✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

راهنمای جامع نرم افزار

# ESET Smart Security

(بسته نرم افزاری حفاظت اینترنتی هوشمند "ESET")

شامل اجزای یکپارچه ضد ویروس، ضد جاسوس افزار،

دیواره آتش شخصی و ضد هرزنامه "ESET"

نسل جدید فناوری "Nod32"

سازگار با سیستم‌های عامل ویندوز "Vista"، "XP"، "2000" و "2003"

"ESET Smart Security" توسط شرکت "ESET" ابداع و گسترش یافته است. جهت کسب اطلاعات بیشتر در خصوص این نرم افزار می‌توانید با شرکت ضدویروس امین به عنوان نمایندگی رسمی و انحصاری شرکت "ESET" در ایران به شماره ۲۲۰۱۹۵۱۸ تماس حاصل نموده و یا به وب سایت "www.nod32.ir" مراجعه کنید.



در این راهنما به جای عبارت "ESET Smart Security" از واژه "ESS" استفاده گردیده است.



REV.20071129-003

## فهرست مندرجات

## ۱ – حفاظت اینترنتی هوشمند "ESET" (ESET Smart Security)

"ESS" اولین نمونه نرم افزاری در مسیر امنیت یکپارچه و کامل رایانه‌ها است. این نرم افزار از سرعت و دقت ضدویروس "Nod32" که در حال حاضر از آخرین نگارش موتور پویش "ThreatSense" بهره مند است و همچنین از ماژولهای ضد هرزنامه و دیواره آتش شخصی مناسبی استفاده می نماید. نتیجه این ترکیب سیستم حفاظتی هوشمندی است که دائما رایانه کاربر را از انواع حملات و کدهای مخرب حفاظت می کند.

"ESS" ترکیبی ناهماهنگ از محصولات مختلف در یک پکیج نرم افزاری نیست. بلکه نتیجه یک تلاش طولانی در ارائه راهکاری برای دستیابی به حداکثر حفاظت رایانه‌ای و حداقل تاثیر منفی بر روی سیستم کاربر می‌باشد. فناوری‌های پیشرفته مورد استفاده در نرم‌افزار که بر پایه هوش مصنوعی بنا شده‌اند، قادرند با استفاده از روشهای پیشگیرانه تهدیدات نفوذی اعم از ویروسها، جاسوس افزارها، اسبهای تروا، کرم‌ها، "Adware" ها، "rootkit" ها و دیگر تهدیدات اینترنتی را بدون تاثیر منفی بر روی کارایی سیستم دفع نمایند.

### ۱-۱- ویژگی‌های جدید

تجربه طولانی مدت متخصصین شرکت "ESET" در معماری جدید نرم افزار "ESS" به صورت کامل نمایان گردیده است. "ESS" حداکثر حفاظت رایانه‌ای را در کنار حداقل استفاده از منابع سیستمی و همچنین حداقل مزاحمت در انجام امور جاری کاربر فراهم آورده است. این نرم افزار مدرن امنیتی شامل ماژولهای مختلفی است که هر یک از آنها تنظیمات پیشرفته خاص خود را دارند. در ادامه به مرور مختصر ویژگی‌های هر یک از این ماژول‌ها می‌پردازیم:

- ماژول ضدویروس و ضد جاسوس افزار

این ماژول بر اساس هسته پویش "ThreatSense" بنا نهاده شده است که برای اولین بار در نرم افزار ضدویروس "Nod32" بکارگرفته شد. به بیان دیگر در معماری جدید "ESS" از هسته "ThreatSense" به صورت بهینه‌تری استفاده به عمل آمده است.

| ویژگی | توضیحات |
|---|---|
| پاکسازی فایلها به صورت بهینه | سیستم ضدویروس به صورت کاملا هوشیارانه فایلهای آلوده را پاکسازی کرده و اکثر تهدیدات شناسایی شده را بدون نیاز به دخالت کاربر پاک می‌کند. |
| حالت پویش در پس زمینه کار رایانه | پویش رایانه می‌تواند در پس زمینه امور جاری رایانه و بدون کاهش کارایی آن انجام شود. |
| فایلهای بروزرسانی کوچک | پردازش‌های مربوط به بهینه‌سازی هسته موجبات کوچک شدن اندازه فایلهای بروزرسانی نرم افزار را – حتی کوچکتر از فایلهای بروزرسانی نگارش ۲/۷ – فراهم آورده است. همچنین حفاظت از فایلهای بروزرسانی در مقابل تخریب بهبود یافته است. |
| حفاظت از نرم‌افزارهای معروف مدیریت پست الکترونیک | اکنون دیگر امکان پویش نامه‌های الکترونیکی وارده نه تنها در نرم افزار "MS Outlook" بلکه در نرم افزارهای "Outlook Express" و "Windows Mail" نیز فراهم شده است. |

| | |
|---|---|
| چند مورد بهینه شده دیگر | - دسترسی مستقیم به "file system" جهت افزایش سرعت و ظرفیت<br>- بلوکه کردن دسترسی به فایلهای آلوده<br>- افـزایش هماهنگی نـرم افـزار بـا برنامـه "windows security center" در ویـنـدوز "XP" و "Vista" |

- دیواره آتش شخصی

دیواره آتش شخصی تمامی ترافیک بین رایانه حفاظت شده و دیگر رایانه‌های موجود در شبکه را کنترل می‌کند. دیـواره آتـش شـرکت "ESET" شامل ویژگی‌های کاربردی و پیشرفته‌ای ذیل است:

| ویژگی | توضیحات |
|---|---|
| پویش ارتباطات شبکه‌ای سطح پایین | پویش ارتباطات شبکه‌ای در لایه "data link" باعث می‌شود تا دیواره آتش "ESET" بر حجم زیادی از حملات غیر قابل شناسایی فائق آید. |
| پشتیبانی از "IPV6" | دیواره آتش "ESET" آدرسهای "IPV6" را نمایش داده و کاربر را قادر می‌سازد تا بتواند برای آن آدرس‌ها قانون (Rule) تعریف کند. |
| کنترل فایلهای اجرایی | کنترل تغییرات در فایلهای اجرایی به جهت غلبه بر آلودگی ویروسی انجام می‌پذیرد. همچنین امکان اصلاح فایلهای برنامه‌های کاربردی "sign" شده (امضا شده) نیز وجود دارد. |
| پویش فایلها به صورت یکپارچه با پروتکل‌های "HTTP" و "POP3" | پویش فایل‌ها در پروتکل‌های کاربردی "POP3" و "HTTP" به صورت یکپارچه انجام می‌شود. لذا کاربران در زمان مرور وب و یا دانلود نامه‌های الکترونیکی با هیچ خطری روبرو نخواهند بود. |
| سیستم شناسایی نفوذ به رایانه | دیواره آتش شخصی "ESET" توانایی شناسایی ویژگی‌های ارتباطات شبکه‌ای و همچنین انواع مختلف حملات شبکه‌ای را داشته و می‌تواند به صورت خودکار چنین حملاتی را دفع نماید. |
| پشتیبانی به روشهای تعاملی، خودکار و یا حالت پشتیبانی بر اساس "policy" تعریف شده | کاربران می‌توانند چگونگی عکس العمل دیواره آتش شخصی در مواجه با تهدیدات را اعم از انجام دفاع خودکار و یا تعریف قوانین جهت مقابله با تهدیدات مشخص کنند. ضمن اینکه در حالت "policy – based"، حفاظت از رایانه بر اساس قوانین از پیش تعیین شده کاربر و یا مدیر سیستم انجام می‌پذیرد. |
| جایگزینی مناسب برای نرم افزار "windows firewall" | دیواره آتش شخصی "ESET" علاوه بر اینکه جایگزین مناسبی برای برنامه "windows firewall" است، با برنامه "windows security center" نیز دارای تعامل مناسبی می‌باشد. در نتیجه کاربر می‌تواند از طریق "windows security center" نسبت به وضعیت امنیتی رایانه خود آگاهی حاصل کند. نکته آخر اینکه "ESS" به صورت پیش فرض دیواره آتش استاندارد ویندوز را غیر فعال می‌کند. |

- ضد هرزنامه

ماژول ضد هرزنامه "ESET" علاوه بر فیلترنمودن نامه‌های الکترونیک ناخواسته باعث افزایش امنیت و راحتی در نقل و انتقال اطلاعات الکترونیک می‌گردد.

| ویژگی‌ها | توضیحات |
|---|---|
| ویژگی امتیاز دهی به نامه‌های الکترونیکی وارده | به تمامی نامه‌های الکترونیک وارده عددی در بازه صفر تا ۱۰۰ اختصاص پیدا می‌کند. عدد صفر به معنی این است که نامه دریافتی هرزنامه نمی‌باشد و عدد ۱۰۰ به معنی آن است که نامه دریافتی هرزنامه است. سپس این نامه‌های وارده به پوشه "junk mail" و یا هر پوشه دیگر که توسط کاربر مشخص شده است انتقال می‌یابند. ضمن اینکه پویش نامه‌های دریافتی به صورت موازی نیز انجام پذیر است. |
| پشتیبانی از فناوری‌های مختلف پویش | - استفاده از فناوری تحلیل "Bayes"<br>- پویش بر اساس قوانین تعریف شده<br>- بررسی جامع بانک اطلاعاتی مربوط به هرزنامه |
| یکپارچگی و هماهنگی کامل با نرم‌افزارهای مدیریت نامه‌های الکترونیک | کاربران نرم‌افزارهای "Microsoft outlook"، "Outlook express" و "Windows Mail" می‌توانند از مزایای ضد هرزنامه "ESET" بهره مند گردند. |
| امکان گزینش و انتخاب هرزنامه‌ها به صورت دستی | با استفاده از این ماژول می‌توان به صورت دستی شرایط هرزنامه بودن یا عدم هرزنامه بودن یک نامه الکترونیکی را مشخص کرد. |

### ۲-۱- نرم افزار و سخت افزار مورد نیاز

جهت کارکرد بهینه و بی عیب و نقص "ESS" لازم است حداقل سخت افزار و نرم افزار ذیل فراهم گردد:

| سیستم عامل | سخت افزار |
|---|---|
| ویندوز "2000"، "XP"، "2000" سرور و "2003" سرور | - پردازنده ۴۰۰ مگاهرتزی ۳۲ یا ۶۴ بیتی<br>- حافظه موقت به میزان ۱۲۸ مگابایت<br>- فضای خالی بر روی دیسک سخت به میزان ۳۵ مگابایت<br>- کارت گرافیک "super VGA" با رزولوشن ۶۰۰ در ۸۰۰ پیکسل |

| | |
|---|---|
| ویندوز ویستا | - پردازنده یک گیگا هرتزی ۳۲ یا ۶۴ بیتی<br>- حافظه موقت به میزان ۵۱۲ مگابایت<br>- فضای خالی بر روی دیسک سخت به میزان ۳۵ مگابایت<br>- کارت گرافیک "super VGA" با رزولوشن ۶۰۰ در ۸۰۰ پیکسل |

## ۲- نصب نرم افزار

پس از خرید نرم افزار می‌توانید فایل نصب کننده آن را از وب سایت شرکت "ESET"دانلود نمائید. این فایل نصب کننده تحت عنوان دو نام قابل دانلود است.

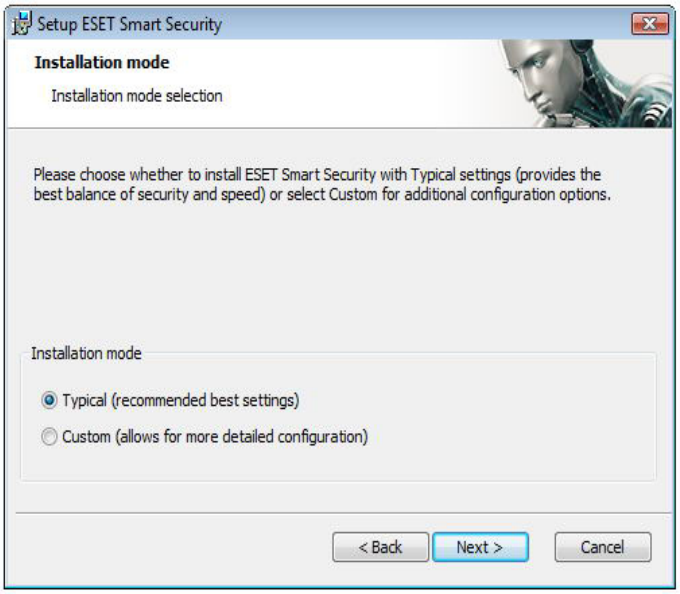
ESS - nt**-***.ms (نگارش معمولی "ESET" )

ESSbe-nt**-***.ms (نگارش تجاری "ESS" )

با اجرای فایل نصب کننده فرایند نصب نرم افزار آغاز می‌گردد. دو روش نصب نرم افزار با سطوح جزئیات نصب متفاوت وجود دارد.

