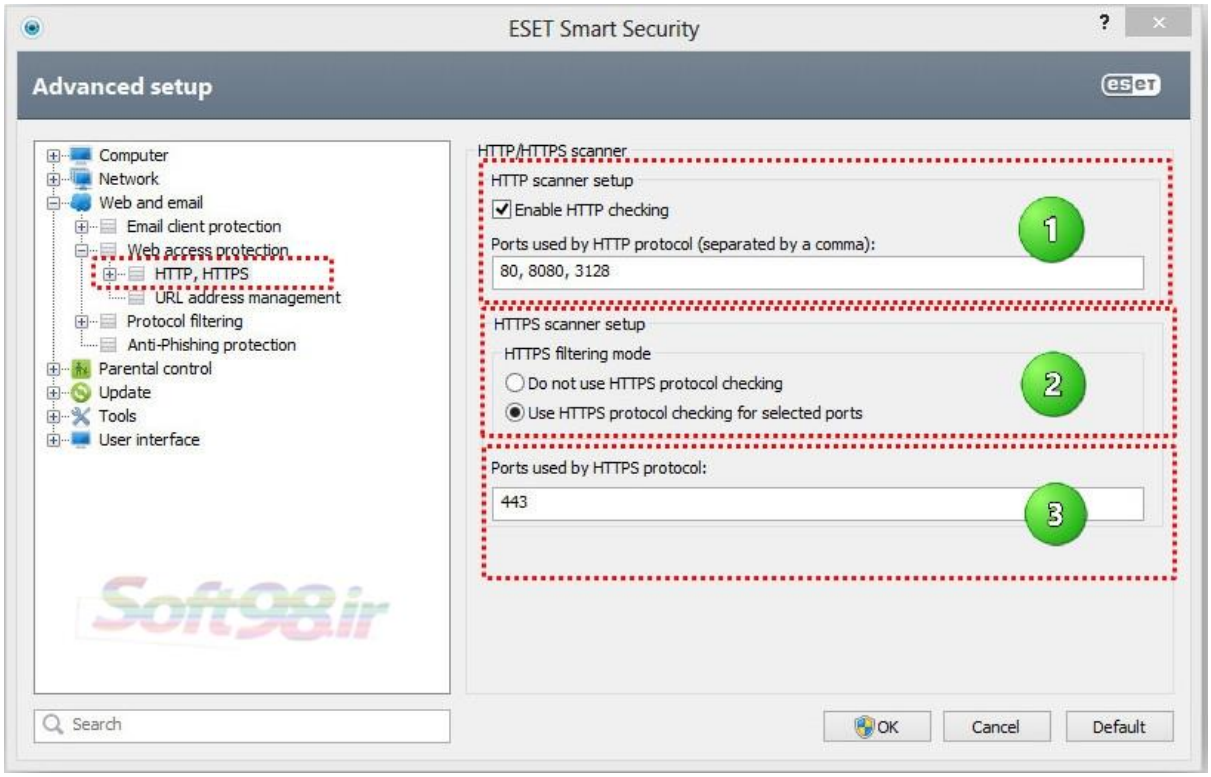
add addresses from own accounts : اضافه کردن آدرس از اکانتهای خود

Web access protection

اتصال به اینترنت از ویژگی های استاندارد برای کامپیوتر های شخصی است .متاسفانه اینترنت، رسانه اصلی برای توزیع کد های مخرب تبدیل شده است به همین دلیل دقت در تنظیمات حفاظت دسترسی به وب ضروری است. این نرم افزار با بهره گیری از متدهای ThreatSense تمامی نامه های ورودی را مورد تجزیه و تحلیل قرار می دهد.

www.ParsBook.org

HTTP , HTTPS



ویژگی اصلی"web access protection" کنترل ارتباطات بین برنام ههاي مرورگر وب و سرورهاي راه دور بر اساس قوانین پروتکل"HTTP" است.

۱-فعال کردن اسکنر پروتکل HTTP و انتخاب پورت مورد استفاده در پروتکل (پورتهای پیش فرض 3128 , 8080 ,80)

۲-فعال یا غیر فعال کردن اسکنر پروتکل HTTPS و انتخاب پورت مورد استفاده ی پروتکل

۳-پورت مورد استفاده در پروتکل HTTPS (پورت پیش فرض 443)

www.ParsBook.org

URL address managment

مدیریت آدرسهای URL شامل ۳ حالت کاری میشود :

List of addresses excluded from filtering-1 : لیست آدرس های خارج از فیلترینگ(به لحاظ کدهای مخرب مورد بررسی قرار نمی گیرند.)

List of allowed addresses-2 : لیست آدرسهای مجاز

List of blocked addresses-3 : لیست آدرسهای مسدود شده(نرافزار از دسترسی سایتهای موجود در این لیست جلوگیری می کند.)

Allow access only to URL addresses in the list of allowed addresses : با تیک این گزینه فقط اجازه دسترسی به آدرس های URLدر لیست آدرس های مجاز داده خواهد شد و بقیه سایتها مسدود خواهند شد.

List active : برای فعال کردن لیست مو جود

Notify when applying address from the list : اطلاع رسانی در هنگام استفاده از آدرسهای لیست

www.ParsBook.org

اضافه کردن یک سایت به عنوان سایت امن

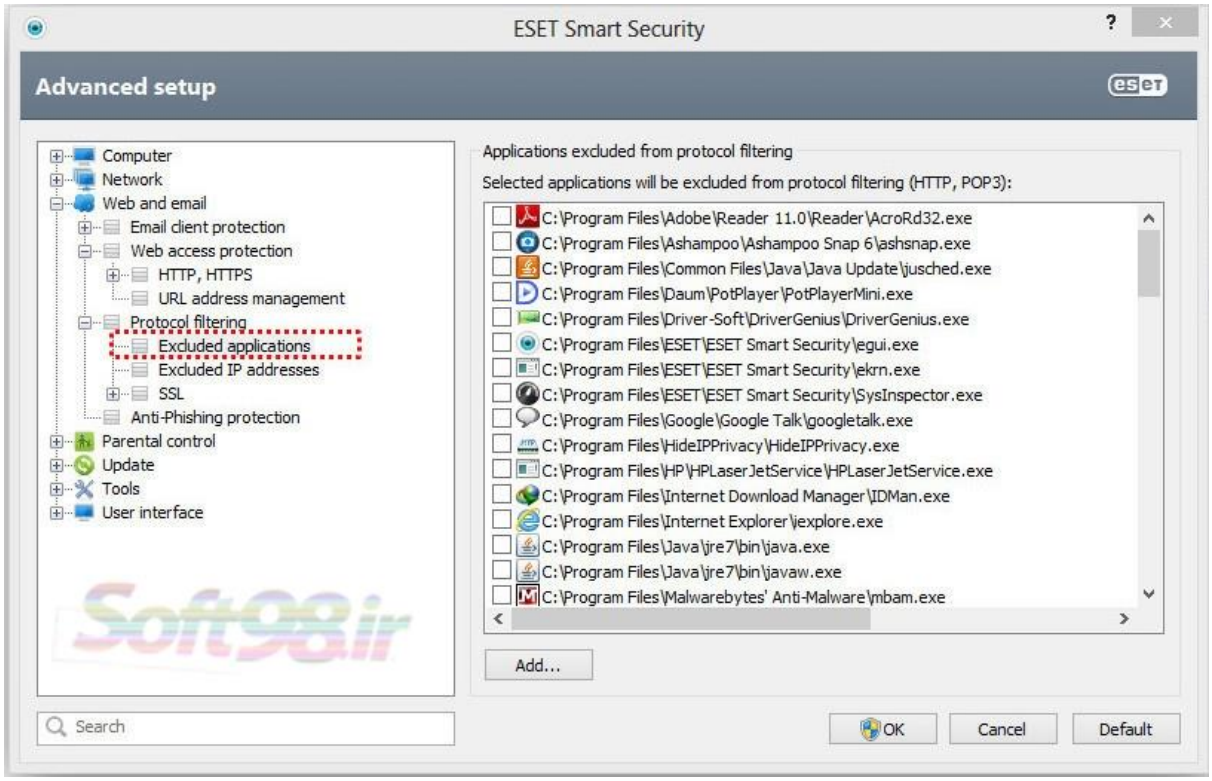
برای این کار در پنجره **URL address management** روی گزینه **add** کلیک میکنیم .در پنجره باز شده نام سایت مورد نظر را وارد می کنیم.حتما اول و آخر اسم سایت باید * وارد شود.به عنوان مثال برای معرفی سایت **soft98** به عنوان سایت امن باید بصورت ***soft98.ir*** وارد گردد.

آدرسهایی را که در فهرست "excluded"وارد شده اند در زمان دسترسی به لحاظ وجود کدهای مخرب مورد بررسی قرار نمی گیرند.