الف) نصب عادی یا "Typical"

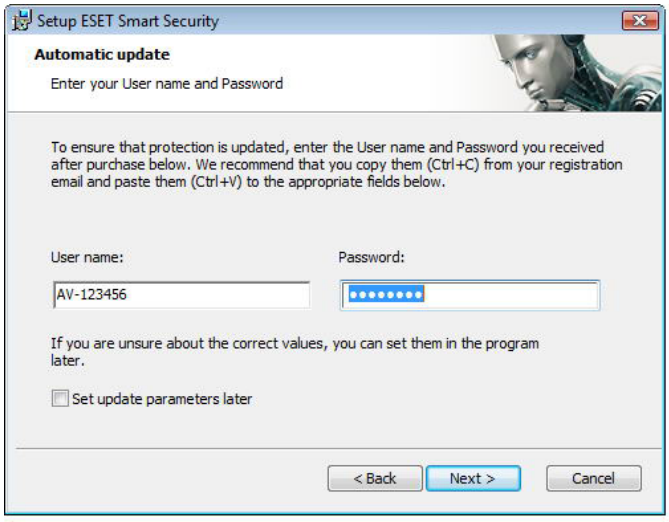
ب) نصب سفارشی یا "Custom"




### ۲-۱- نصب عادی نرم افزار

این روش نصب برای کاربرانی مناسب است که قصد دارند از "ESS" با تنظیمات پیش فرض آن استفاده نمایند. این تنظیمات پیش فرض باعث ایجاد حداکثر سطح امنیتی شده و برای کاربرانی که قصد پیکربندی جزئیات مربوط به تنظیمات نرم افزار را ندارند بهترین راه حل است.

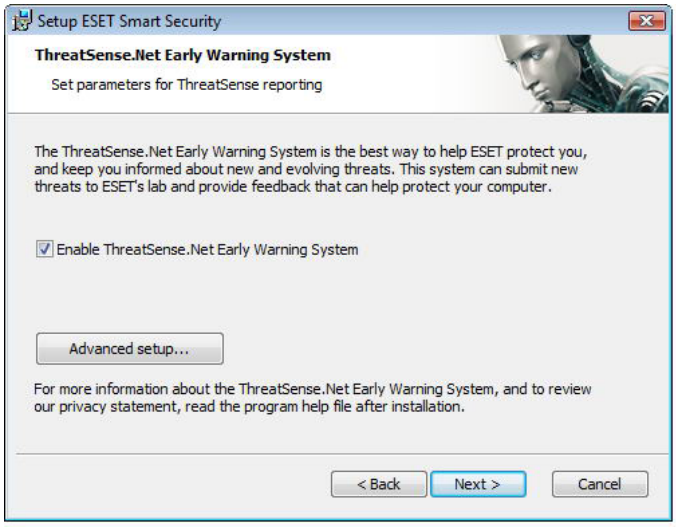
اولین و در واقع یکی از مهمترین مراحل در نصب نرم افزار درج شناسه کاربری و کلمه عبور جهت دریافت فایلهای بروزرسانی نرم افـزار به صورت خودکار است. زیرا بروزرسانی نرم افزار نقـش بـسیار مهمی را در ایجاد حفاظت دائم سیستم خواهد داشت.




همانطور که در شکل بالا نمایان مـی‌باشـد لازم اسـت شناسـه کاربری و کلمه عبور خود را کـه بـه هنگـام خریـد و یـا ثبـت محصول دریافت نموده‌اید در فیلدهای مربوطه وارد نمائیـد. در صورتی که در حال حاضر این اطلاعات را در دسـترس ندارید نیز می‌توانید با انتخاب گزینه

"set update parameters later"

به مرحله بعدی نصب نرم افزار رفته و در زمان مناسب نسبت به درج اطلاعات مورد نظر اقدام کنید.

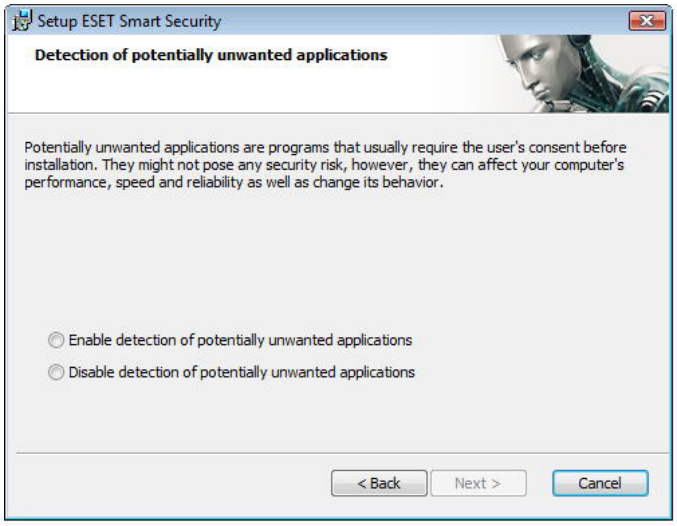



گـــام بعـــدی پیکربنـــدی سیـــستم هـــشدار اولیـــه "ThreatSense.net" اسـت. شـرکت "ESET" از ایـن سیستم جهت کسب آگاهی سریع و مستمر بـه منظـور بـروز تهدیدات جدید استفاده می‌کند تـا بتوانـد در کمتـرین زمـان ممکن تمهیدات لازم جهت مقابلـه بـا تهدیـد جدیـد را بـرای کاربران خود به ارمغان آورد. از این سیـستم همچنـین جهـت ارسال تهدیدات جدید به لابراتوار شرکت "ESET" اسـتفاده به عمل می‌آید. در این لابراتوار است که تهدیدات جدید مورد تحلیل و پـردازش قـرار گرفتـه و سـپس بـه بانـک اطلاعـاتی شناسه ویروسهای رایانه‌ای نرم افزارهای شرکت "ESET" افزوده می‌گردند.

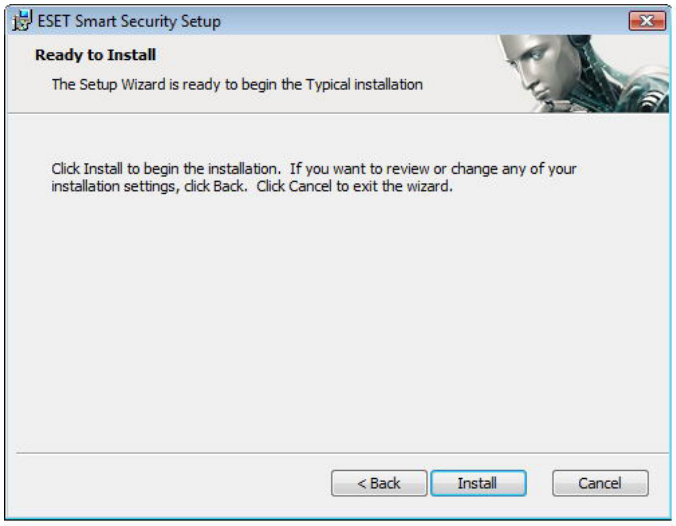
همانطور که در شکل بالا پیدا است، گزینه "enable ThreatSense.net early warning system" به صورت پیش فرض فعـال است. جهت دسترسی به تنظیمات پیشرفته این سیستم به منظور ارسال فایلهای مشکوک بـه آلـودگی بـه سـایت شـرکت "ESET" می‌توانید بر روی گزینه "Advanced Setup ..." کلیک کنید.

در مرحله بعدی فرایند نصب به پیکربندی گزینه شناسایی برنامه‌هایی که به صورت بالقوه ناخواسته هستند پرداخته می‌شود. برنامه‌های ناخواسته لزوما جزء کدهای مخرب به حساب نمی‌آیند، لـیکن مـی‌تواننـد اثـرات نـامطلوبی در کـارایی سیـستم عامـل داشـته باشـند. نرم افزارهای ناخواسته اغلب به همراه برنامه‌های رایانه‌ای دیگر به صورت رایگان (bundle) عرضه می‌شوند و معمولا شناسایی آنهـا در زمان نصب این برنامه‌های رایانه‌ای خیلی ساده نیست. با اینکه این برنامه‌ها در زمان نصب پیام‌هایی را نمایش می‌دهند، نصب آنها بدون موافقت و رضایت کاربر نیز به سادگی امکان پذیر است.

توصیه می‌شود گزینه "enable detection of potentially unwanted applications" را انتخاب کنید تا "ESS" بتواند این نوع تهدیدات رایانه‌ای را نیز شناسایی نمایید.




آخرین قدم در فرایند نصب عادی نرم افزار عبارت از تائید نصب نرم افزار با کلیک بر روی گزینه "install" است.



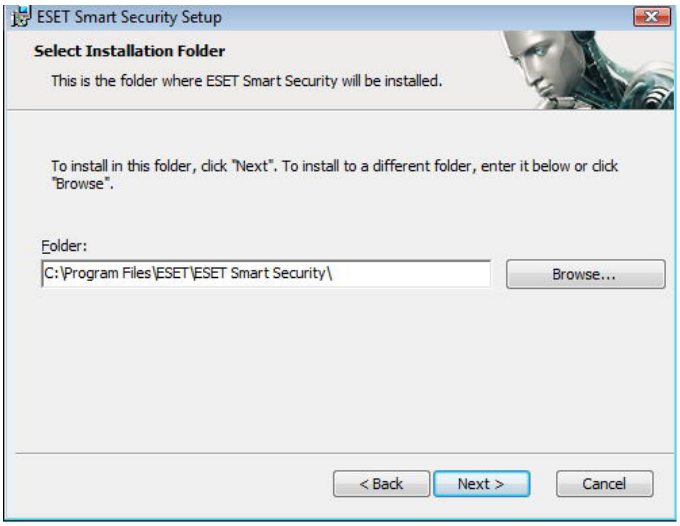

### ۲-۲- نصب نرم افزار به صورت سفارشی

این روش نصب نیز برای کاربرانی طراحی گردیده است که با چگونگی تنظیم نرم افزارهای رایانه‌ای آشنایی کامل داشته و تمایل دارند تنظیمات پیشرفته مورد نظر خود را در طی فرایند نصب اعمال دارند.

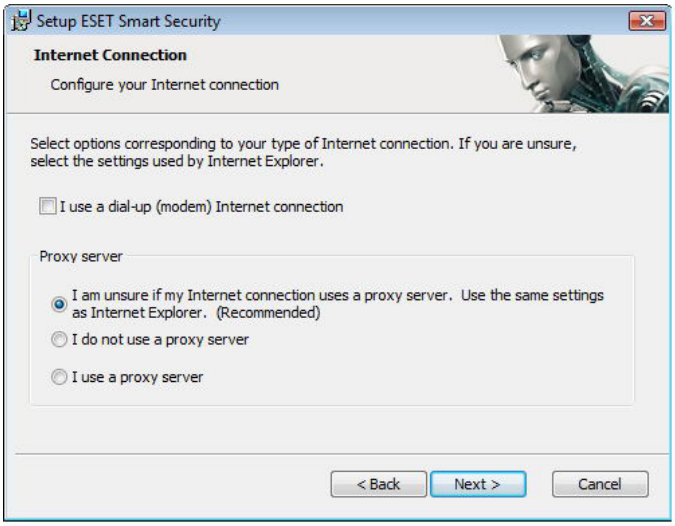
در این روش نصب اولین قدم عبارت از انتخاب مسیر نصب نرم افزار است. به صورت پیش فرض نرم افزار در مسیر

"C:\program files\ ESET\ ESET Smart Security\"

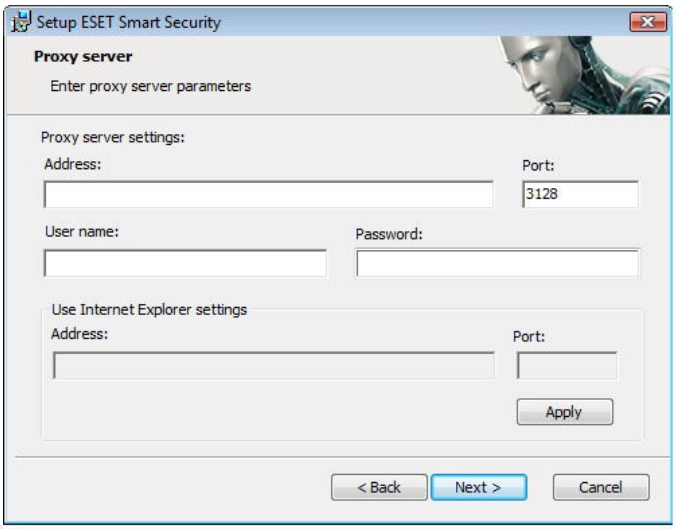
نصب می‌شود. جهت تغییر مسیر نصب می‌توانید بر روی دکمه "... Browse" کلیک کنید. لیکن این امر توصیه نمی‌شود.




در گام بعدی شناسه کاربری و کلمه عبور خود را درج خواهید کرد. این مرحله مانند مرحله مشابه در فرایند نصب عادی است. پس از اینکه شناسه کاربری و کلمه عبور خود را درج کردید، بر روی گزینه "next"کلیک کنید تا بتوانید تنظیمات مربوط به بستر ارتباطی اینترنت را مشخص نمائید.

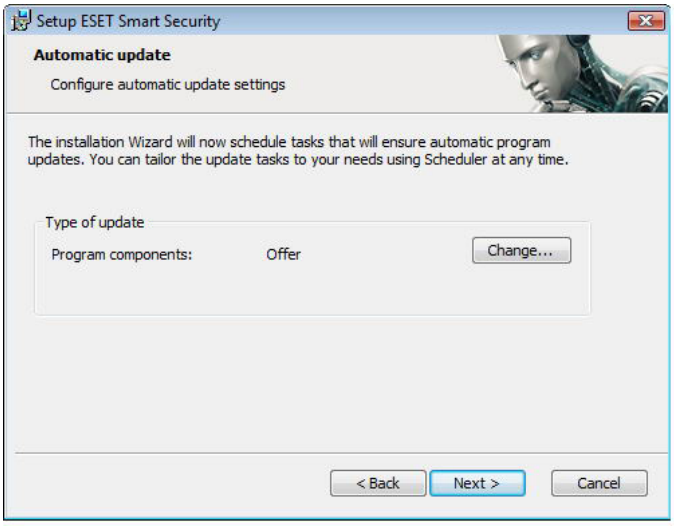



اگر از سرور "proxy" استفاده می‌کنید، لازم است تنظیمات مربوط به سرور "proxy" را به طور صحیح درج نمائید تا فرایند بروزرسانی بانک اطلاعاتی شناسه ویروسها با مشکلی روبرو نشود. همچنین اگر از این نکته که آیا از سرور "proxy" استفاده می‌کنید یا خیر اطلاعی ندارید، گزینه انتخاب شده پیش فرض را بدون تغییر پذیرفته و بر روی "next" کلیک کنید. همچنین اگر از سرور "proxy" استفاده نمی‌کنید نیز می‌توانید گزینه مناسب را انتخاب کرده و بر روی "next" کلیک نمائید.