Protocol filtering

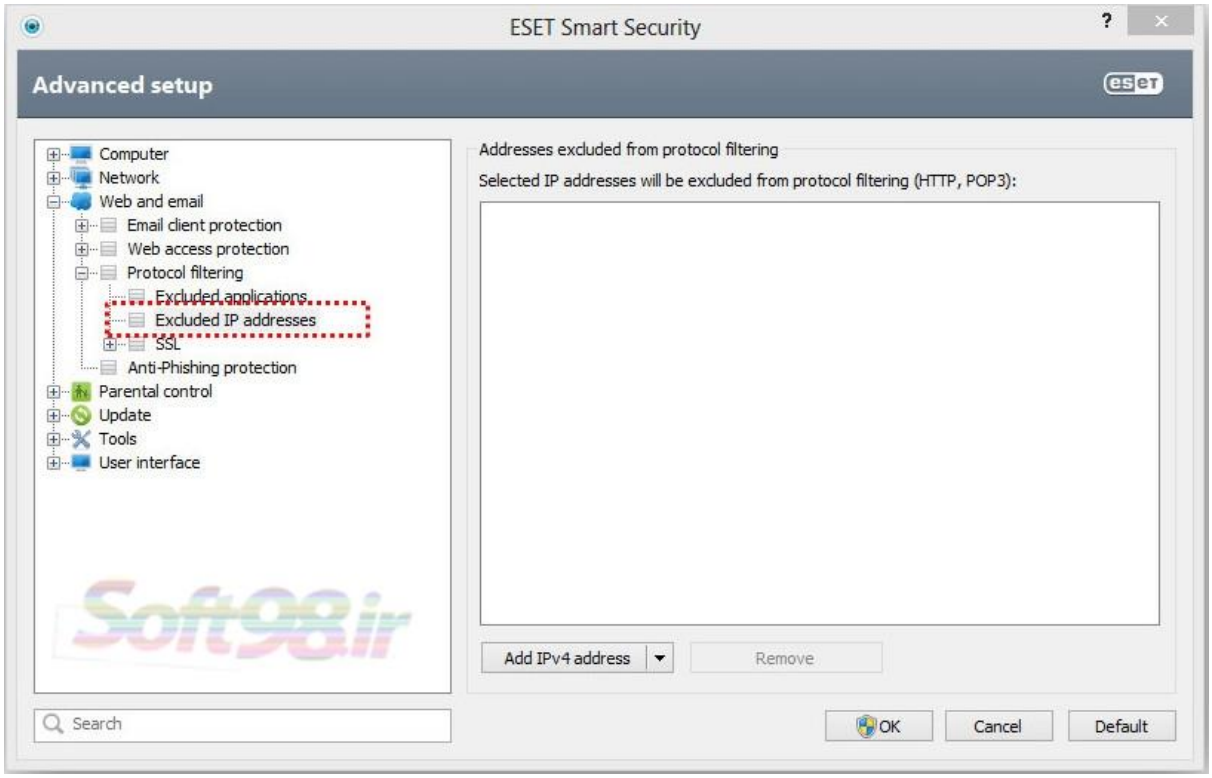
www.ParsBook.org

Excluded applications



برای حذف بررسی محتوای ارتباط برنامه ها با شبکه آنها را در لیست انتخاب کنید .ارتباط (HTTP/POP3/IMAP) برنامه های انتخاب شده برای تهدید بررسی نمی شود . **توصیه میشود از این گزینه فقط برای برنامه های شناخته شده و مطمئن استفاده شود.**

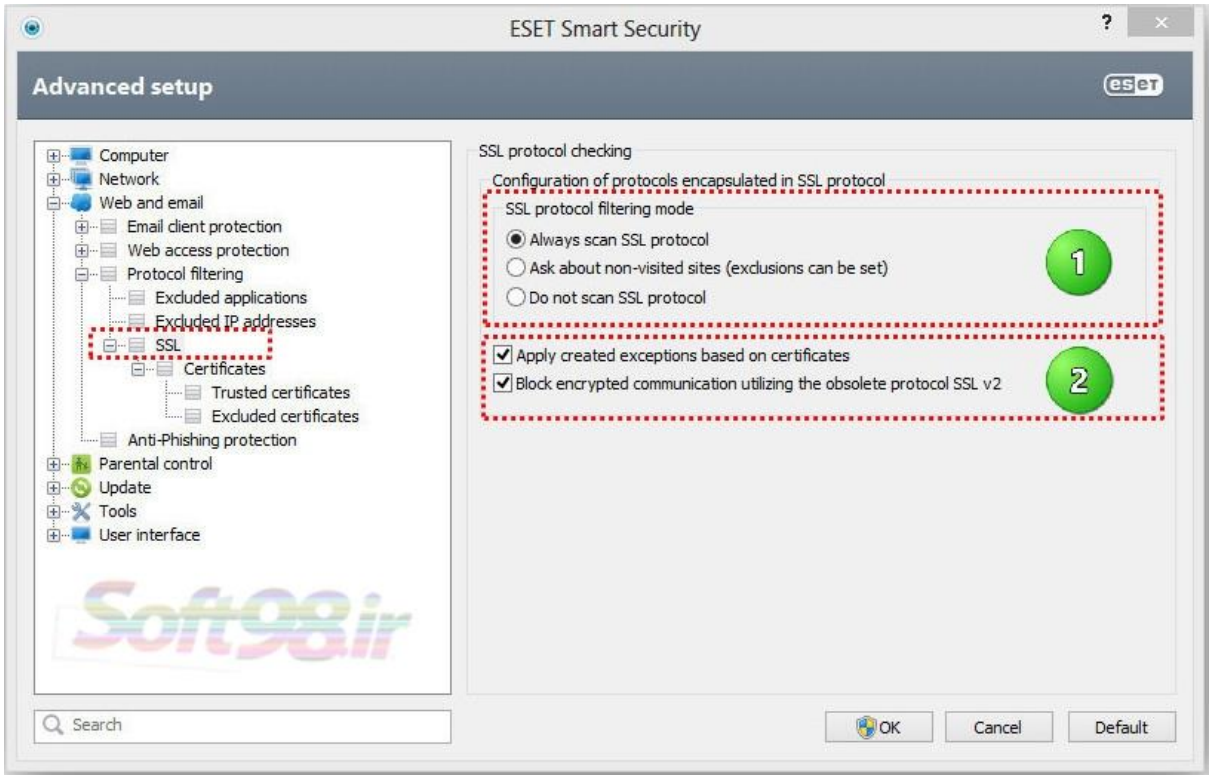
Excluded IP addresses



www.ParsBook.org

IP های موجود در لیست از پروتکل محتوای فیلترینگ حذف خواهد شد. بدین معنی که تمامی ارتباطات ارسالی و دریافتی (HTTP/POP3/IMAP) آدرس های انتخاب شده برای تهدیدات بررسی نمی شود. **توصیه می شود از این گزینه تنها برای آدرسهای شناخته شده و قابل اعتماد استفاده کنید.**

SSL



با استفاده از ESET Smart Security شما میتوانید پروتکل های محصور شده در پروتکل SSL را بررسی کنید.

توضیحات شماره ۱

Always scan SSL protocol : انتخاب این گزینه برای اسکن تمام ارتباطات محافظت شده SSL به جز ارتباطات حفاظت شده توسط گواهینامه های خارج از بررسی کردن.

Ask about non-visited sites : اگر شما وارد یک سایت محافظت شده با SSL(با گواهی ناشناخته)، پنجره محاوره ای انتخاب کردن ،نمایش داده میشود .این حالت شما را برای ایجاد یک لیست از گواهینامه های SSL که از اسکن حذف خواهد شد، قادر میسازد.

Do not scan SSL protocol : در صورت انتخاب، این گزینه ارتباطات SSL اسکن نخواهد شد.

توضیحات شماره ۲

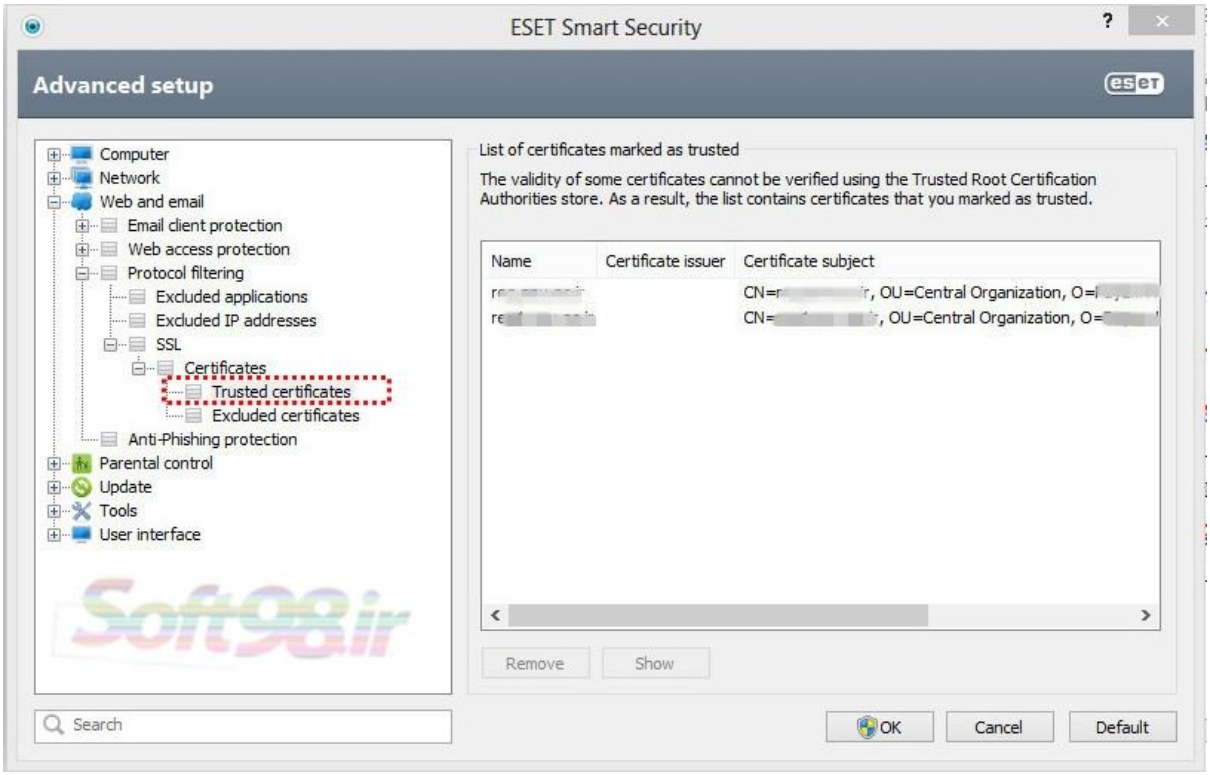
Apply created exceptions based on certificates : درخواست ایجاد استثنا بر اساس گواهینامه ها فعال کردن قسمت استفاده از محرومیت های مشخص شده، در گواهینامه های حذف شده و قابل اعتماد برای اسکن ارتباطات SSL

Block encrypted communication utilizing the obsolete protocol SSL v2 :

مسدود کردن ارتباط رمزنگاری شده با پروتکل SSL v2

www.ParsBook.org

Trusted certificates



در این قسمت شما می توانید یک لیست سفارشی از گواهینامه های قابل اعتماد درست کنید.

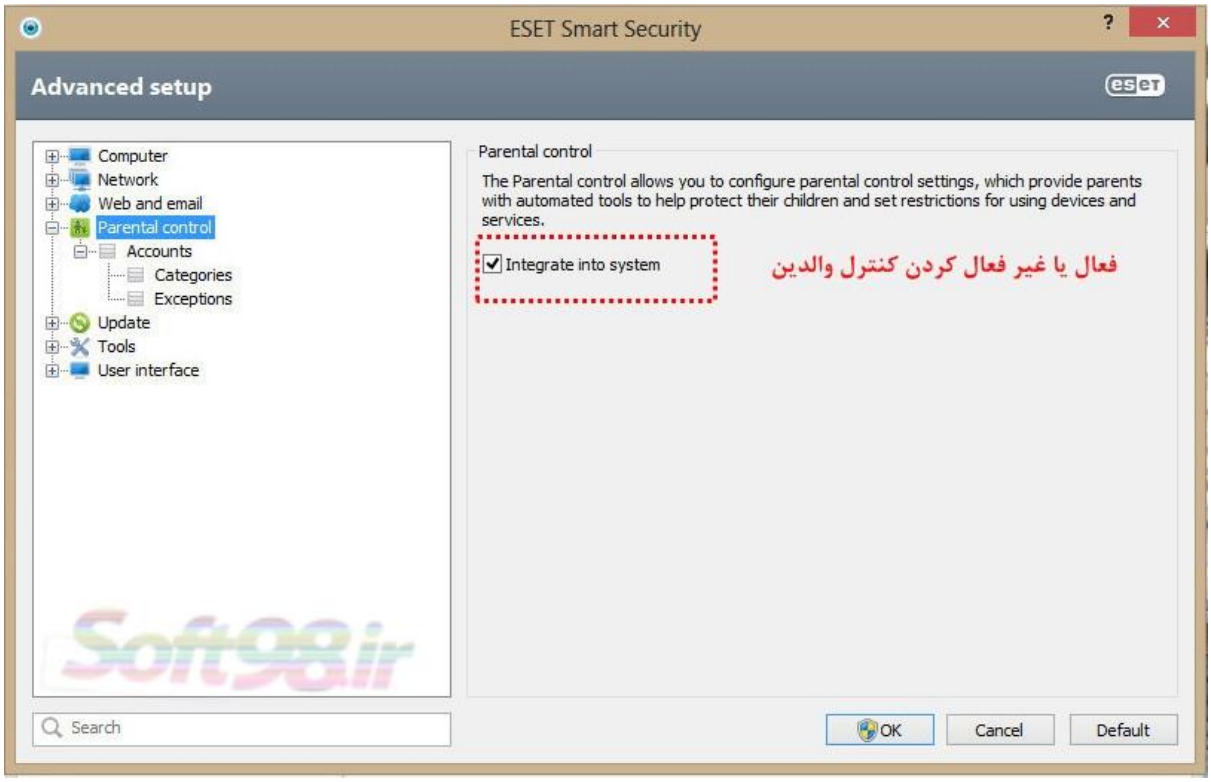
Excluded certificates

www.ParsBook.org

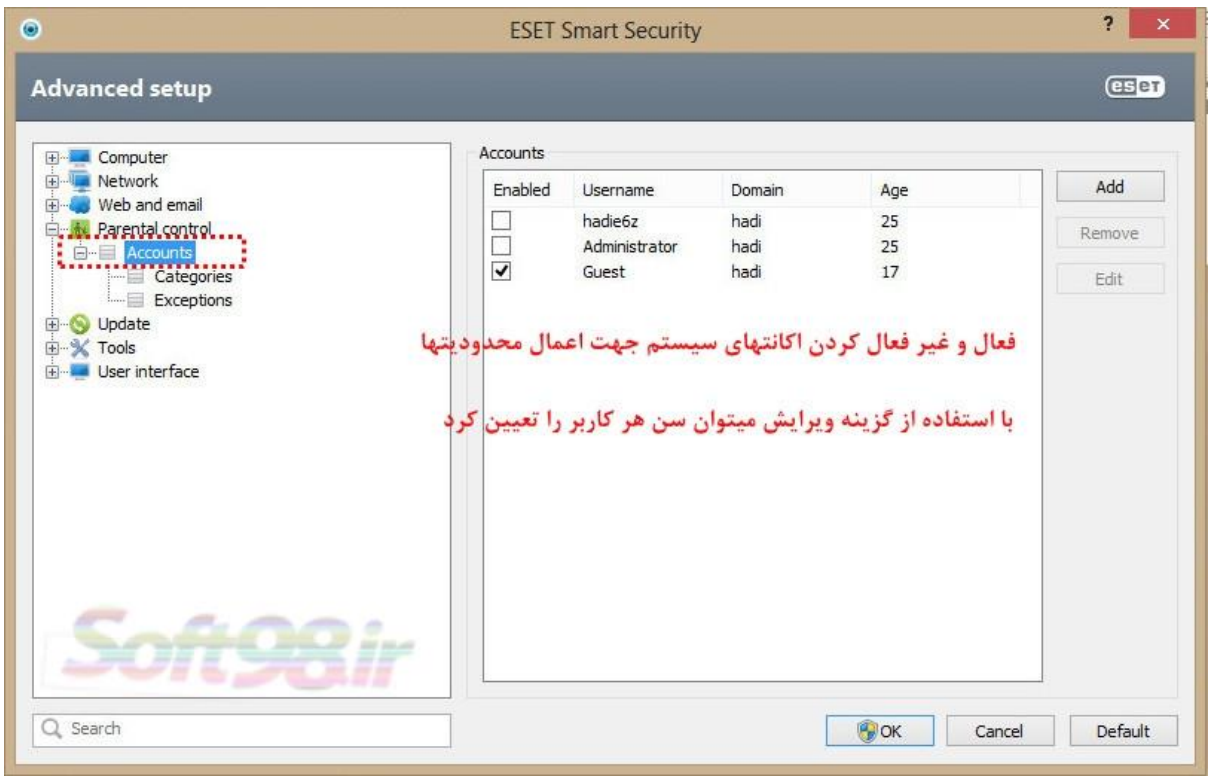
Anti-phishing protection

www.ParsBook.org

تنظیمات مربوط به قسمت Parental Control



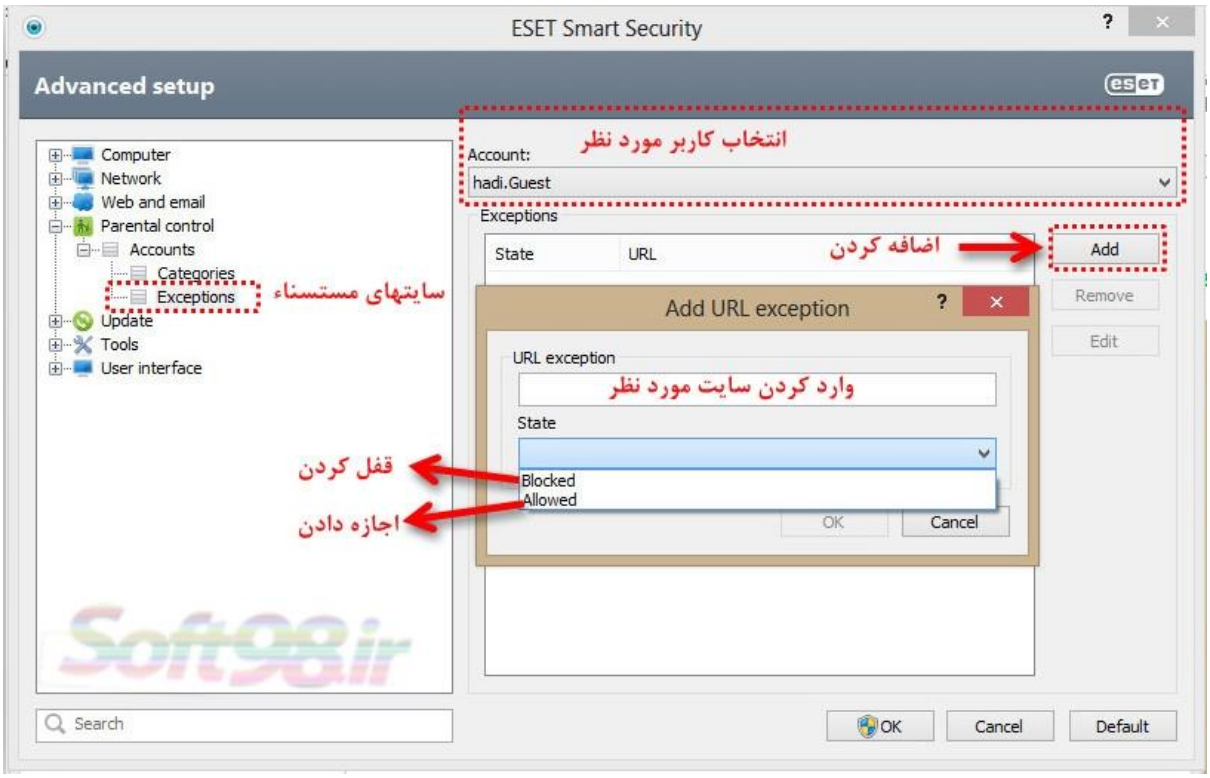
Parental Control



www.ParsBook.org

Categories

Exceptions



www.ParsBook.org

تنظیمات مربوط به قسمت Update

بروزرسانی مستمر سیستم، پایه اصلی در دستیابی به حداکثر سطح حفاظتی است. بروزرسانی شامل دو حالت میشود :