جهت پیکربندی تنظیمات سرور "proxy"پس از انتخاب گزینه "I use a proxy server"، بر روی "next" کلیک کنید. سپس در فیلد آدرس لازم است نام یا "IP" سرور "proxy" را درج کنید. در فیلد "port" نیز پورتی را که سرور "proxy" اتصالات آن را می‌پذیرد وارد کنید. این فیلد به صورت پیش فرض با شماره "3128" پر شده است. همچنین اگر دسترسی به سرور "proxy" نیازمند داشتن شناسه کاربری و کلمه عبور خاص خود است، لازم

است این اطلاعات را در فیلدهای "user name" و "password" درج نمائید تا بتوانید بدون هیچگونه مشکلی به سرور "proxy" دسترسی پیدا کنید. در صورت تمایل می‌توان از تنظیمات "proxy" انجام شده در نرم افزار "Internet Explorer" استفاده کرد. بدین منظور کافی است بر روی دکمه "apply" کلیک کرده و سپس گزینه مورد نظر را انتخاب و تائید نمود.




اکنون می‌توانید با کلیک بر روی "next" به پنجره پیکربندی تنظیمات بروزرسانی خودکار نرم افزار دست یابید. در این پنجره است که قادر خواهید بود چگونگی بروزرسانی اجزای برنامه به صورت خودکار را مشخص نمائید. جهت دسترسی به تنظیمات پیشرفته در این زمینه بر روی گزینه "change ..." کلیک کنید.

اگر تمایل ندارید اجزای برنامه مورد بروزرسانی قرار گیرند ، گزینه

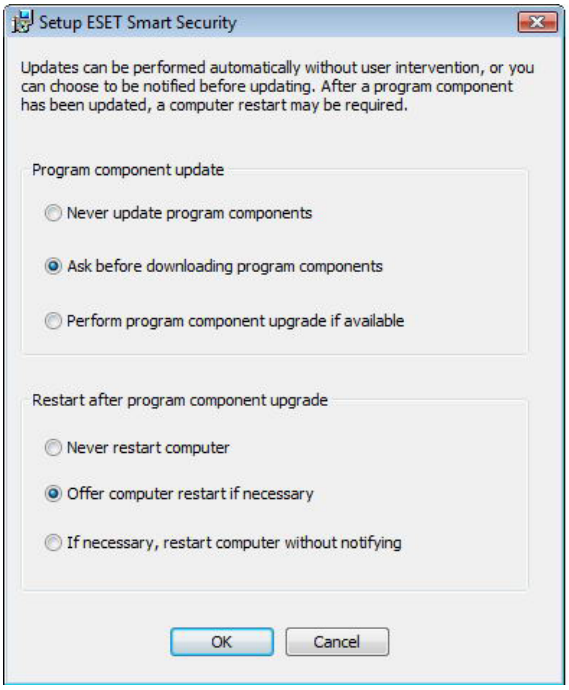
"never update program components"

را برگزینید. انتخاب گزینه "ask before downloading program components" نیز باعث می‌شود تا قبل از دانلود فایلهای بروزرسانی اجزای نرم افزار، پنجره‌ای گشوده شده و تائیدیه کاربر را جهت دانلود این فایلها اخذ کند.

جهت ارتقاء اجزای برنامه به صورت خودکار و بدون اخذ مجوز کاربر نیز می‌توان گزینه

"perform program component upgrade if available"

را فعال کرد.



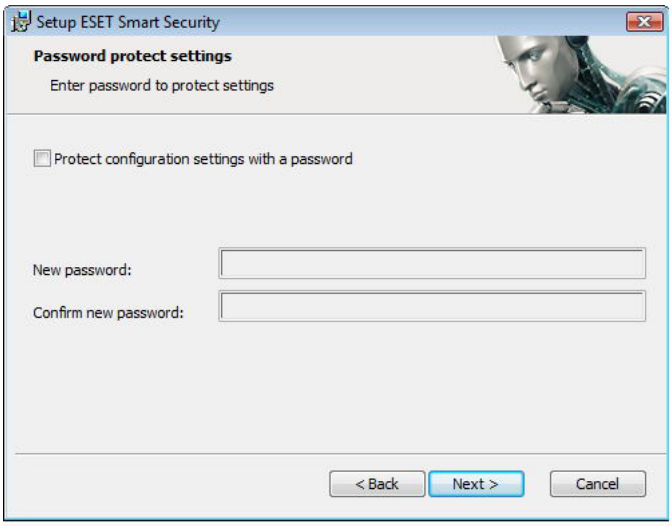

توجه:

معمولا پس از ارتقاء و بروزرسانی اجزای برنامه لازم است رایانه راه‌اندازی مجدد (Reboot) شود. لذا گزینه توصیه شده در این زمینه عبارت از

"If Necessary , Restart Computer Without Notifying"

خواهد بود.

در گام بعدی فرایند نصب می‌توان برای حفاظت از پارامترهای برنامه با استفاده از کلمه عبور مبادرت به درج یک کلمه عبور نمود تا افراد غیرمجاز نتوانند تنظیمات مورد نظر کاربر را تغییر دهند.




توجه داشته باشید که در روش نصب سفارشی تنظیمات مربوط به پیکربندی سیستم هشدار اولیه "ThreatSense.Net" و شناسایی نرم افزارهایی که به صورت بالقوه ناخواسته هستند مانند روش نصب عادی انجام می‌پذیرند که قبلا مورد بررسی قرارگرفته اند.

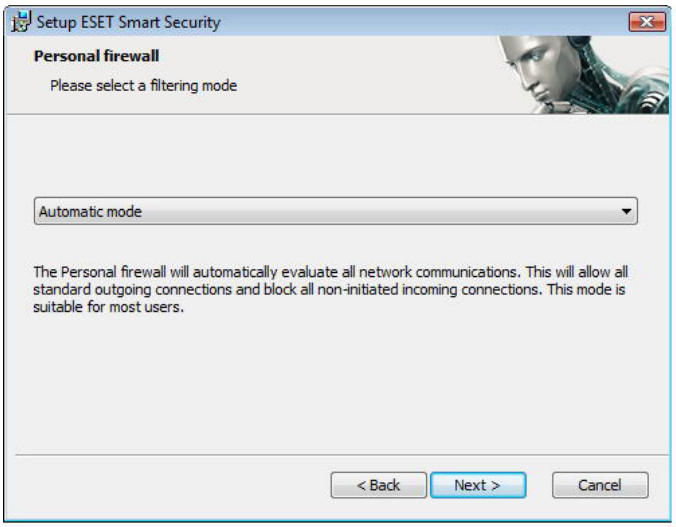
در آخرین گام نصب نرم افزار به صورت سفارشی قادر خواهید بود تا مد یا حالت فیلتر نمودن دیواره آتش شخصی "ESET" را مشخص کنید.

در اینجا سه حالت وجود دارد:

الف) حالت خودکار

ب) حالت تعاملی

ج ) حالت مبتنی بر سیاست تعیین شده از قبل



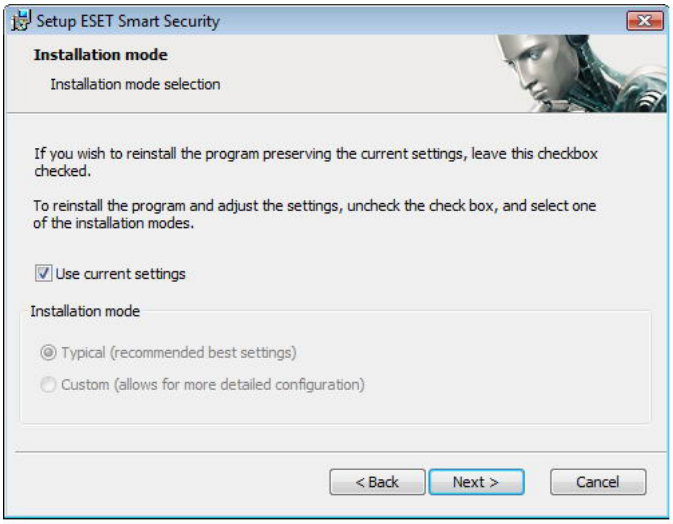

مد توصیه شده جهت اکثر کاربران، حالت خودکار است. در این حالت تمامی ارتباطات خروجی استاندارد ( که به صورت خودکار و با استفاده از تنظیمات از پیش تعیین شده مورد تحلیل قرار میگیرند) فعال شده و اتصالات ورودی نامطلوب نیز به طور خودکار بلوکه می‌گردند.

حالت تعاملی جهت کاربران حرفه‌ای مناسب می‌باشد. در این حالت ارتباطات بر اساس قوانین تعریف شده توسط کاربر مورد تحلیل قرار می‌گیرند. لذا اگر قانونی برای یک اتصال وجود نداشته باشد، نرم افزار در مورد عبور دادن ترافیک و یا بلوکه نمودن آن طی پنجره‌ای از کاربر سوال خواهد نمود.

در حالت مبتنی بر سیاست تعیین شده از قبل نیز نرم افزار بر اساس قوانین از پیش تعریف شده مدیر سیستم ارتباطات را ارزیابی می‌نماید. لذا اگر هیچ قانونی وجود نداشته باشد، ارتباط به صورت خودکار بلوکه شده و کاربر هیچ پیغام هشداری را نیز مشاهده نخواهد کرد. لذا توصیه شرکت "ESET" این است که صرفا مدیران شبکه جهت پیکربندی ارتباطات شبکه از مد یا حالت "policy–based" استفاده نمایند.

در آخرین قدم نصب نیز پنجره‌ای جهت اخذ نظر کاربر مبنی بر نصب نرم افزار گشوده شده و کاربر می‌بایست بر روی دکمه "install" کلیک کند.

### ۳-۲- استفاده از تنظیمات اصلی



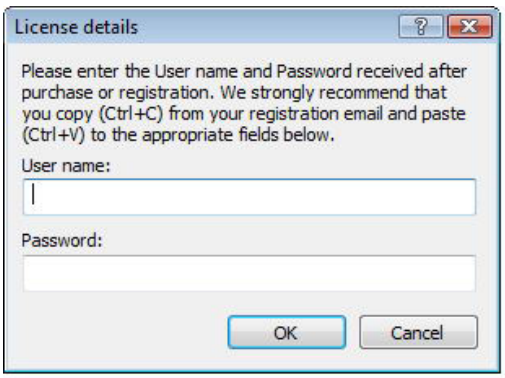

اگر نرم افزار "ESS" را نصب مجدد نمائید، گزینه "use current settings" نمایش داده خواهد شد. به منظور استفاده از تنظیمات انجام شده در نصب قبلی نرم افزار جهت نصب جدید کافی است این گزینه را تیک بزنید.

### ۴-۲- درج شناسه کاربری و کلمه عبور

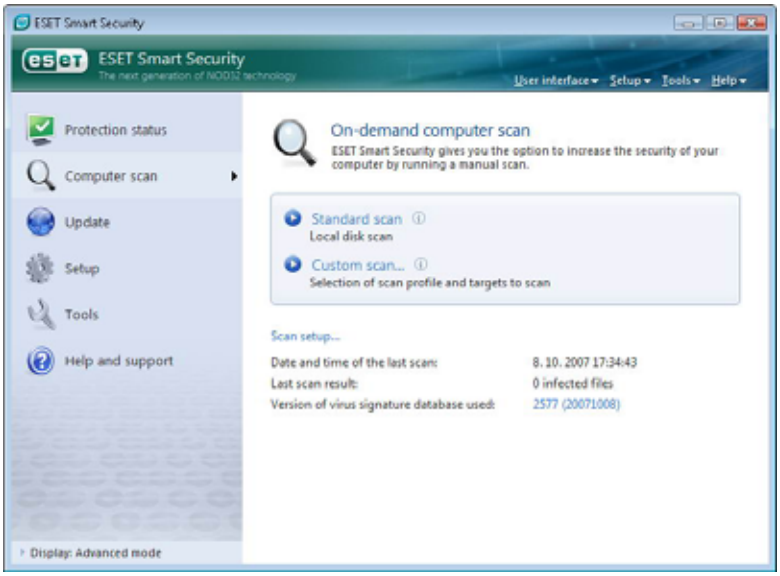
جهت کارایی بهینه نرم افزار لازم است نرم افزار به صورت خودکار مورد بروزرسانی قرار گیرد. این امکان صرفا زمانی فراهم است که شناسه کاربری و کلمه عبور در تنظیمات مربوط به بروزرسانی نرم افزار درج گردیده باشند. لذا اگر در طی فرایند نصب مبادرت به درج این اطلاعات نکرده‌اید می‌توانید پس از اتمام نصب نرم افزار بر روی گزینه "update" موجود در پنجره اصلی نرم افزار کلیک کرده و سپس بر روی گزینه

"user name and password setup…"

کلیک نموده و نهایتا این اطلاعات را در پنجره "License Details" وارد کنید.



### ۵-۲- پویش دستی رایانه




پس از نصب "ESS" لازم است رایانه را به لحاظ وجود کدهای مخرب مورد پویش قرار دهید. به منظور اجرای سریع پویش لازم است گزینه "computer scan" را در پنجره اصلی نرم افزار انتخاب کرده و پس از آن گزینه "standard scan" را برگزینید. برای کسب اطلاعات بیشتر در این خصوص می‌توانید به بخش "پویش رایانه" موجود در همین راهنما مراجعه کنید.

## ۳- راهنمای کاربران مبتدی

در این بخش به مرور اجمالی "ESS" و تنظیمات پایه‌ای آن پرداخته می‌شود.

### ۱-۳- آشنایی با طراحی و حالتهای مختلف رابط گرافیکی کاربر

پنجره اصلی "ESS"به دو بخش تقسیم شده است. از قسمت سمت چپ این پنجره جهت دسترسی به منوی اصلی و در عین حال ساده و قابل فهم استفاده می‌شود.

در قسمت سمت راست نیز اطلاعات گوناگونی که مرتبط با آیتم انتخاب شده در سمت چپ هستند به نمایش در می‌آیند. در ادامه به بررسی آیتم‌های مختلف منوی اصلی می‌پردازیم:

- گزینه وضعیت حفاظت (protection status)

با استفاده از این گزینه به اطلاعات مختلفی در زمینه وضعیت امنیتی رایانه دست پیدا می‌کنید. اگر مد پیشرفته انتخاب شده باشد، وضعیت تمامی ماژولهای حفاظتی قابل ملاحظه خواهد بود و کاربر می‌تواند با کلیک بر روی هر ماژول، اطلاعات جاری مربوط به آن را مشاهده کند.

- گزینه پویش رایانه (computer scan)

کاربران می‌توانند از این گزینه جهت پیکربندی و پویش دستی رایانه استفاده کنند.

- گزینه "update"

این گزینه نیز جهت دسترسی به ماژول بروزرسان نرم افزار که وظیفه بروزرسانی بانک اطلاعاتی شناسه ویروسهای رایانه‌ای را بر عهده دارد بکار می‌رود.

- گزینه "setup"

کاربران می‌توانند با استفاده از این گزینه سطح امنیتی رایانه خود را تعیین کنند. اگر مد پیشرفته فعال شده باشد، زیر منوهای ضدویروس ، ضد جاسوس افزار، دیواره آتش شخصی و ماژول ضد هرزنامه نمایان خواهند شد.

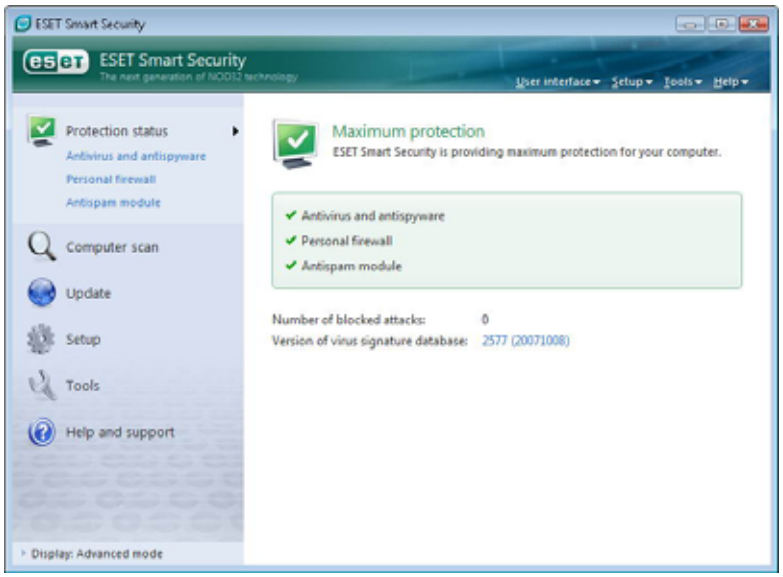
- گزینه "tools"

این گزینه صرفا در زمانی که مد پیشرفته فعال است قابل مشاهده می‌باشد و از آن جهت دسترسی به فایلهای ثبت رخدادها، مخزن قرنطینه و همچنین برنامه زمان بندی خودکار استفاده می‌گردد.

- گزینه "help and support"

از این گزینه جهت دسترسی به فایل راهنمای نرم افزار، بانک اطلاعات و آگاهی "ESET" ، وب سایت شرکت "ESET" و همچنین دسترسی به خدمات فنی مشتریان استفاده می‌شود.

رابط گرافیکی کاربر "ESS" دارای دو حالت استاندارد و پیشرفته است و کاربر همواره می‌تواند بین این دو مد سوئیچ نماید. جهت این منظور کافی است بر روی لینک "Display" که در گوشه پائین سمت چپ پنجره اصلی "ESS" قرار دارد، کلیک کنید.



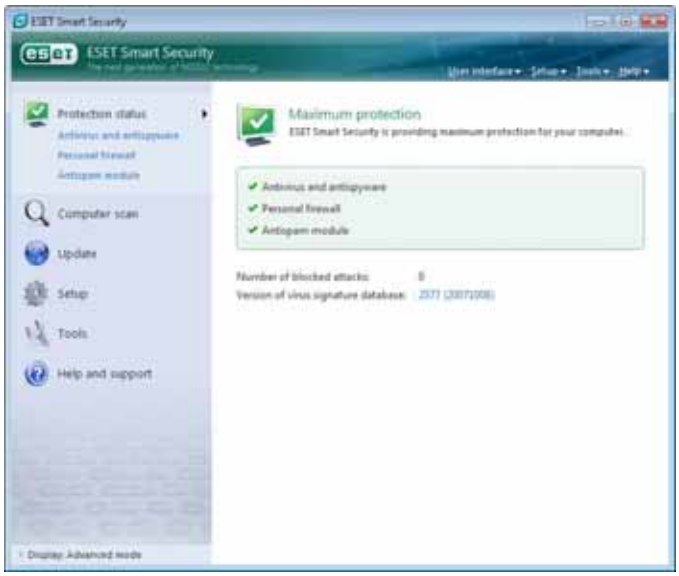

در مد استاندارد صرفا دسترسی به ویژگی‌هایی که برای عملکرد عادی نرم افزار لازم هستند، وجود دارد و به بیان دیگر گزینه های پیشرفته به نمایش در نیامده‌اند.


تغییر به مد پیشرفته امکان دسترسی به گزینه "tools"را در منوی اصلی فراهم می‌آورد. در قسمت "tools" است که کاربر می‌تواند به فایلهای ثبت رخدادها، مخزن قرنطینه و همچنین برنامه زمان بندی خودکار نرم افزار دست یابد.

*توجه: تمامی موارد دیگری که در این راهنما مورد بررسی قرار می‌گیرند مربوط به رابطه گرافیکی کاربر در مد پیشرفته می‌باشند.*

### ۱-۱-۳- بررسی وضعیت عملکرد سیستم

جهت مشاهده وضعیت حفاظتی رایانه کافی است بر روی گزینه "protection status" در قسمت سمت چپ پنجره اصلی نرم افزار کلیک کنید. با انجام این عمل در قسمت سمت راست پنجره خلاصه وضعیت عملکرد "ESS" را مشاهده خواهید نمود. ضمن اینکه یک زیر منوی دارای سه آیتم نیز ظاهر خواهد شد. این سه آیتم عبارت از "Antivirus and Anti Spyware"، "Personal Firewall" و ماژول "Anti Spam" هستند. با کلیک بر روی هر یک از آنها اطلاعات با جزئیات بیشتری در رابطه با ماژول انتخاب شده به نمایش در خواهد آمد.




اگر ماژولهای فعال به صورت صحیح در حال انجام وظایف خود باشند، یک علامت تیک سبز رنگ در کنار آنها به نمایش در آمده و اطلاعات اضافی مربوط به ماژول در قسمت بالایی پنجره قابل مشاهده خواهد بود.

ضمن اینکه راه حل (solution) پیشنهاد شده "ESET" در رابطه با ماژول مورد نظر نیز نمایان می‌گردد. نکته آخر اینکه به منظور انجام تنظیمات مربوط به هر یک از ماژولها، کافی است بر روی گزینه "setup" موجود در منوی اصلی کلیک کرده و پس از آن نیز بر روی ماژول مورد نظر کلیک نمائید.

### ۲-۱-۳- در زمان عملکرد غیر صحیح سیستم چه باید کرد؟


اگر "ESS" مشکلی را در مورد هر یک از ماژولهای حفاظتی خود شناسایی کند، آن مشکل را در قسمت "protection status" گزارش می دهد. ضمن اینکه چگونگی حل مشکل حادث شده نیز توسط نرم افزار به آگاهی کاربر می‌رسد.

در صورتی که نتوان مشکل حادث شده را با استفاده از فهرست مشکلات و راه حل‌های آنها حل نمود، می‌توان بر روی گزینه "help and support" کلیک نمود تا به فایلهای راهنما دست یافت و یا بتوان بانک اطلاعات "ESET" را مورد کاوش قرار داد.

اگر پس از انجام موارد فوق باز هم مشکل حادث شده مرتفع نگردید می‌توانید یک پیام در خواست خدمات پشتیبانی به واحد خدمات فنی "ESET" ارسال کنید تا متخصصین این شرکت در اسرع وقت نسبت به آگاهی رسانی و رفع مشکل ایجاد شده اقدام کنند.

### ۲-۳- تنظیمات مربوط به بروزرسانی نرم افزار

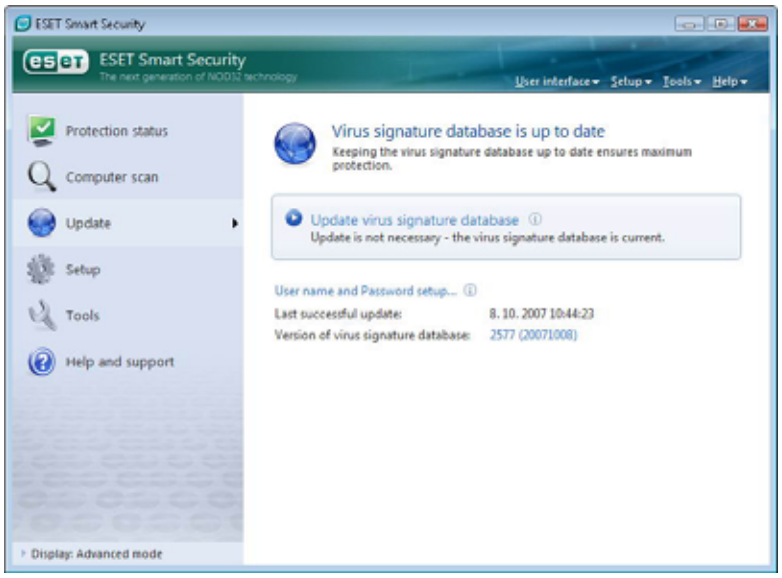
یکی از بخشهای اصلی در حفاظت رایانه در مقابل انواع کدهای مخرب عبارت از بروزرسانی بانک اطلاعات شناسه ویروسهای رایانه‌ای و همچنین بروزرسانی و ارتقاء اجزای نرم افزار است. لذا لازم است توجه ویژه‌ای به این امر و تنظیمات مربوط به بروزرسانی نرم افزار معطوف گردد.

بدین جهت کافی است از منوی اصلی گزینه "update" را برگزیده و سپس بر روی گزینه

"update virus signature database"

در قسمت سمت راست پنجره اصلی نرم افزار کلیک کنید تا نرم افزار در صورت وجود، این اطلاعات را دانلود نماید. ضمن اینکه با کلیک بر روی گزینه

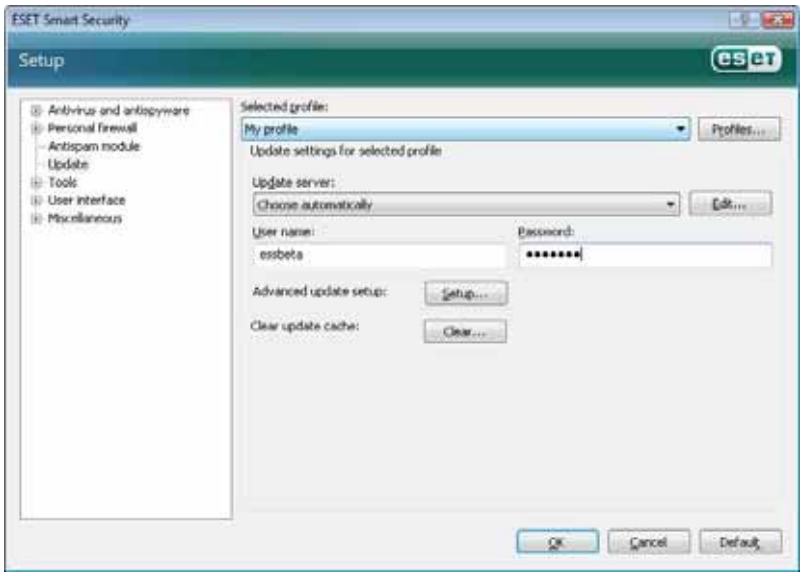
"user name and password setup…"




یک کادر محاوره‌ای گشوده شده و می‌توان شناسه کاربری و کلمه عبوری که در زمان خرید نرم افزار دریافت شده است را در فیلدهای این کادر درج کرد.