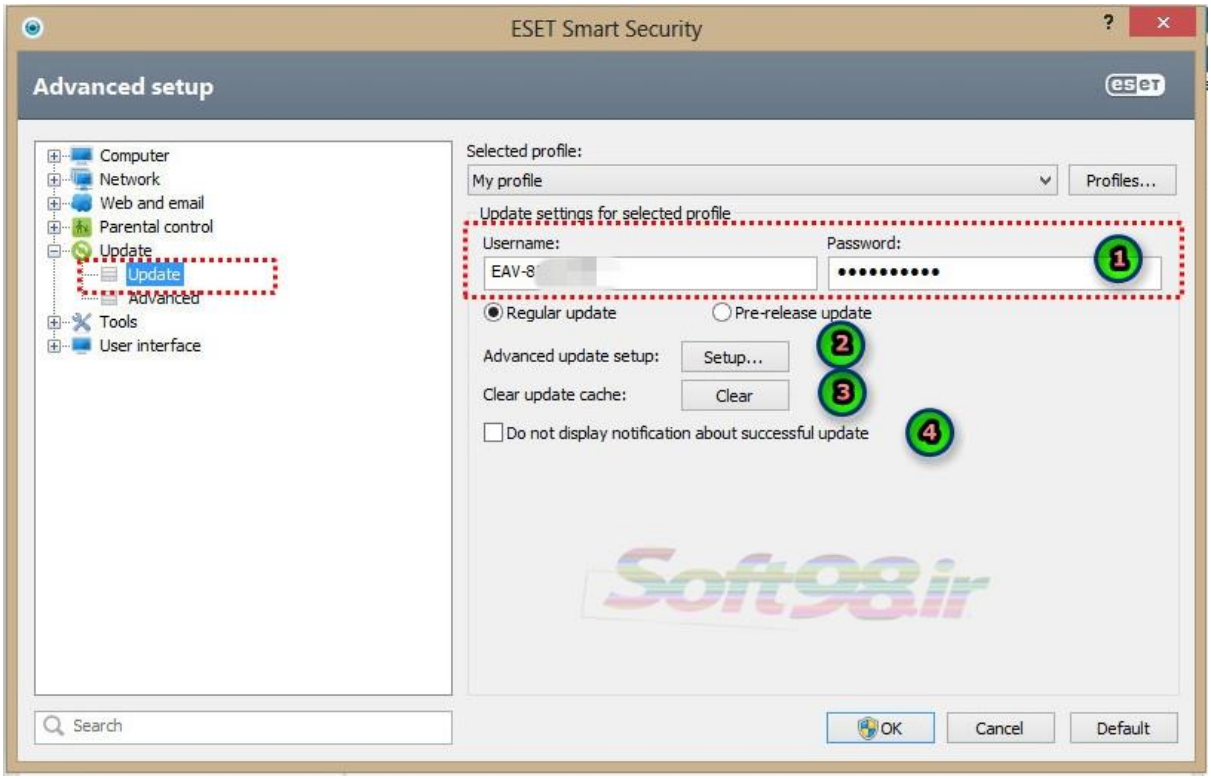
۱-بروزرسانی بانک اطلاعاتی شناسه ویروسهای رایانه ای(بروزرسانی دیتابیس)

۲-بروزرسانی کامل اجزای نرم افزار (بروزرسانی نسخه نرم افزار)

برای کسب اطلاعات در مورد وضعیت بروزرسانی نرم افزار کافی است بر روی گزینه"update"موجود در منوی اصلی نرم افزار کلیک کنید .این اطلاعات عبارت است از نسخه فعلی نرم افزار و شماره بانک اطلاعاتی شناسه ویروسهای رایانه ای و نیاز و یا عدم نیاز به بزورسانی نرم افزار می باشد.

www.ParsBook.org

تنظیمات مربوط به قسمت Update



۱-محل وارد کردن username و password

۲-تنظیمات پیشرفته update

۳-پاک کردن update Cache

۴-با تیک دار کردن این گزینه دیگر اخطار آپدیت موفق نمایش داده نمی شود.

مهم : یکی از کاربردی ترین قسمتهای نسخه های قبلی آپدیت آفلاین بود که با دادن آدرس فایلهای آپدیت، سیستم شروع به آپدیت دیتابیس خودش میکرد ولی در این نسخه قسمت update server حذف شده است.

پروفایلهای بروزرسانی:

کاربران می توانند با ایجاد پروفایلهای بروزرسانی متعدد از تنظیمات و پیکربندی های گوناگونی جهت انجام فرایند بروزرسانی استفاده به عمل آورند .ایجاد این نوع پروفایلها برای کاربرانی که نرم افزار را بر روی رایانه همراه خود نصب نموده اند، بسیار بهتر و موثرتر است .زیرا پیکربندی تنظیمات اینترنت این نوع کاربران دائما از نقطه ای به نقطه دیگر تغییر می کند و لذا اگر برای هر محل، تنظیمات مربوطه را در قالب یک پروفایل بروزرسانی ذخیره سازی کنند، با هیچ مشکلی در طی فرایند بروزرسانی روبرو نخواهند شد.

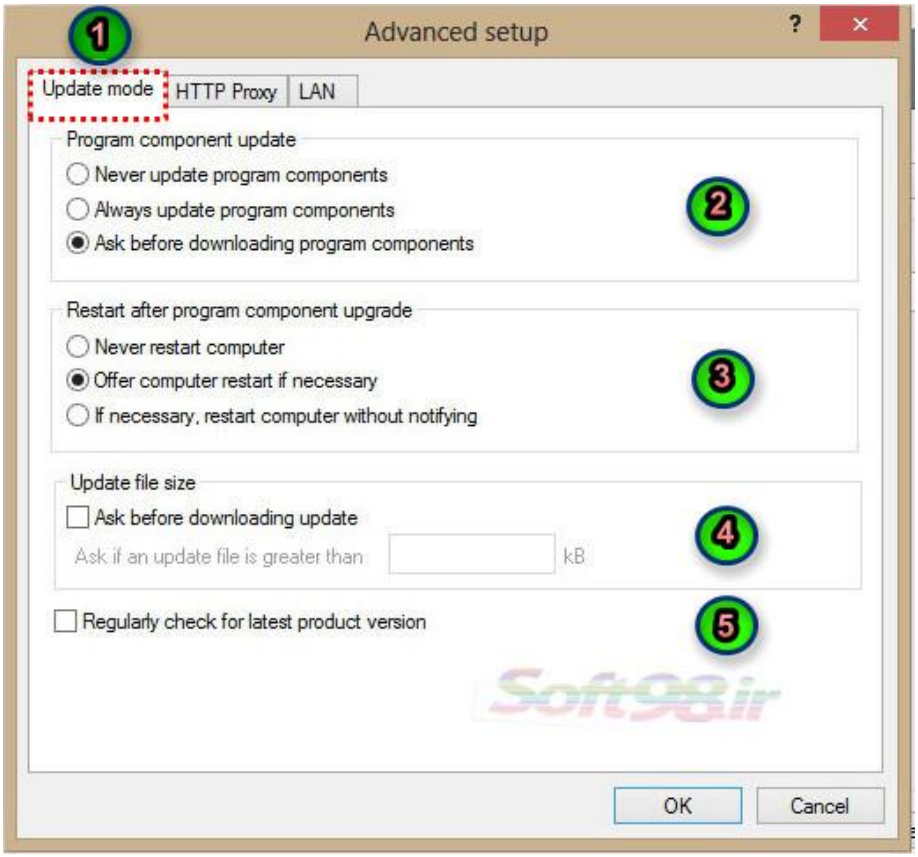
منوی بازشونده"selected profile"نمایانگر پروفایل انتخاب شده جاری است .به صورت پیش فرض این گزینه بر روی گزینه"my profile"تنظیم گردیده است .به منظور ایجاد یک پروفایل جدید کافی است بر روی دکمه"profiles..."کلیک کرده و سپس گزینه"add..."را برگزینید و پس از آن نامی را برای پروفایل جدید ثبت نمائ ید . در زمان ایجاد یک پروفایل جدید قادرخواهید بود تا تنظیمات مربوط به هر یک از پروفایلهای موجود را با استفاده از منوی بازشونده "copy settings from profile" کپی نموده و مورد استفاده قرار دهید.

www.ParsBook.org

تنظیمات پیشرفته بروزرسانی:

جهت مشاهده تنظیمات پیشرفته بروزرسانی کافی است بر روی دکمه"setup..." کلیک نمائید .با انجام این کار پنجره ای باز می شود که حاوی سربرگهای حالت بروزرسانی "LAN" ، "HTTP proxy"، (update mode) است.

سربرگ "update mode"



"program component update"

اطلاعات موجود در این قسمت شامل گزینه هایی است که با بروزرسانی اجزا ی نرم افزار مرتبط هستند . در قسمت "program component update" سه گزینه وجود دارد که عبارتند از:

۱-عدم بروزرسانی اجزای نرم افزار

۲-بروزرسانی همیشگی اجزای نرم افزار

۳-اجازه از کاربر در مورد دانلود اجزای نرم افزار

www.ParsBook.org

"restart after program component upgrade"

پس از بروزرسانی اجزای نرم افزار لازم است تا سیستم راه اندازی مجدد گردد تا ماژولهاییبروز شده بتوانند به صورت کامل وظایف خود را به انجام رسانند .در قسمت "restart after program component upgrade" سه گزینه زیر وجود دارد:

۱-عدم راه اندازی مجدد رایانه

۲-ارائه پیشنهاد به راه اندازی مجدد رایانه در صورت نیاز

۳-راه اندازی مجدد رایانه در صورت نیاز بدون اطلاع قبلی به کاربر.

Update file size

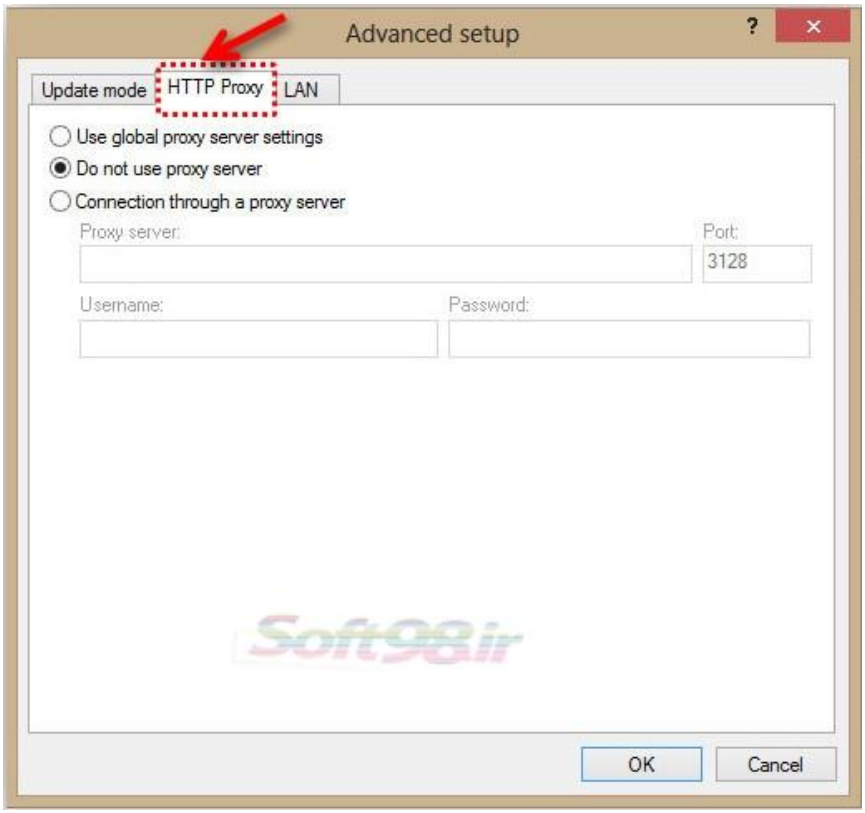
در این قسمت میتوان یک محدودیت حجمی دانلود آپدیت ، قبل از دانلود را فراهم کرد.

با تیک دار کردن گزینه Ask before downloading update این قابلیت فعال شده و با وارد کردن حجم مورد نظر با واحد KB این محدودیت اعمال می شود. بدین شکل که اگر از حجم آپدیت از مقدار وارد شده بیشتر باشد از کاربر برای دانلود اجازه گرفته می شود.

Regulary check for latest product version

با تیک دار کردن این گزینه بطور منظم بررسی برای نسخه جدید نرم افزار انجام می شود.

سرور "proxy"



گزینه های موجود:

۱-استفاده از تنظیمات سرور "proxy" اصلی(global)

۲-عدم استفاده از سرور "proxy"

۳-اتصال از طریق یک سرور "proxy"

www.ParsBook.org

با انتخاب **گزینه اول** از گزینه های مربوط به پیکربندی سرور"proxy" در قسمت"proxy server" پنجره تنظیمات پیشرفته استفاده به عمل خواهد آمد.

با انتخاب **گزینه دوم** از هیچ سرور"proxy" استفاده نمی شود.

گزینه سوم زمانی استفاده می شود که کاربر برای بروزرسانی از یک سرور"proxy"بجز آن سروری که در پنجره تنظیمات پیشرفته نرم افزارمشخص کرده است، استفاده می نماید .بنابراین برای این کار باید کاربر اطلاعات مربوط به این سرور"proxy"از جمله آدرس، پورت ارتباطی و در صورت نیاز username و password مرتبط را در فیلدهای مربوطه وارد کنید.

اتصال به شبکه "LAN"

همانطور که می دانید اگر عملیات بروزرسانی از روی یک سرور محلی دارای سیستم عامل مبتنی بر شبکه(NT–based) انجام می پذیرد،به صورت پیش فرض تمامی ارتباطات ایستگاه های کاری با سرور پس از تائید اعتبار برقرار می گردند.

با انتخاب گزینه"system account"از حساب کاربری سیستمی جهت تائید اعتبار استفاده می شود .معمولا اگر هیچ نوع اطلاعاتی در زمینه تائید اعتبار در قسمت تنظیمات بروزرسانی درج نشده باشد، عملیات مربوط به تائید اعتبار صورت نخواهد پذیرفت.

www.ParsBook.org

به منظور اطمینان از اینکه نرم افزار جهت تائید اعتبار از اطلاعات کاربری که در حال حاضر به شبکه متصل است استفاده به عمل خواهد آورد نیز م یتوان گزینه"current user" را برگزید .ایراد این روش آن است که نرم افزار نصب شده بر روی ایستگاه کاری درصورتی که هیچ کاربری از طریق آن ایستگاه به شبکه وصل نشده باشد، قادر به اتصال و دریافت فایلهای بروزرسانی نخواهد بود.

کاربران می توانند برای بروزرسانی نرم افزار از طریق تائید اعتبار یک حساب کاربری خاص، شناسه کاربری و کلمه عبور آن حساب را در قسمت"specified user" وارد کنند.

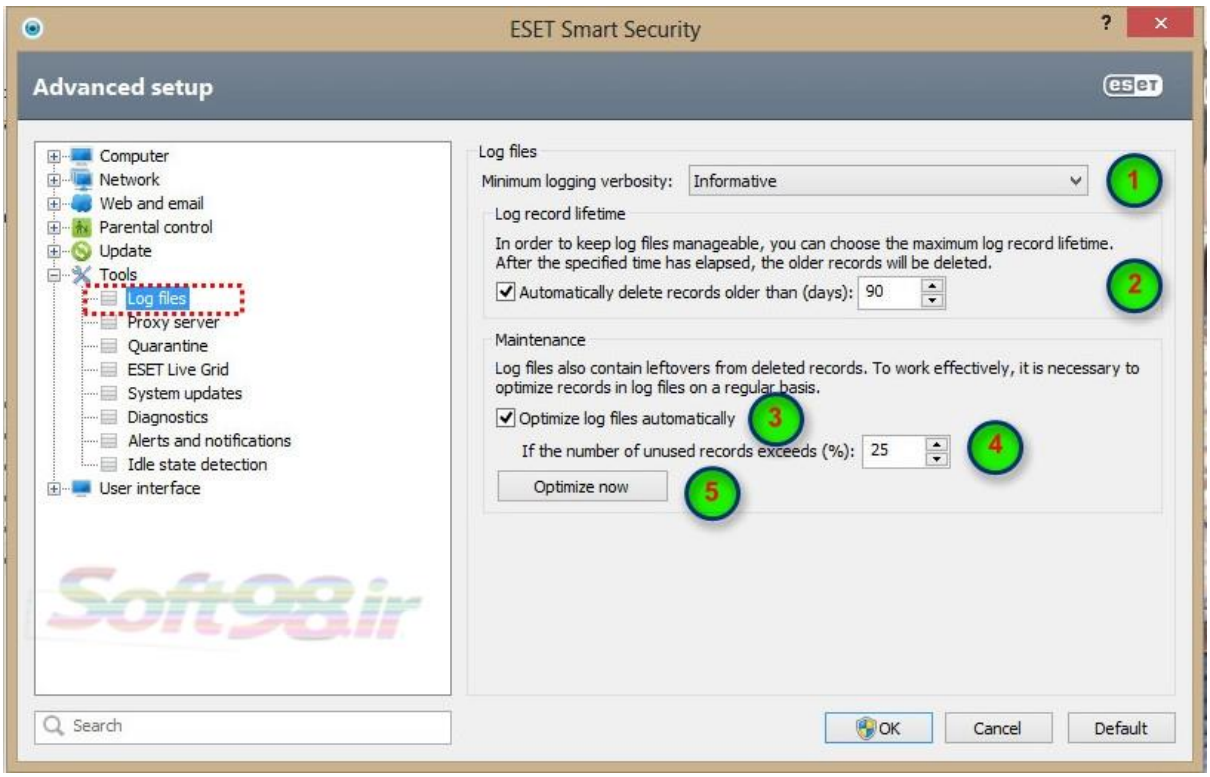
Advanced

www.ParsBook.org

تنظیمات مربوط به قسمت Tools

Log files

با استفاده از فایلهای ثبت رخدادها(log files) می توان تمامی رخدادهای مهم مربوط به نرم افزارو همچنین اطلاعات مربوط به تهدیدات شناسایی شده را مرور نمود.



۱- جهت مشخص کردن سطح"logging verbosity" مورد استفاده قرار می گیرد .گزینه های موجود در اینجا عبارتند از:

Diagnostic : تمامی رکوردها به علاوه اطلاعات مورد نیاز جهت تنظیم بهینه نرم افزار را ثبت خواهد کرد.

Informative : تمامی رکورد ها واطلاع رسانی پیام ها، از جمله پیام های بروز رسانی موفقیت آمیز را ثبت خواهد کرد.

Warnings : خطا هایی بحرانی و پیام های هشدار دهنده را ثبت خواهد کرد.

Errors : " خطا در دانلود فایل و خطاهای بحرانی را ثبت خواهد کرد.

Critical : فقط رخدادهای خطاهای بحرانی (خطا ی شروع آنتی ویروس، Personal firewall ، و غیره...) را ثبت خواهدکرد.

۲- جهت تنظیم زمان حذف اتوماتیک رخدادهای ثبت شده قدیمی

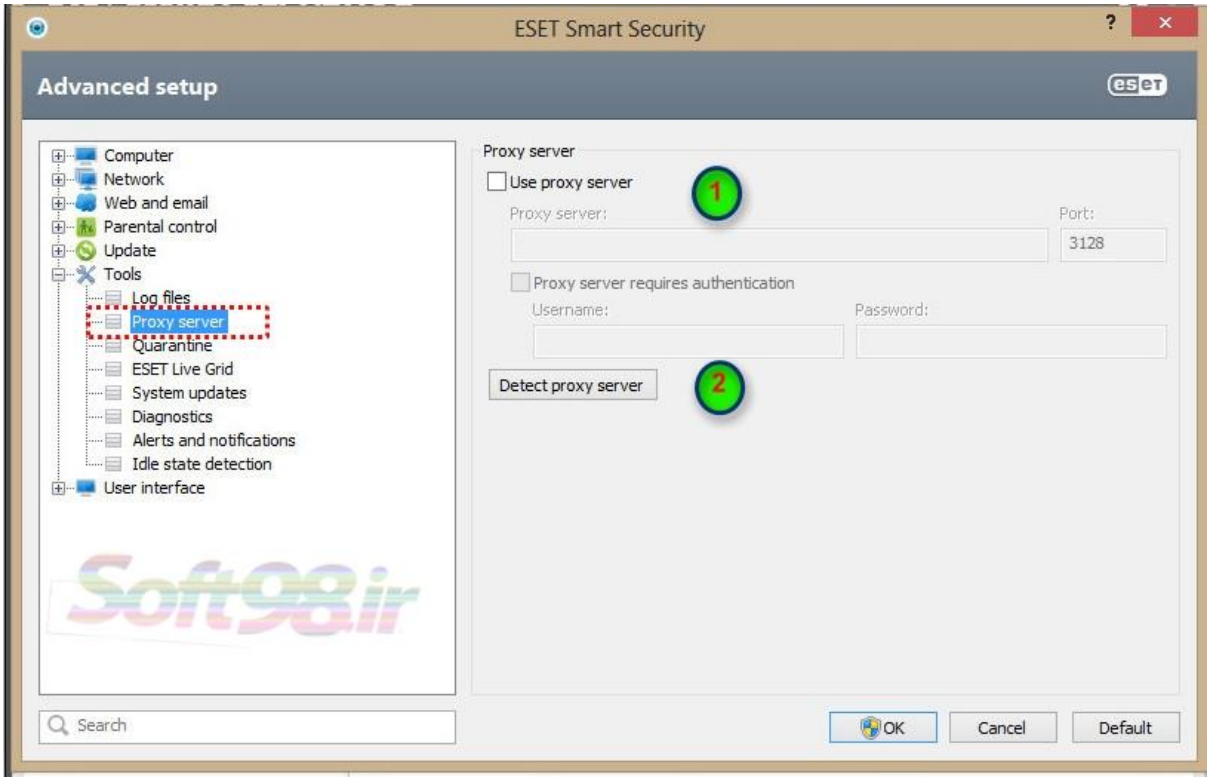
۳- فعال کردن بهینه سازی خودکار فایل های ثبت رخداد

۴- درصد ذکر شده مربوط به عدم استفاده از رخدادهایی که اتفاق می افتد.