توجه داشته باشید که اگر این اطلاعات را در زمان نصب نرم افزار وارد کرده باشید، نیازی به درج مجدد آنها نخواهد بود.

پنجره تنظیمات پیشرفته (برای گشودن این پنجره می‌توان از کلید F5 صفحه کلید استفاده کرد) نیز شامل گزینه‌ها با جزئیات بیشتری در خصوص بروزرسانی نرم افزار است. در این پنجره لازم است گزینه "update server" بر روی گزینه "choose automatically" تنظیم شده باشد. ضمن اینکه جهت دیگر تنظیمات پیشرفته مربوط به بروزرسانی نرم افزار نظیر مد بروزرسانی ، دسترسی به سرور "proxy" ، دسترسی به فایلهای بروزرسانی موجود بر روی سرور محلی و ایجاد کپی‌هایی از بانک اطلاعاتی شناسه ویروسها (مورد استفاده در نگارش تجاری "ESS") می‌توان بر روی گزینه "setup …" کلیک نمود.

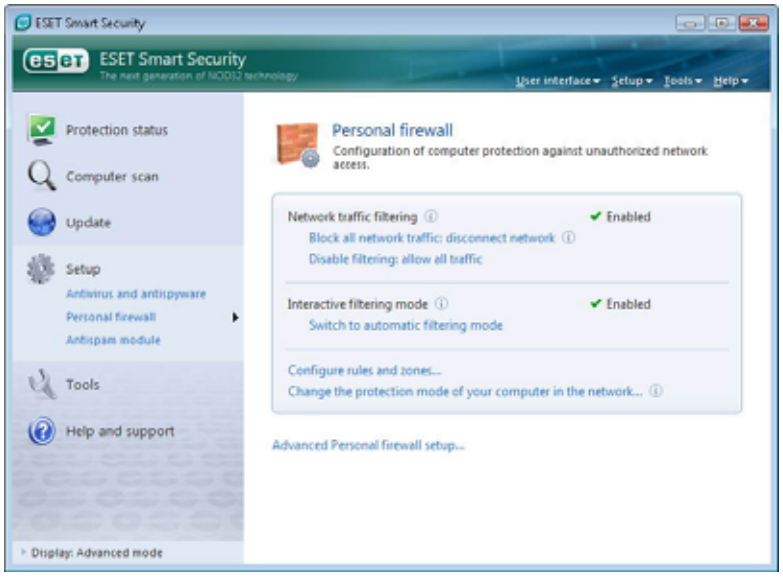



### ۳-۳- تنظیمات مربوط به ناحیه یا منطقه ایمن (trusted zone)

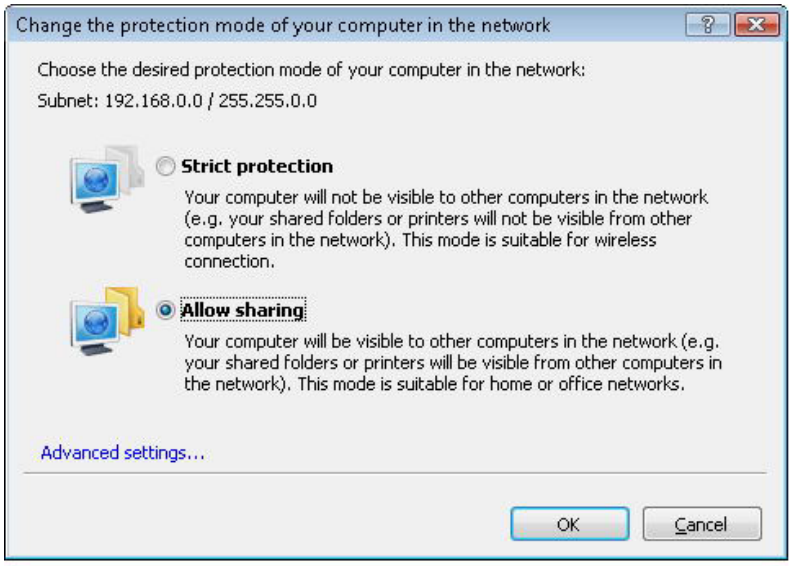
پیکربندی مربوط به ناحیه ایمن یکی دیگر از قدمها در ایجاد حفاظت جهت رایانه‌های موجود در شبکه‌های رایانه ای است. کاربر می‌تواند با پیکربندی ناحیه ایمن امکان دسترسی دیگر کاربران شبکه را به رایانه خود فراهم آورد (به اشتراک گذاشتن اطلاعات). بدین منظور کافی است بر روی آیتم "setup" در پنجره اصلی نرم افزار کلیک کرده و سپس گزینه "personal firewall" را برگزینید. در ادامه نیز می‌بایست گزینه

"change the protection mode of your computer in the network…"

را انتخاب نمائید. در این لحظه است که یک پنجره جدید گشوده شده و به کاربر امکان می‌دهد تا بتواند تنظیمات مربوط به مد حفاظتی رایانه در یک شبکه رایانه‌ای و یا یک ناحیه ایمن را انجام دهد.



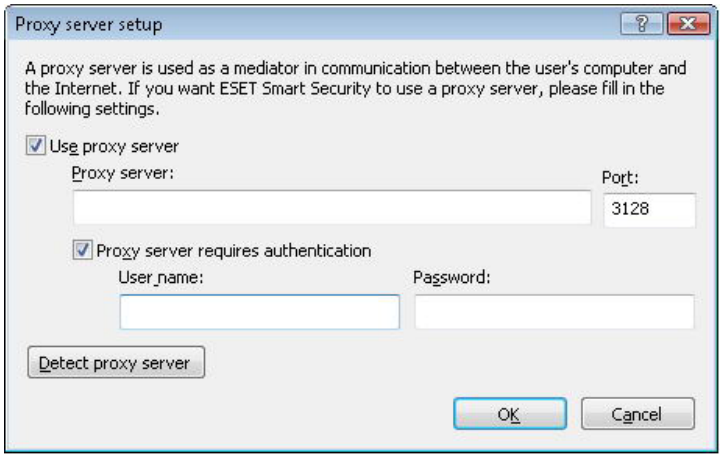
حفاظت ناحیه ایمن به مجرد اتمام نصب "ESS" و همچنین زمانی که رایانه به یک شبکه جدید متصل می‌شود، آغاز می‌گردد. بنابراین به صورت پیش فرض در بسیاری از مواقع نیازی به تعریف ناحیه ایمن وجود ندارد. چرا که به محض اینکه "ESS" یک ناحیه جدید را شناسایی کند، طی یک پنجره محاوره‌ای از کاربر می‌خواهد تا سطح امنیتی مورد نظر جهت آن ناحیه را تنظیم نماید.




*هشدار: پیکربندی ناصحیح یک ناحیه ایمن می‌تواند به عنوان یک خطر امنیتی برای رایانه کاربر تلقی گردد.*

*توجه: به صورت پیش فرض، در یک ناحیه ایمن تمامی ایستگاه‌های کاری دسترسی کامل به فایلها و چاپگرهای به اشتراک گذاشته شده دارند، ترافیک ورودی "RPC" فعال است و همچنین امکان استفاده از سرویس "Remote Desktop Sharing" نیز فراهم آمده است.*

### ۴-۳- تنظیمات مربوط به سرور "proxy"

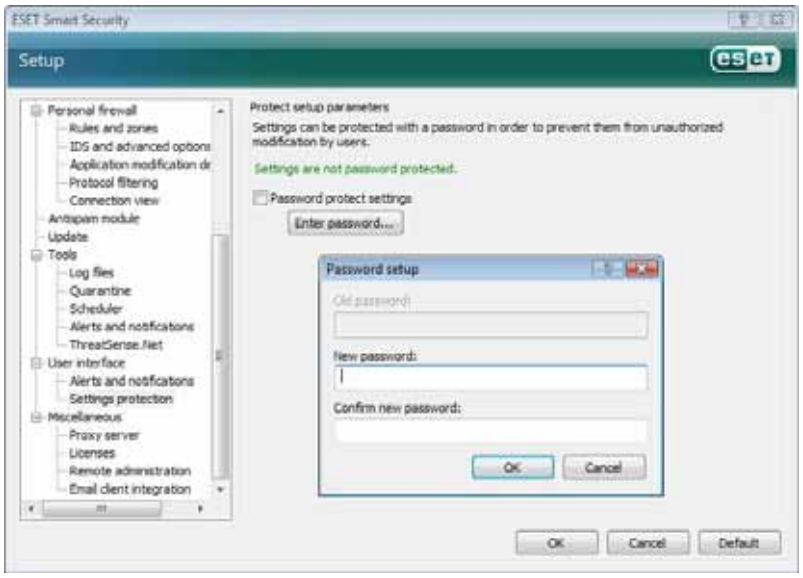



اگر کاربر جهت اتصال به اینترنت از سرور "proxy" استفاده می کند و قصد دارد از رایانه‌ای که "ESS" بر روی آن نصب شده جهت اتصال به اینترنت بهره جوید، لازم است تنظیمات مربوط به سرور "proxy" را در پنجره تنظیمات پیشرفته (کلید F5) لحاظ نماید. برای دسترسی به پنجره پیکر بندی سرور "proxy" کافی است بر روی گزینه "miscellaneous" کلیک کرده و پس از آن آیتم "proxy server" را از نمودار درختی پیشرفته انتخاب کنید. در ادامه گزینه "use proxy server" را تیک زده و سپس "IP" و پورت سرور "proxy" را به همراه شناسه کاربری و کلمه عبور در فیلدهای مربوطه درج نمائید.

اگر اطلاعات ذکر شده در بالا در دسترس کاربر نباشد، می‌تواند با کلیک بر روی دکمه "Detect proxy server" این اطلاعات را جهت استفاده در "ESS" بدست آورد.

*توجه: ممکن است گزینه‌های مربوط به سرور "proxy" برای پروفایلهای مختلف بروزرسانی متفاوت باشند. لذا در چنین شرایطی برای درج اطلاعات مربوط به سرور "proxy" از تنظیمات پیشرفته بروزرسانی استفاده کنید.*

### ۵-۳- حفاظت از تنظیمات انجام شده




تنظیمات امنیتی "ESS" می‌تواند به عنوان یکی از ابعاد سیاست نامه امنیتی سازمانی بسیار حائز اهمیت باشد. چرا که دسترسی غیرمجاز به این تنظیمات موجب به مخاطره افتادن امنیت رایانه می گردد. از این جهت کاربر می‌تواند برای حفاظت از تنظیمات انجام شده توسط کلمه عبور اقدام نماید.

بدین منظور لازم است پس از کلیک بر روی گزینه "setup"، گزینه

"enter entire advanced setup tree …"

را انتخاب نموده و سپس آیتم "user interface" را برگزیده و در ادامه بر روی "settings protection" کلیک کند و نهایتا برروی دکمه "enter password…" کلیک نماید. در خاتمه نیز کلمه عبور را تایپ کرده و سپس جهت تائید آن مجددا کلمه عبور را تایپ می‌نماید و سپس بر روی "OK" کلیک می‌کند. از این کلمه عبور برای اصلاح تنظیمات آتی "ESS" استفاده خواهد شد.

## ۴- کار با بسته نرم افزاری "ESS"

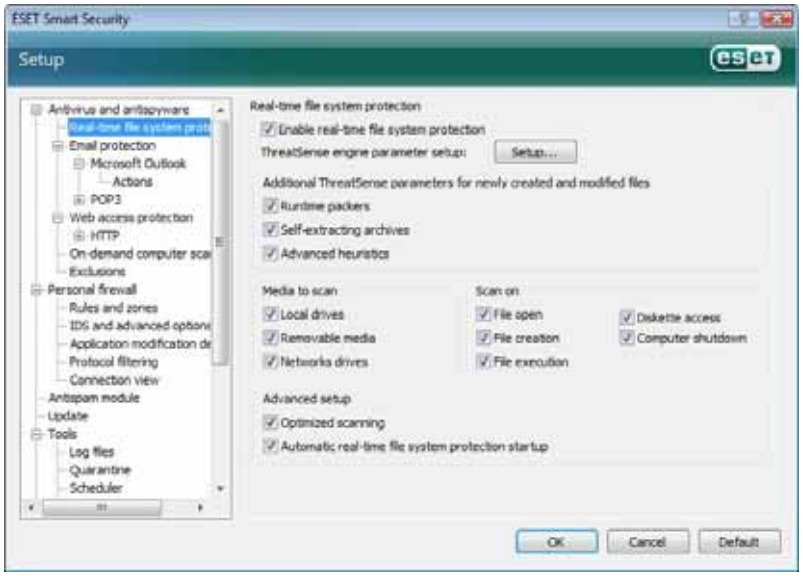
### ۴-۱- حفاظت ضدویروس و ضد جاسوس افزار

ماژول ضدویروس "ESS" با کنترل فایلها، نامه‌های الکترونیک و ارتباطات اینترنتی رایانه را از هجوم کدهای مخرب محافظت می‌کند. در زمانی که یک تهدید دارای کد مخرب شناسایی گردد، ماژول ضدویروس ابتدا آن را بلوکه کرده و سپس فایل آلوده را پاکسازی می‌کند. ضمن اینکه امکان حذف فایل آلوده و یا انتقال آن به مخزن قرنطینه نیز وجود دارد.

#### ۴-۱-۱- حفاظت "real–time" از سیستم فایلها (گارد نرم افزار)

حفاظت "real–time" از سیستم فایلها به معنی کنترل تمامی رخدادهایی در رایانه است که با ماژول ضدویروس ارتباط دارند. به بیان دیگر تمامی فایلها در زمان ایجاد و یا اجرا به لحاظ وجود آلودگی ویروسی مورد پویش قرار می‌گیرند. حفاظت "real–time" از سیستم فایلها از زمان راه‌اندازی رایانه (system startup) اجرا می‌گردد.

### ۱-۱-۱-۴- تنظیمات مربوط به کنترل نرم افزار




حفاظت "real–time" از سیستم فایلها (گارد نرم افزار) تمامی واحدهای حافظه (فلاپی، CD و ...) را به لحاظ وجود آلودگی ویروسی مورد بررسی قرار می‌دهد و رخدادهای گوناگون مرتبط با تهدیدات رایانه‌ای بر نوع این کنترل تاثیر می‌گذارند. سیستم کنترل نرم افزار از روش‌های شناسایی مربوط به فناوری "ThreatSense" بهره می‌جوید. ضمن اینکه رفتار سیستم کنترلی می‌تواند در مواجه با فایلهای موجود و فایلهایی که اخیرا ایجاد گردیده‌اند، متفاوت باشد.

به عنوان مثال برای فایلهایی که اخیرا ایجاد گردیده‌اند می‌توان از سطح عمیق‌تری از کنترل استفاده نمود.

### ۱-۱-۱-۴- آیتم‌های مورد نظر جهت پویش

به صورت پیش فرض تمامی انواع حافظه به لحاظ وجود تهدیدات رایانه‌ای مورد پویش قرار می‌گیرند که عبارتند از:

۱- هارد دیسک رایانه

۲- حافظه های قابل حمل نظیر دیسکت ها، حافظه‌های دارای پورت USB و ...

۳- درایوهای شبکه‌ای (mapped drives)

توصیه شرکت "ESET" این است که از تنظیمات پیش فرض مربوط به این مقوله استفاده شود و حتی الامکان این تنظیمات تغییر پیدا نکند.

### ۱-۱-۱-۴- پویش در زمان بروز یک رخداد

به صورت پیش فرض تمامی فایلها در زمان ایجاد، باز شدن و یا اجرا مورد پویش قرار می‌گیرند. توصیه می‌شود از تنظیمات پیش فرض مربوطه استفاده شود. زیرا حداکثر سطح حفاظتی را برای رایانه تضمین خواهد کرد.

گزینه "diskette accESS" کنترل سکتور راه‌اندازی (boot sector) دیسکت را بر عهده دارد. ضمن اینکه گزینه "computer shutdown" نیز وظیفه کنترل سکتورهای راه‌اندازی دیسکت سخت را در زمان خاموش نمودن رایانه عهده‌دار است. اگرچه ویروسهای

راه‌اندازی (boot viruses) امروزه رایج نیستند، لیکن توصیه می‌شود دو گزینه اخیر را فعال نگه دارید تا حفاظت کاملتری از رایانه به عمل آید.

### ۳-۱-۱-۴- پارامترهای "ThreatSense" اضافی در مورد فایلهای ایجاد شده جدید

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

علاوه بر فایلهایی که اخیرا ایجاد گردیده‌اند، پویش فایل‌های آرشیو شده خود اجرا (self–extracting files) و همچنین "runtime packer" ها نیز مورد پویش قرار می‌گیرند.

### ۴-۱-۱-۴- تنظیمات پیشرفته

جهت کاهش اثرات نامطلوب در زمان حفاظت "real–time" رایانه، فایلهایی که یک بار مورد پویش قرار گرفته‌اند به صورت مجدد پویش نخواهند گردید (مگر اینکه این فایلها مورد تغییر قرار گرفته باشند).

همچنین فایلها پس از هر بار بروز رسانی بانک اطلاعاتی شناسه ویروسهای رایانه‌ای مورد پویش قرار می‌گیرند. تنظیمات مربوط به این رفتار در پیکربندی گزینه "optimized scanning" انجام می‌پذیرد. لذا اگر این ویژگی غیر فعال شده باشد، تمامی فایلها در هر بار دسترسی به آنها مورد پویش قرار خواهند گرفت.

به صورت پیش فرض، حفاظت "real–time" با شروع کار رایانه آغاز می‌گردد و یک حفاظت مستمر و بی وقفه را از رایانه به عمل می‌آورد. لذا در موارد خاص - به عنوان مثال در زمان درگیر شدن گارد "ESS" با گارد یک نرم افزار امنیتی دیگر – امکان لغو حفاظت "real–time" نرم افزار "ESS" از طریق غیر فعال نمودن گزینه

"Automatic real–time file system protection startup"

فراهم آمده است.

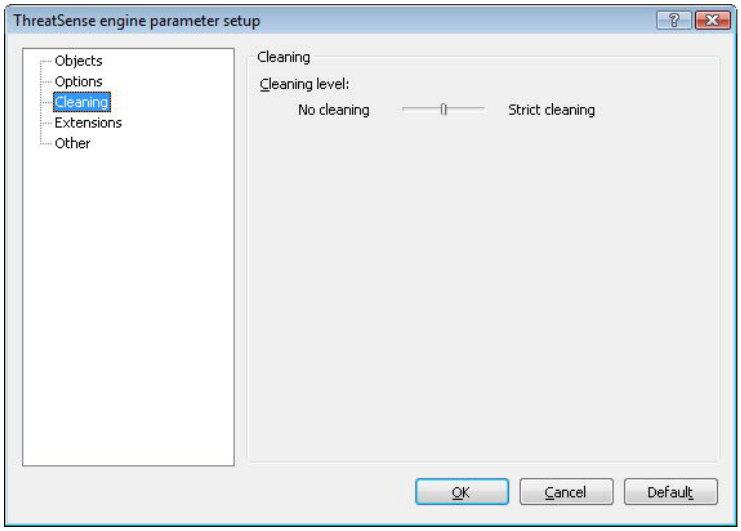
### ۲-۱-۱-۴- سطوح پاکسازی آیتم‌های دارای آلودگی ویروسی

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

- ✓ اولین سطح عبارت از نمایش پنجره هشدار به همراه دیگر گزینه‌ها جهت مقابله با تهدید شناسایی شده است. لذا کاربر باید یکی از روش‌های مقابله‌ای ارائه شده را برای هر یک از تهدیدات شناسایی شده برگزیند. این گزینه مناسب کاربران حرفه‌ای است که با گام‌های مختلف مبارزه با تهدید رایانه‌ای آشنایی کامل دارند.
- ✓ سطح بعدی سطح پیش فرض نرم افزار است. در این حالت نرم افزار روش مقابله از پیش تعیین شده را در مورد تهدید شناسایی گردیده به صورت خودکار اعمال می‌کند. شناسایی و پاک نمودن فایل آلوده نیز طی یک پنجره

کوچک که در گوشه پائین سمت راست صفحه نمایش قابل رویت خواهد بود 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 شده‌ای برای مقابله با آن تهدید تعیین نگردیده باشد، مقابله خودکار با آن تهدید انجام نخواهد پذیرفت.

- ✓ سطح سوم سطح تهاجمی‌تری است. در این سطح تمامی آیتم‌های 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 می‌شود از سطح مورد نظر در شرائط بسیار ویژه استفاده گردد.




### ۳-۱-۱-۴- چه زمانی می‌بایست پیکربندی تنظیمات حفاظت "real–time" را اصلاح نمود.

حفاظت "real–time" یکی از اجزای اصلی در تامین امنیت یک سیستم رایانه‌ای است. بنابراین در زمان اصلاح و تغییر پارامترهای آن باید توجه خاصی مبذول گردد و توصیه شرکت "ESET" آن است که در این موارد بسیار خاص تنظیمات مربوط به آن تغییر پذیرد.

پس از نصب "ESS" تمامی تنظیمات می‌بایست به گونه‌ای انجام پذیرند که حداکثر سطح حفاظتی را برای کاربران ایجاد کنند. جهت استفاده از تنظیمات پیش فرض نیز می‌توان بر روی دکمه "default" موجود در گوشه پائین سمت راست پنجره "real–time file system protection" کلیک نمود.

### ۴-۱-۱-۴- بررسی حفاظت "real–time"

جهت بررسی وضعیت عملکرد صحیح حفاظت "real–time" در شناسایی تهدیدات رایانه‌ای می‌توان از فایل تست موجود در سایت eicar.com استفاده نمود.

این فایل تست یک فایل ویژه بی خطر است که توسط تمامی نرم افزارهای ضدویروس قابل شناسایی است و توسط شرکت eicar به منظور تست عملکرد نرم افزارهای ضدویروس ایجاد گردیده است. جهت دانلود این فایل می‌توان به آدرس اینترنتی ذیل مراجعه نمود.

"HTTP://www.eicar.org/download/eicar.com"

*توجه: "eicar" مخفف عبارتی است که به معنای انستیتوی اروپایی در زمینه تحقیقات ضدویروس‌های رایانه‌ای می‌باشد.*

*توجه: قبل از دانلود فایل تست لازم است دیواره آتش شخصی را غیر فعال کنید. در غیر این صورت دیواره آتش شخصی از دانلود فایل تست جلوگیری به عمل می‌آورد.*

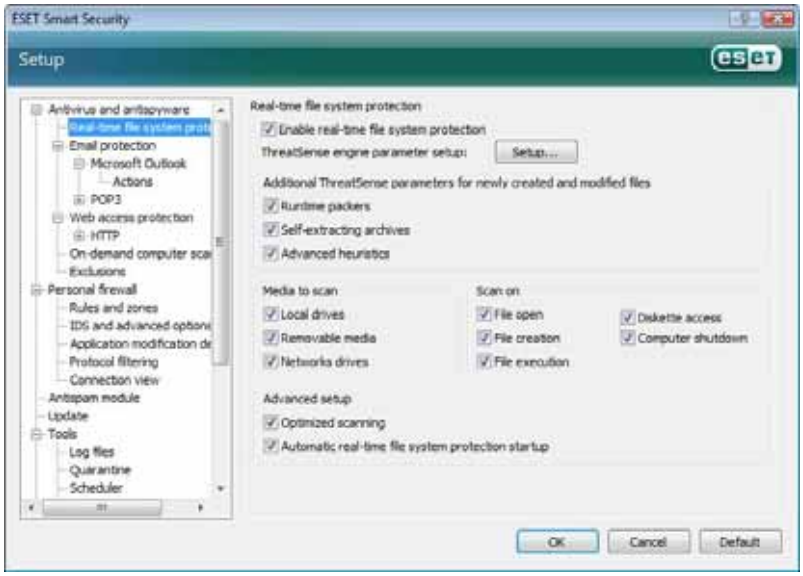
### ۵-۱-۱-۴- در زمان عملکرد غیر صحیح حفاظت "real–time" چه باید کرد؟

در این زیر بخش به بررسی وضعیت‌های مختلف عملکرد غیر صحیح حفاظت "real–time" و روش حل معضل ایجاد شده خواهیم پرداخت.

*الف) حفاظت "real–time" غیر فعال شده است.*

اگر حفاظت "real–time" بصورت غیر عمدی توسط کاربر غیر فعال گردیده باشد، لازم است مجددا فعال شود. به منظور فعال سازی مجدد آن کافی است به قسمت "setup" مراجعه و پس از انتخاب گزینه "antivirus and antispyware" با کلیک بر روی گزینه "enable" در قسمت"real–time file system protection" موجود در پنجره اصلی مبادرت به فعال سازی حفاظت "real–time" نمائید.

همچنین یکی از دلایل محتمل عدم اجرای حفاظت "real–time" در زمان راه‌اندازی رایانه نیز می‌تواند غیر فعال بودن راه‌اندازی خودکار آن باشد. جهت فعال کردن این مورد نیز می‌توانید با فشردن کلید "F5" صفحه کلید وارد پنجره تنظیمات پیشرفته شده و در قسمت مربوط به نمودار درختی تنظیمات پیشرفته بر روی گزینه "real–time file system protection" کلیک نموده و پس از آن در قسمت پائینی پنجره تنظیمات پیشرفته گزینه "automatic real–time file system protection startup" را تیک بزنید.




*ب) زمانی که حفاظت "real–time" تهدیدات را شناسایی و رفع آلودگی نمی‌کند.*

در ابتدا اطمینان حاصل کنید که بجز "ESS" هیچ نرم افزار ضدویروس دیگری بر روی رایانه نصب نشده است. نکته اینجاست که در صورت وجود دو گارد ضدویروس مقیم در حافظه احتمال تداخل آنها با یکدیگر و عدم کارکرد آنها وجود دارد. لذا توصیه می‌شود هر نرم افزار ضدویروس دیگری که در کنار "ESS" بر روی رایانه نصب است را حذف نمائید.