۵- شروع به بهینه سازی

www.ParsBook.org

Proxy server



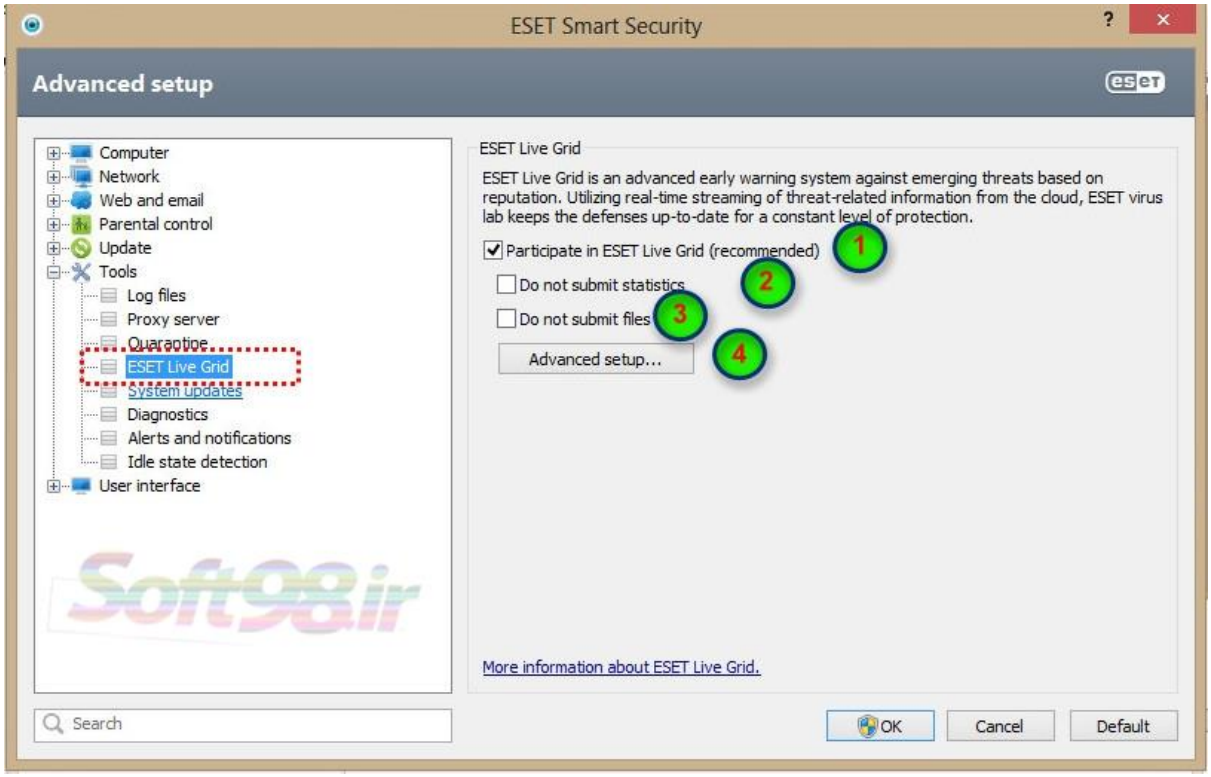
۱-فعال کردن سرور پروکسی

در این قسمت باید آدرس سرور و شماره پورت را وارد کرد. درصورتی که سرور دارای یوزر و پسورد باشد باید تیک گزینه مربوطه را فعال کرده و یوزر و پسورد را درج کرد.

۲-شناسایی سرور پروکسی

Quarantine

www.ParsBook.org



۱- مشارکت در شبکه زنده ESET

فعال یا غیر فعال کردن شبکه زنده ESETکه وظیفه آن ارسال فایل های مشکوک و ناشناس و اطلاعات آماری به آزمایشگاه ESET است.

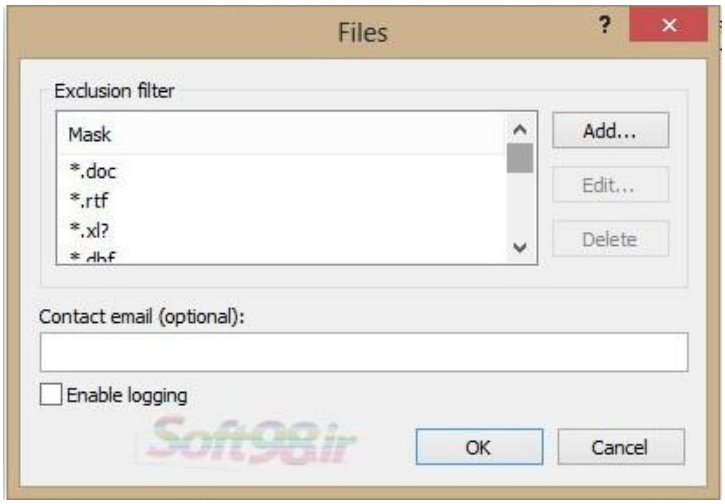
۲-عدم ارسال آمار

اطلاعات ارسالی مربوط به تهدیدی که به تازگی کشف شده می باشد که ممکن است شامل نام نفوذکننده و اطلاعات تاریخ و زمان آن باشد. نسخه ESET Smart Securityاین اطلاعات را که شامل نسخه سیستم عامل کامپیوتر شما و تنظیمات مکان است در خود نگاه می دارد و این آمار به طور معمول یک یا دو بار در روز به سرور ESET تحویل می دهد.

۳-عدم ارسال فایلها

در صورت تیک دار نبودن این گزینه فایل های مشکوک، یا مواردی که رفتاری شبیه نفوذ در محتوا دارند برای تجزیه و تحلیل با استفاده فن آوری شبکه زنده ESETبه شرکت ESET فرستاده می شوند.

۴-تنظیمات پیشرفته ESET Live Grid

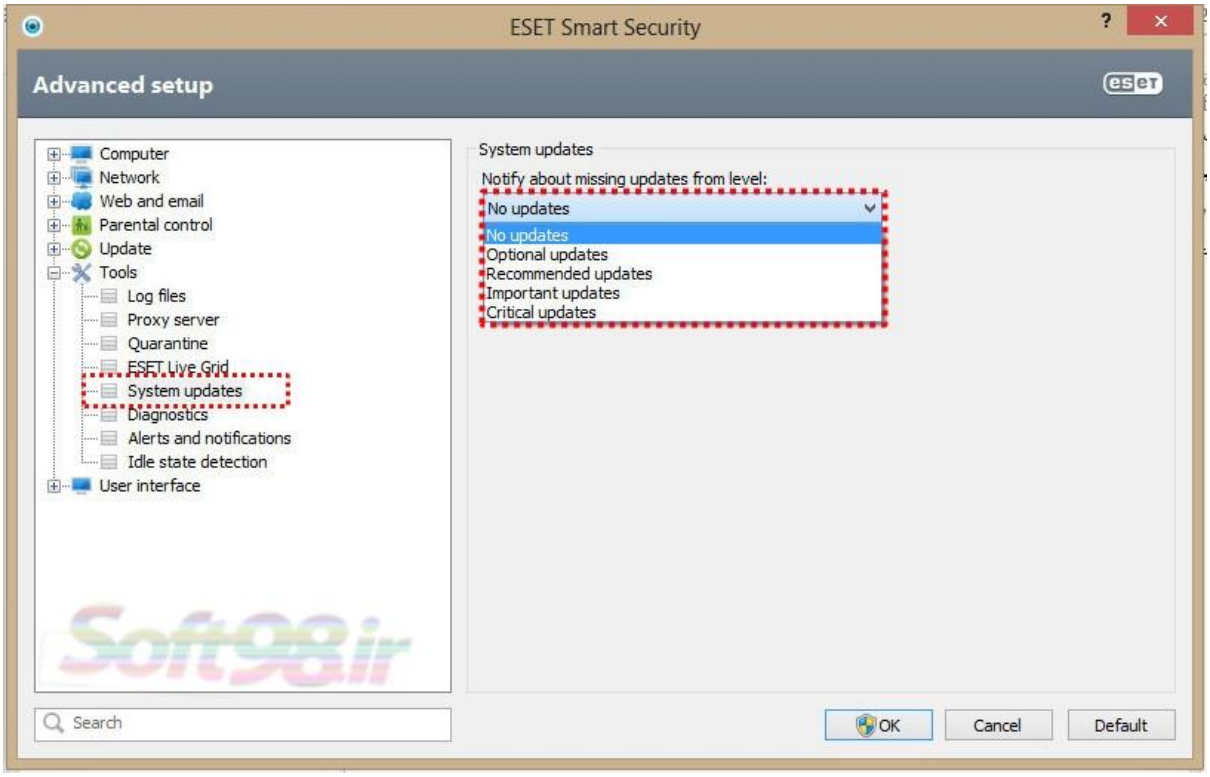


فیلتر حذف(Exclusion filter)

کاربران می توانند با استفاده از این ویژگی فایلهایی که تمایلی به ارسال آنها ندارند را مشخص نمایند . به صورت پیش فرض برخی ازفایلهای اسنادی در فهرست حذف از ارسال ثبت گردیده اند و کاربر می تواند در صورت نیاز انواع دیگری از فایلها را به این فهرست اضافه کند.

پست الکترونیک(contact email)

آدرس پست الکترونیکی ثبت شده در این قسمت در کنار فایلهای مشکوک ارسال می گردد تا اگر نیاز به جزئیات بیشتری برای تجزیه و تحلیل آیتم های دریافتی بود، از طریق این آدرس بتوان با کاربر ارتباط برقرار کرد.



No updates : بدون بروزرسانی

Optional updates : بروزرسانی هایی که به عنوان اولویت کم و زیاد برای دانلود ارائه شده است.

Recommended updates : بروزرسانی هایی که به عنوان مشترک و بالاتر برای دانلود ارائه شده است.

Important updates : بروزرسانی هایی که به عنوان مهم و بالاتر برای دانلود ارائه شده است.

Critical updates : فقط بروزرسانی بحرانی

Diagnostics

این قابلیت تمامی پروسه های ESET را در موقع crash تخلیه می کند. (به عنوان مثال ekrn) این قابلیت می تواند به توسعه دهندگان برای اشکال زدایی و رفع مشکلات مختلف ESET Smart Securityکمک کند.

Do not generate memory dump : به صورت پیش فرض غیر فعال است.

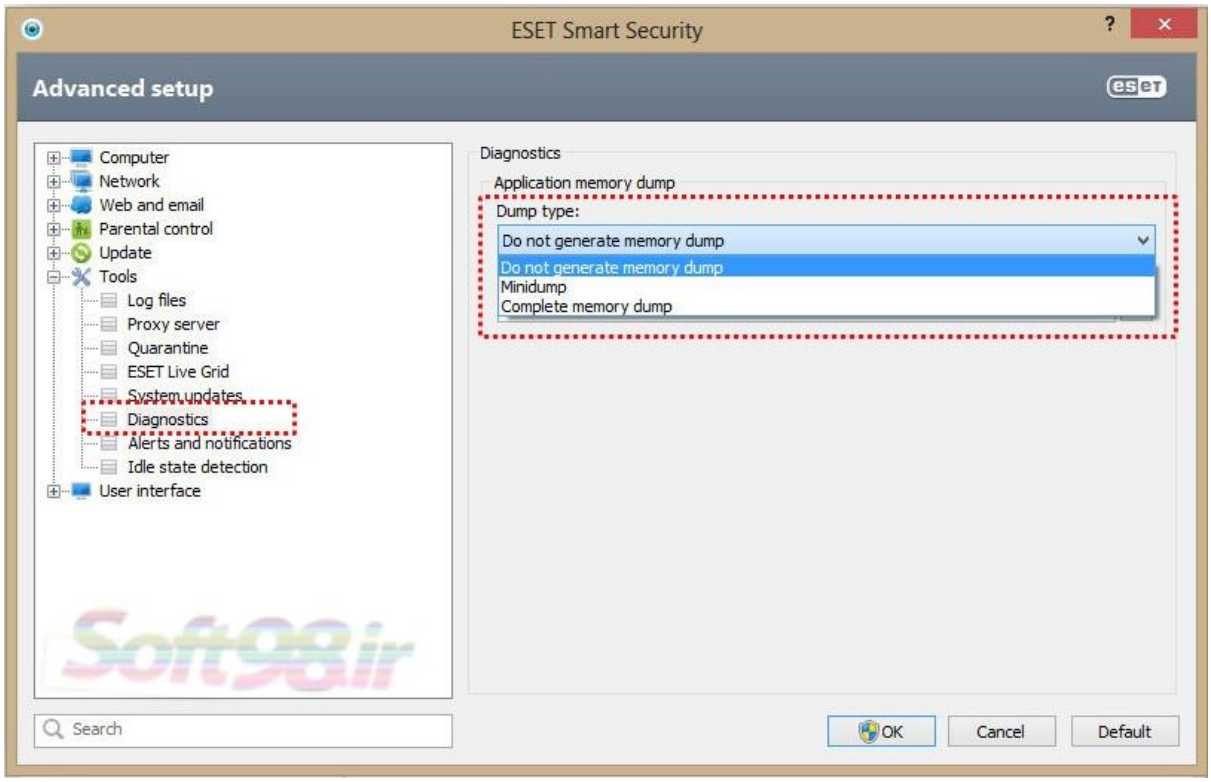
Minidump : ثبت کوچکترین اطلاعات مفید که شاید به تشخیص قفل غیر منتظره این نرم افزار کمک کند .این نوع تخلیه فایل می تواند زمانی که فضا محدود است.مفید واقع شود هرچند که با وجود اطلاعات محدود فایل ،ممکن است با تجزیه و تحلیل از این فایل ، خطا کشف نشود.

www.ParsBook.org

Complete memory dump :

ثبت تمام محتویات حافظه سیستم، زمانی که برنامه به طور غیر منتظره ای متوقف می شود.

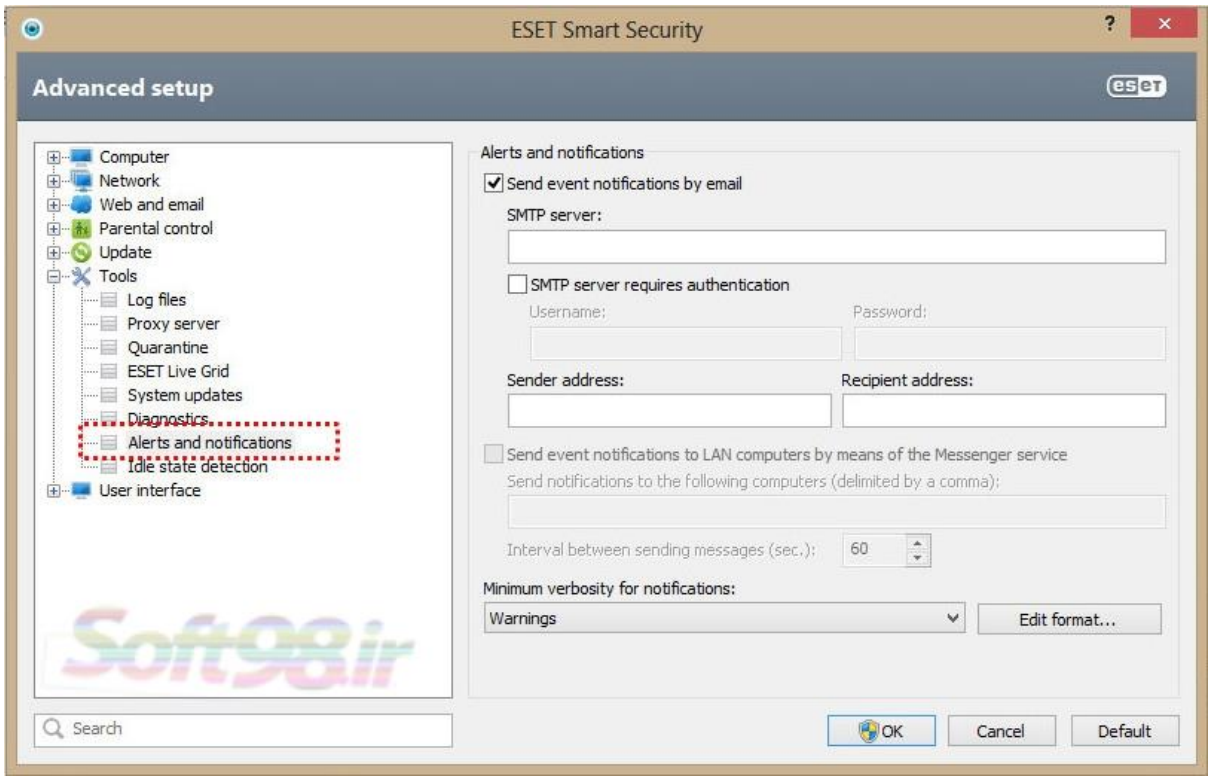
complete memory dump ممکن است اطلاعاتی از پروسه های در حال اجرا ،زمان تخلیه حافظه را جمع آوری کند.



Alerts and notifications

Alerts and notifications قابلیتی است که اگریک رویداد با سطح verbosity رخ دهد،یک ایمیل ارسال شود.

با تیک دار کردن این گزینه ، می توان این قابلیت را فعال کرد.



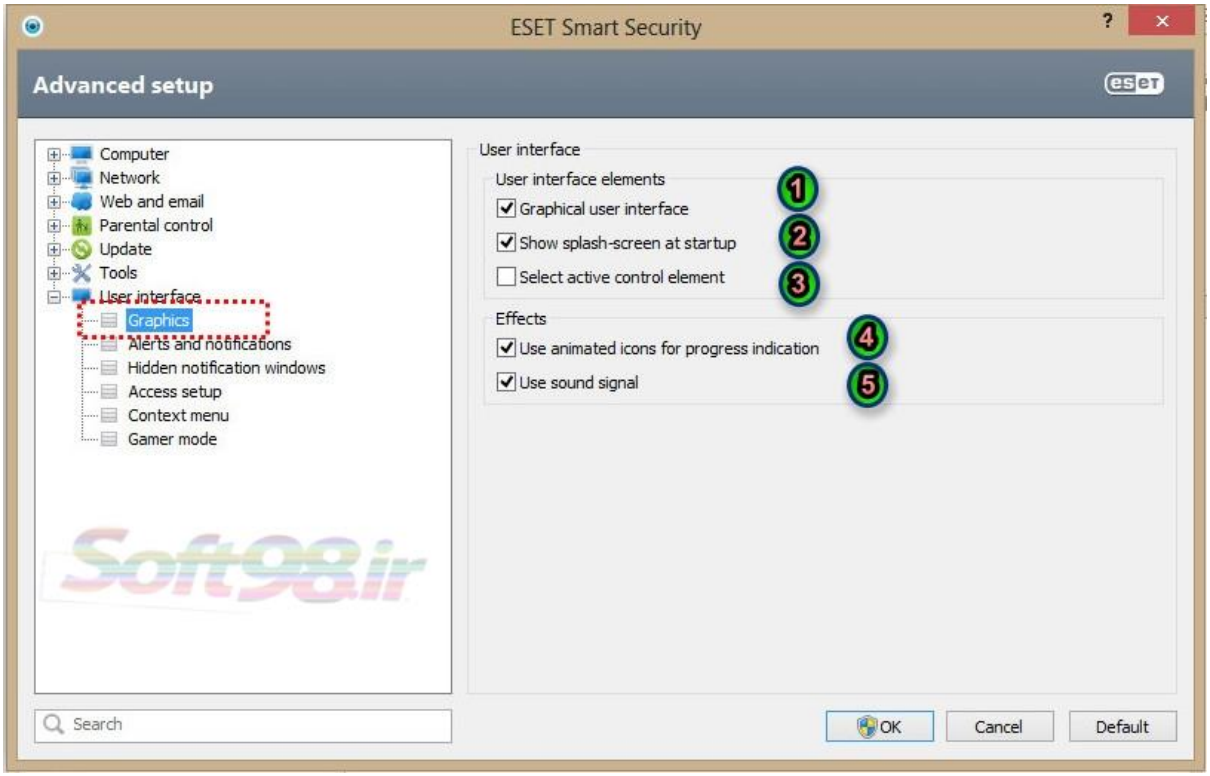
www.ParsBook.org

Idle state detection

www.ParsBook.org

تنظیمات مربوط به قسمت User interface

Graphics



۱-با تیک دار بودن این گزینه رابط کاربری حالت گرافیکی بهتری دارد.

۲-این گزینه جهت نمایش صفحه Splash (صفحه شروع بکار اولیه نرم افزار) در حالت راه اندازی کامپیوتر است.