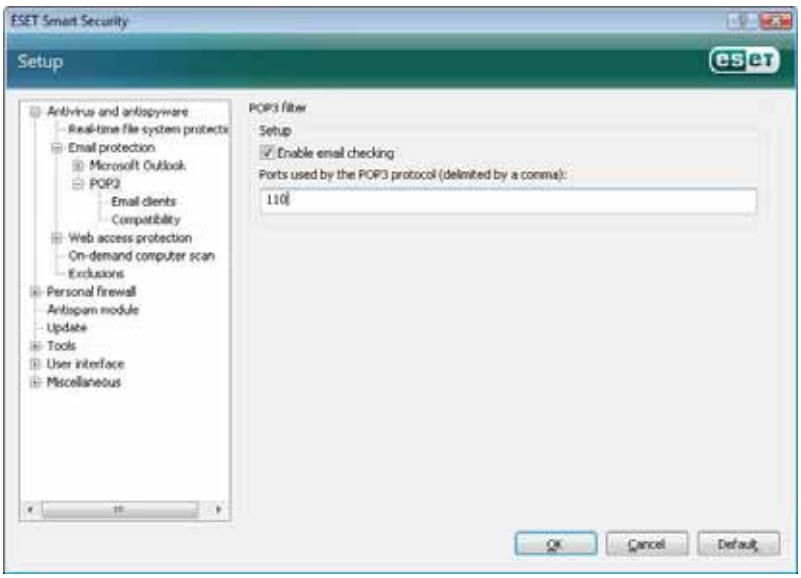
*ج) حفاظت "real–time" آغاز نمی‌گردد.*

اگر حفاظت "real–time" در زمان راه‌اندازی رایانه آغاز به کار نکند و حال آنکه این قابلیت از قبل فعال است، ممکن است دلیل اصلی این مورد تداخل حفاظت "real–time" با یک برنامه دیگر باشد. در این شرائط بهتر است طی یک نامه الکترونیک موارد را با قسمت خدمات فنی شرکت "ESET" در میان گذاشته تا نسبت به ارائه طریق جهت حل مشکل اقدام شود.

### ۲-۱-۴- حفاظت از نامه‌های الکترونیک

با استفاده از "ESS" تمامی نامه‌های الکترونیکی دریافتی از طریق پروتکل "POP3" مورد کنترل قرار می‌گیرند. همچنین "ESS" با استفاده از برنامه "plug–in" مربوط به نرم افزار "Microsoft Outlook" تمامی ارتباطات نرم افزارهای مدیریت پست الکترونیک (اعم از ارتباطات "POP3" ، "MAPI" ، "IMAP" و "HTTP" ) را کنترل می‌کند. به بیان دیگر این نرم افزار با بهره‌گیری از متدهای "ThreatSense" تمامی نامه‌های ورودی را مورد تجزیه و تحلیل قرار می‌دهد. این بدان معنی است که بررسی کدهای مخرب حتی قبل از تطابق آنها با بانک اطلاعاتی شناسه ویروسهای رایانه‌ای نرم افزار انجام می‌پذیرد. نکته آخر اینکه پویش ارتباطات پروتکل "POP3" مستقل از نوع نرم افزار مدیریتی پست الکترونیکی مورد استفاده می‌باشد.

#### ۱-۲-۱-۴- بررسی پروتکل "POP3"




معروف ترین و رایج‌ترین پروتکل که نرم افزارهای مدیریت پست الکترونیک از آن جهت دریافت نامه‌های الکترونیکی استفاده می‌کنند عبارت از پروتکل "POP3" است و جالب اینجاست که کنترل این پروتکل توسط "ESS" کاملا به صورت مستقل از نرم افزار کاربردی مدیریت پست الکترونیک مورد استفاده به انجام می‌رسد.

ماژولی که بررسی این پروتکل را بر عهده دارد نیز در ابتدای شروع کار رایانه فعال شده و در حافظه موقت به صورت مقیم باقی می‌ماند. لذا لازم است جهت عملکرد صحیح این ماژول همواره از فعال بودن آن اطمینان حاصل کنید. به صورت پیش فرض تمامی ارتباطات پورت ۱۱۰ (پورت مربوط به POP3) به صورت خودکار مورد پویش قرار می‌گیرد. ضمن اینکه در صورت نیاز می‌توان پورتهای دیگری

را نیز جهت پویش مشخص نمود. فقط لازم است شماره پورتها را با کاما از یکدیگر جدا کنید. نکته آخر اینکه ارتباطات کد شده مورد کنترل قرار نمی‌گیرند.

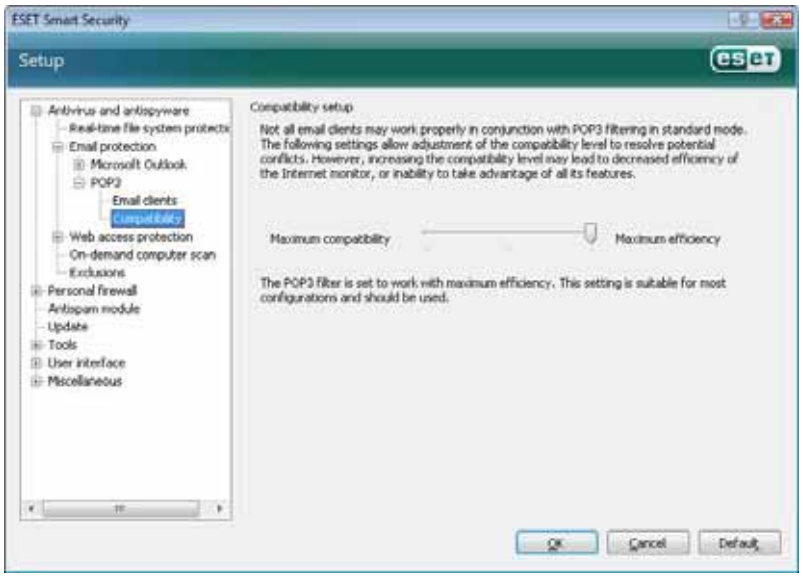
### ۱-۱-۲-۱-۴- سازگاری

ممکن است برخی از نرم‌افزارهای مدیریت پست الکترونیک با فیلترینگ پروتکل "POP3" سازگاری لازم را نداشته باشند. به عنوان مثال اگر سرعت ارتباط اینترنت پائین باشد، ممکن است به هنگام کنترل و بررسی نامه‌های دریافتی دچار خطای "timeout" شوند. در چنین شرائطی بهتر است روند کنترل و بررسی نامه‌های دریافتی را اصلاح نمائید. به عنوان مثال در زمانی که سرعت ارتباط اینترنتی پائین است می‌توان با کاهش سطح کنترل باعث افزایش سرعت فرایند پاکسازی فایلهای دارای آلودگی ویروسی گردید.

بنابر این به منظور تنظیم سطح کنترل فرایند فیلترینگ پروتکل "POP3" کافی است پس از انتخاب گزینه "antivirus and antispyware" به قسمت "email protection" رفته و سپس قسمت "compatibility" را از بخش "POP3" برگزینید.

اگر گزینه "maximum efficiency" فعال باشد، تهدیدات شناسایی شده از نامه‌های آلوده پاک گردیده و اطلاعات مربوط به تهدید شناسایی شده قبل از عنوان نامه الکترونیکی مورد نظر درج می‌گردد. در این حالت لازم است گزینه های "clean" و یا "delete" فعال بوده و یا یکی از دو سطح پاکسازی "default" و یا "strict" فعال گردیده باشند.

حالت "medium compatibility" روش دریافت نامه‌های الکترونیکی را اصلاح می‌کند.

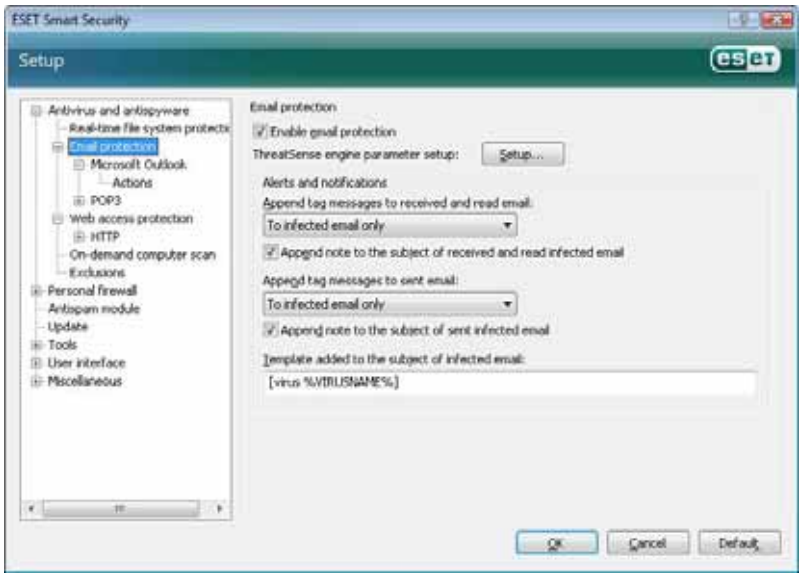



به بیان دیگر نامه الکترونیک به مجرد دریافت توسط نرم افزار مدیریت نامه‌های الکترونیکی مورد پویش قرار می‌گیرد. همانطور که پیدا است خطر آلودگی دیگر فایلها در حالت اخیر افزایش می‌یابد. نکته دیگر اینکه تنظیمات سطح پاکسازی و ایجاد برچسب‌های پیام مربوط به آلودگی نامه دریافتی دقیقا شبیه حالتی است که "maximum efficiency" انتخاب گردیده است.

زمانی که حالت "maximum compatibility" نیز انتخاب شده باشد، "ESS" کاربر را از دریافت یک نامه دارای آلودگی ویروسی آگاه می‌سازد. ضمن اینکه هیچگونه اطلاعاتی در رابطه با تهدید شناسایی شده به ردیف موضوع نامه و یا بدنه نامه افزوده نمی‌شود و تهدیدات شناسایی شده به صورت خودکار حذف نمی‌گردند. لذا لازم است کاربر نسبت به پاک کردن نامه آلوده دریافتی از طریق نرم افزار مدیریت پست الکترونیک خود اقدام نماید.

### ۲-۲-۱-۴- یکپارچگی با نرم افزارهای "Microsoft Outlook"، "Outlook Express" و "Windows Mail"

یکپارچگی "ESS" با نرم افزارهای مدیریت پست الکترونیک باعث افزایش سطح حفاظتی فعال در مقابله با تهدیداتی است که از طریق نامه‌های آلوده رایانه را تهدید می‌کنند.




بنابراین اگر نرم افزار مدیریت پست الکترونیک کاربر جزء نرم افزارهایی است که توسط "ESS" پشتیبانی شده‌اند، می‌توان یکپارچگی مربوط به آنها را در "ESS" فعال نمود. اگر این یکپارچگی فعال شود، نوار ابزار ضد هرزنامه "ESS" به صورت مستقیم در رابط گرافیکی کاربر نرم افزار مدیریت پست الکترونیک به نمایش در خواهد آمد تا بتوان حفاظت موثرتری را از نامه‌های الکترونیک به عمل آورد.

برای دسترسی به تنظیمات مربوط به سازگاری و یکپارچگی لازم است پس از کلیک بر روی گزینه "setup" وارد قسمت "enter entire advanced setup tree" شده و سپس به قسمت "miscellaneous" بروید و نهایتا بخش "email client integration" را گزینش نمائید. با استفاده از این پنجره های محاوره‌ای قادر خواهید بود تا تنظیمات مربوط به یکپارچگی "ESS" و نرم افزار مدیریت پست الکترونیک را انجام دهید. نرم افزارهای مدیریت پست الکترونیک پشتیبانی شده در حال حاضر عبارت از "Microsoft Outlook"، "Outlook Express" و "Windows Mail" هستند. نکته آخر اینکه حفاظت از نامه‌های الکترونیکی به مجرد فعال کردن گزینه "enable email protection" موجود در قسمت "antivirus and antispyware" پنجره تنظیمات پیشرفته (کلید F5) آغاز می‌گردد.

### ۱-۲-۱-۴- افزودن برچسب پیام به متن نامه الکترونیک

می‌توان به بدنه یا موضوع هر یک از نامه‌هایی که توسط "ESS" مورد کنترل قرار می‌گیرند یک برچسب پیام افزود. این ویژگی باعث افزایش سطح اعتبار نامه نزد گیرنده شده و همچنین اگر نامه الکترونیک دریافتی حاوی تهدید باشد، اطلاعات ارزشمندی را در خصوص تهدید و فرستنده آن به گیرنده ارائه می‌نماید. برای دسترسی به گزینه‌های مربوط به این ویژگی ابتدا وارد پنجره تنظیمات پیشرفته شده و پس از انتخاب گزینه "antivirus and antispyware protection" آیتم "email protection" را برگزینید.

در اینجا می‌توان با استفاده از گزینه‌های

"append tag messages to received and read mail"

و "append tag messages to sent mail" هم برای نامه‌های دریافتی و هم برای نامه‌های ارسالی از برچسب پیام استفاده نمود. همچنین کاربر می‌تواند مشخص کند که برای چه نوع نامه‌ای (اعم از تمامی نامه‌ها، صرفا نامه‌های آلوده و یا هیچ یک از نامه‌ها) از

برچسب استفاده گردد. ضمن اینکه با استفاده از "ESS" امکان درج پیام در ردیف مربوط به موضوع نامه الکترونیک آلوده نیز وجود خواهد داشت. بدین منظور نیز از گزینه‌های

"append note to the subject of received and read infected email"

و

"append note to the subject of sent infected email"

استفاده به عمل می‌آید.

متن برچسب پیام‌ها نیز در قالب فیلد الگویی که به موضوع نامه الکترونیک آلوده افزوده می‌گردد قابل اصلاح و تغییر است. متن برچسب پیام کمک شایانی به خودکار نمودن فرایند فیلتر نمودن نامه‌های آلوده می‌کند. ضمن اینکه کاربر را قادر می‌سازد تا بتواند نامه‌ای که دارای موضوع خاصی است را (در صورت پشتیبانی توسط نرم افزار مدیریت پست الکترونیک) به پوشه‌ای مجزا انتقال دهد.