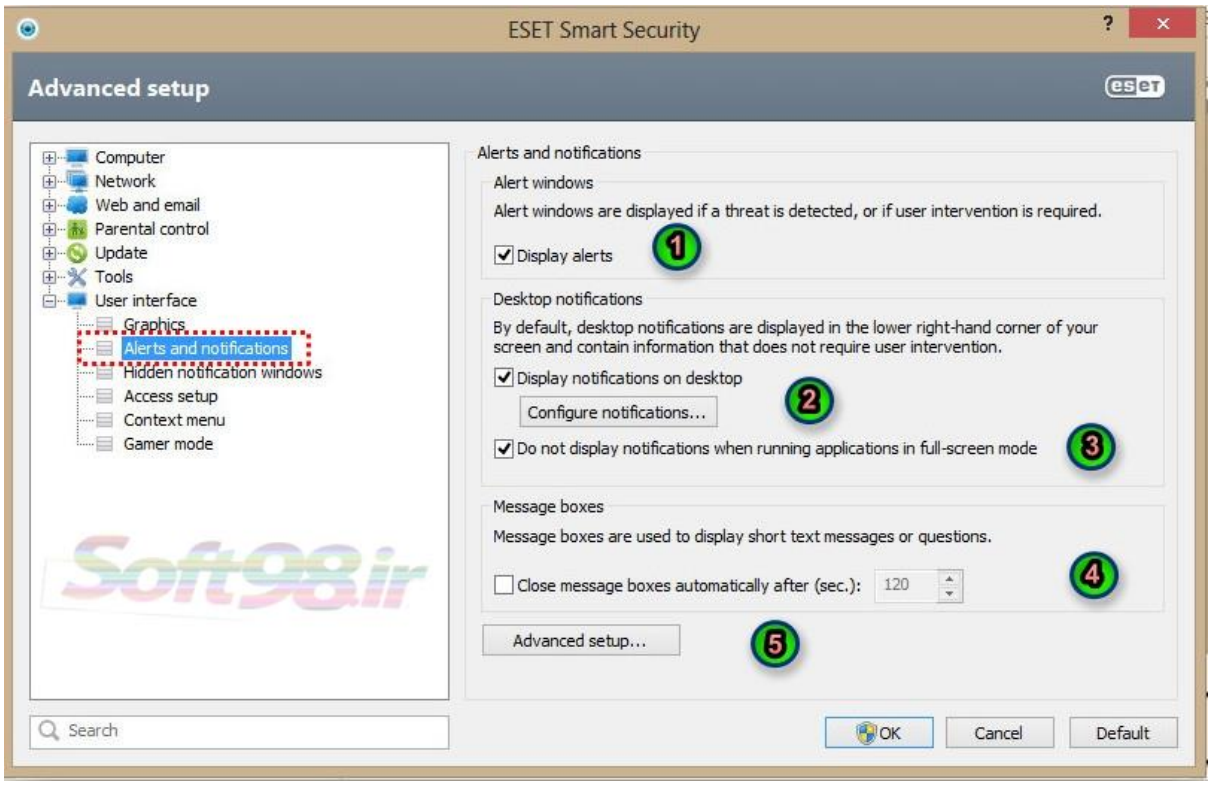
۳- فعال نمودن گزینه"select active control element" باعث میشود هر یک از المانهایی که در منطقه فعال نشانگر ماوس هستند، های لایت گردند . ضمن اینکه پس از کلیک ماوس ، آیتم های لایت شده فعال می گردد .

۴- جهت فعال ساختن آیکون های انیمیشنی نشان دهنده پیشرفت هر یک ازعملکردهای نرم افزار نیز کافی است گزینه "use animated icons for progress indication" را انتخاب نمائید.

۵- برای اینکه نرم افزار از طریق هشدار صوتی وقوع رخدادهای مهم را به اطلاع کاربر برساند باید گزینه "use sound signal" را انتخاب کنید.

www.ParsBook.org

Alert and notification



گزینه"alerts and notifications setup" به کاربر امکان میدهد تا بتواند پیکربند ی تنظیمات مربوط به پیا مهای هشدار و همچنین پیام های آگاهی رسانی را پیکربندی نماید.

۱- غیر فعال کردن این گزینه باعث لغو شدن نمایش پنجر ههای هشدار نرم افزار گردیده و صرفا در موارد بسیار خاص به هیچ وجه توصیه نمی گردد .لذا به کاربران توصیه می شود تا این گزینه در حالت پیش فرض (فعال) خود قرار داشته باشد.

۲- توجه داشته باشید که پیام های آگاهی رسانی و همچنین بالن های حاوی نکات مهم که صرفا جنبه اطلاع رسانی داشته و لذا تداخلی با امور جاری کاربر ندارند و نیازی نیست که کاربر نسبت به بستن آن ها و ... کاری انجام دهد . این پنجره ها در قسمت گوشه سمت راست صفحه نمایش نشان داده می شوند. جهت فعال شدن قابلیت نمایش پنجره های آگاهی رسانی بر روی میز کار رایانه(desktop) باید تیک گزینه "display notifications on desktop" زده شود.
جهت انجام تنظیمات بیشتر مربوط به این پیا مها نیز کافی است بر روی گزینه"configure notifications" کلیک کنید.

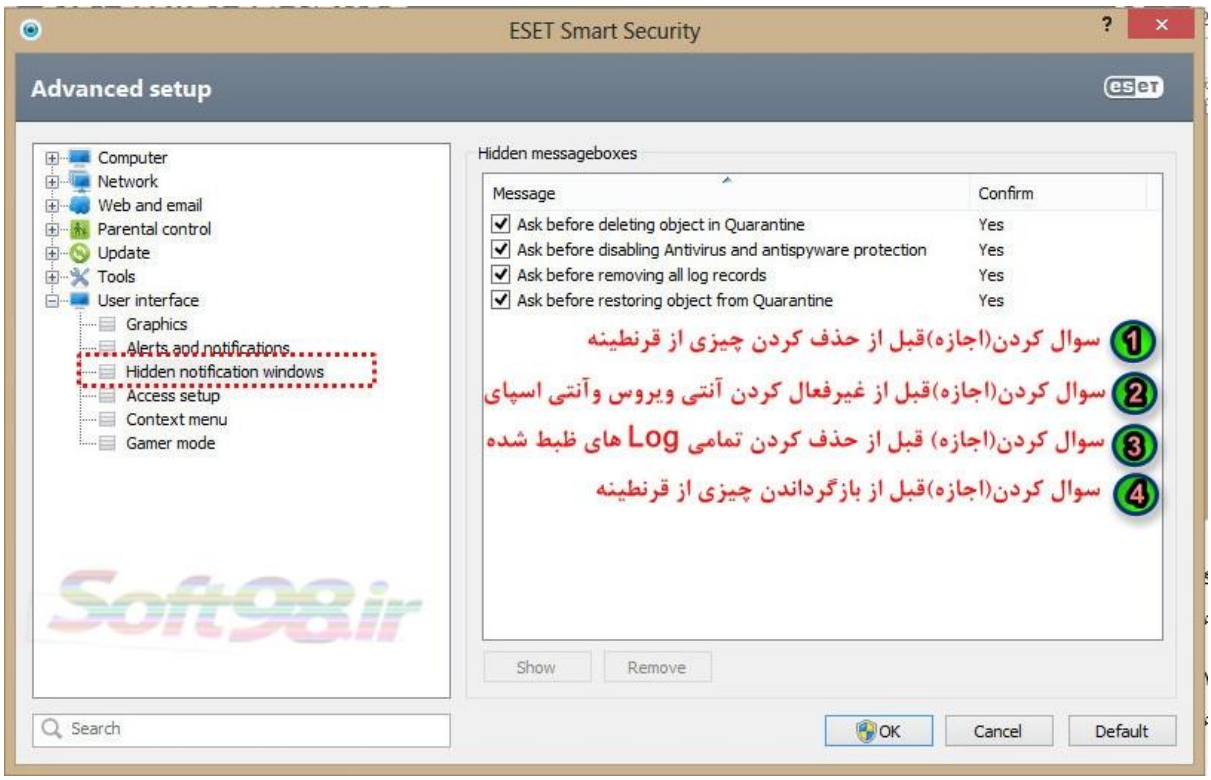
www.ParsBook.org

۳-عدم نمایش پنجره اطلاع رسانی زمانی که برنامه ها در حالت تمام صفحه(Full-screen) هستند

۴- برای بسته شدن خودکار پیامهای هشدار نرم افزار پس از گذشتن یک مدت زمان از قبل تعریف شده می توانید از گزینه "close message boxes automatically after (sec.)"استفاده کنید. پس از درج مدت زمان مورد نظر بر حسب ثانیه، اگر پنجره پیام یا هشدار نرم افزارقبل از سپری شدن این زمان به صورت دستی بسته نشود، با سپری شدن زمان درج شده به صورت خودکار بسته خواهد شد.

۵-تنظیمات پیشرفته (توضیح در اسکرین شات)

Hidden notification windows



www.ParsBook.org

Access setup

برای حفاظت از پارامترهای تنظیمات نرم افزار،می توان یک کلمه عبور تعریف نمود. این کار برای جلوگیری دسترسی افراد غیرمجاز انجام می شود.

Context menu

منوی زمینه، پس از راست کلیک کردن بر روی یک فایل یا فولدر نشان داده میشود.منو زمینه شامل فهرستی از تمام گزینه های قابل انجام بر روی فایل مورد نظر است.

پس از انتخاب ،یک گزینه به منوی راست کلیک اضافه میشود(توضیح در اسکرین شات)

www.ParsBook.org

Gamer mode

Gamer Mode حالتی است که با فعال کردن آن آنتی ویروس دست از اسکن های اتوماتیک و پیامهای هشدار برمیدارد و کمتر از منابع سیستم (Ramوcpu) استفاده میکنه تا در بازی دچار مشکل نشین پیشنهاد میشود اگر از سیستم قوی استفاده می کنین این گزینه را فعال نکنید.

البته در این حالت حفاظت از سیستم در پس زمینه اجرا می شودو هیچ تعاملی با کاربر را ندارد.

امیدوارم که مطالب عنوان شده برای تمامی عزیزان مفید واقع شده باشه.

در صورت وجود مشکل ،آن را در انجمن مطرح نمائید.

برقرار و سبز باشید.

اسفند ۹۱

تهیه شده در انجمن سافت ۹۸

Hadie6z

www.ParsBook.org