### ۳-۲-۱-۴- حذف آلودگی‌ها و تهدیدات رایانه‌ای

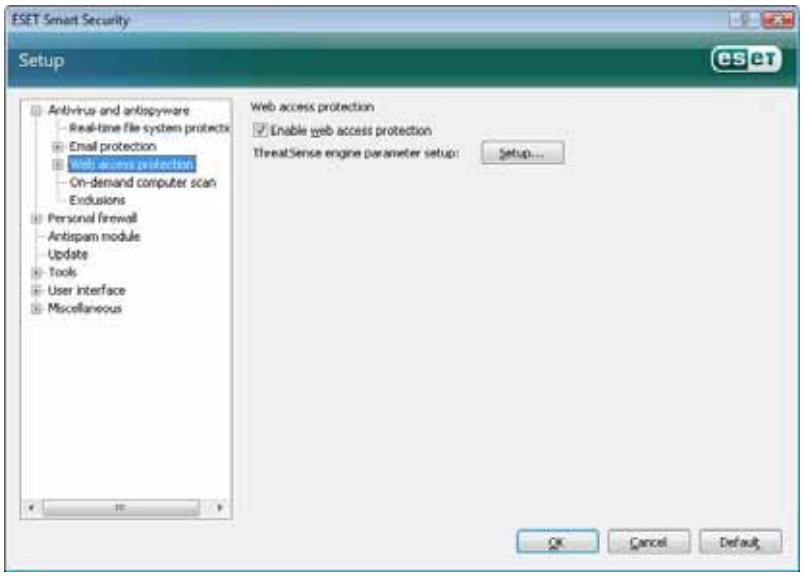
"ESS" در زمان دریافت یک نامه دارای آلودگی ویروسی طی پنجره‌ای به کاربر اطلاع رسانی لازم را انجام می‌دهد. در پنجره این نامه به نام فرستنده، (موضوع) نامه و نام تهدید شناسایی شده اشاره شده است. در قسمت پائین پنجره نیز گزینه‌هایی از قبیل پاکسازی نامه آلوده، پاک کردن آن و یا باقی گذاشتن آن در اختیار کاربر قرار گرفته است.

توصیه "ESET" این است که در اغلب موارد نسبت به پاکسازی نامه آلوده و یا پاک نمودن آن اقدام کنید. در مواردی نیز که لازم است حتما به نامه دسترسی پیدا کنید، می‌توانید از گزینه باقی ماندن نامه (leave) استفاده نمائید. همچنین اگر مد "strict cleaning" فعال باشد، در زمان دریافت یک نامه آلوده صرفا پنجره ای جهت اطلاع رسانی به کاربر گشوده می‌شود که فاقد هرگونه گزینه جهت مقابله با تهدید شناسایی شده است.

### ۳-۱-۴- حفاظت در زمان دسترسی به صفحات وب

یکی از ویژگی‌های استاندارد هر کامپیوتر شخصی عبارت از ارتباط با اینترنت است. متاسفانه، بستر ارتباطی اینترنت به یک وسیله اصلی جهت انتقال کدهای مخرب تبدیل شده است. بدین لحاظ لازم است توجه ویژه‌ای به حفاظت در زمان دسترسی به صفحات وب داشته باشید.

لذا توصیه می‌شود حتما گزینه "enable web access protection" را فعال نمائید. جهت دسترسی به این گزینه کافی است با فشردن کلید "F5" پنجره تنظیمات پیشرفته را گشوده و از نمودار درختی سمت چپ پنجره گزینه "antivirus and antispyware protection" را برگزینید و نهایتا زیر منوی "web access protection" را انتخاب نمائید.

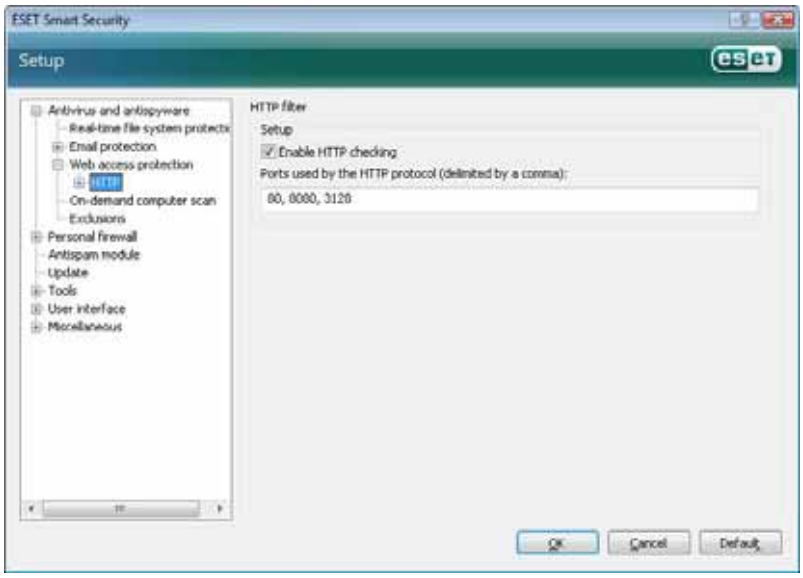



### ۱-۳-۱-۴- پروتکل "HTTP"

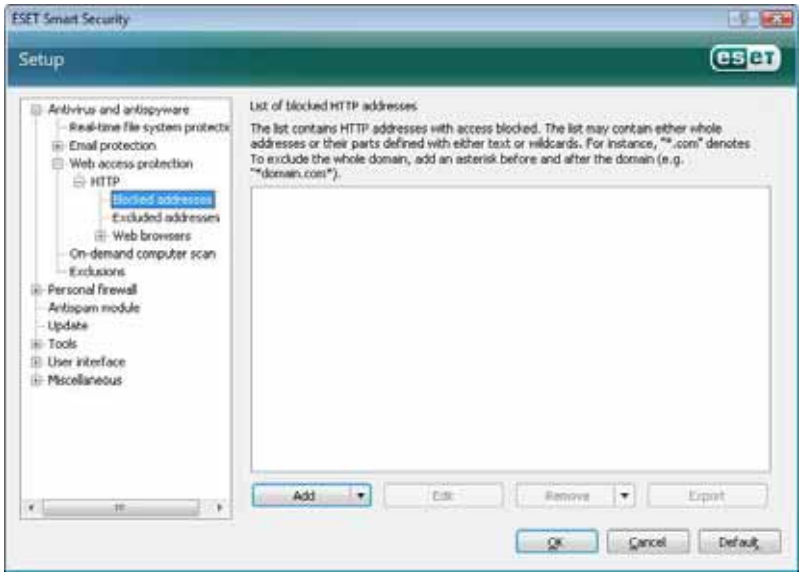
ویژگی اصلی "web access protection" کنترل ارتباطات بین برنامه‌های مرورگر وب و سرورهای راه دور بر اساس قوانین پروتکل "HTTP" است. بنابراین "ESS" به صورت پیش فرض به گونه‌ای پیکربندی شده است که از استانداردهای "HTTP" مربوط به اکثر نرم افزارهای مرورگر استفاده کند. با این حال، تنظیمات مربوط به گزینه‌های کنترل "HTTP" را می‌توان در زیر منوی "HTTP" موجود در قسمت "web access protection" مورد اصلاح و تغییر قرار داد. در پنجره "HTTP filter setup" امکان فعال سازی یا غیر فعال نمودن کنترل "HTTP" با استفاده از گزینه "enable HTTP checking" فراهم آمده است.

ضمن اینکه کاربر قادر خواهد بود تا شماره پورت مورد استفاده سیستم جهت ارتباطات "HTTP" را نیز درج نماید. به صورت پیش فرض از شماره پورت‌های "80" ، "8080" و "3128" استفاده به عمل می‌آید.

جهت درج پورت‌های دیگر لازم است بین شماره پورتها از کاما استفاده شود تا "ESS" تمامی این پورتها را شناسایی و ترافیک "HTTP" آنها را پویش کند.



### ۱-۱-۳-۱-۴- آدرسهای بلوکه شده و صرف نظر گردیده




در قسمت تنظیمات کنترل "HTTP" می‌توان فهرستی از آدرس‌های اینترنتی (url) بلوکه شده و یا صرف نظر گردیده را درج نمود. در کادر محاوره‌ای هر دو قسمت

"blocked addresses"

و

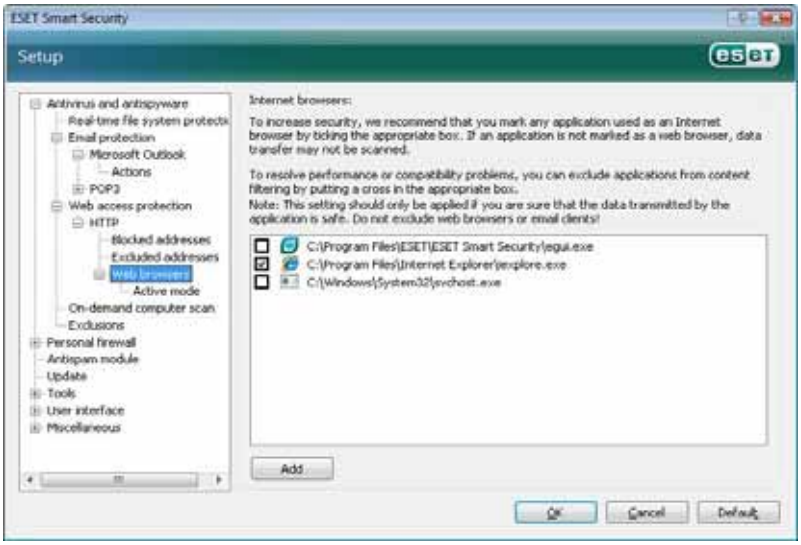
"excluded addresses"

می‌توان دکمه‌های "add"، "edit" و "remove" را ملاحظه نمود. کاربر با استفاده از این دکمه‌ها می‌تواند به ایجاد و ویرایش فهرست و یا حذف آیتم‌های آن مبادرت ورزد. اگر آدرس اینترنتی مورد نظر کاربر جهت مراجعه به آن در فهرست "blocked" قرار داشته باشد، "ESS" از دسترسی کاربر به آن آدرس (توسط مرورگر وب) جلوگیری به عمل می‌آورد.

به بیان دیگر "ESS" صرفا آدرسهایی را که در فهرست "excluded" درج شده‌اند را در زمان دسترسی به لحاظ وجود کدهای مخرب مورد بررسی قرار نخواهد داد. در هر دو فهرست می‌توان از سمبل‌های "*" و"؟" استفاده کرد. در واقع کاربر می‌تواند از "*" به جای هر رشته‌ای از کاراکترها و از "?" صرفا به جای یک کاراکتر استفاده کند. لازم است کاربر در زمان ایجاد فهرست "excluded" توجه و دقت ویژه‌ای داشته باشد. زیرا صرفا باید آدرس‌هایی که ۱۰۰٪ به لحاظ حفاظتی مورد تائید هستند را در این فهرست درج نمود. ضمن اینکه باید به شیوه صحیحی از کاراکترهای "*" و "?" بهره جست.

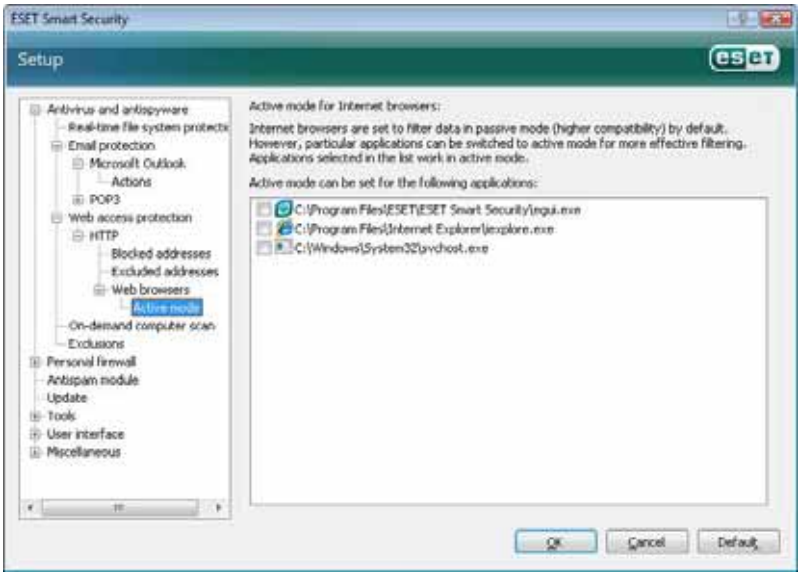
### ۲-۱-۳-۱-۴- مرورگرهای وب

"ESS" دارای ویژگی "web browsers" نیز می‌باشد. کاربر با استفاده از این ویژگی می‌تواند مشخص کند که آیا یک برنامه کاربردی از جمله نرم‌افزارهای مرورگر وب است و یا خیر. به بیان دیگر اگر نرم‌افزاری از طرف کاربر به عنوان یک نرم افزار مرورگر وب مشخص شود، "ESS" تمامی ارتباطات آن از طریق بستر اینترنت را صرف نظر از شماره پورتهای ارتباطی مورد کنترل قرار می‌دهد.




طبیعتا چنین ویژگی مهمی را می‌توان مکمل

ویژگی کنترل پروتکل "HTTP" دانست. چرا که ماژول کنترل کننده "HTTP" صرفا پورتهایی که از قبل مشخص شده‌انـد را مـورد کنترل قرار می‌دهد. لذا با توجه به اینکه بسیاری از سرویس‌های اینترنتی از پورتهایی با شماره‌های نامعلوم و یا متغیر استفاده می‌کنند، استفاده از ویژگی مورد بحث اهمیت دو چندانی پیدا می‌کند.



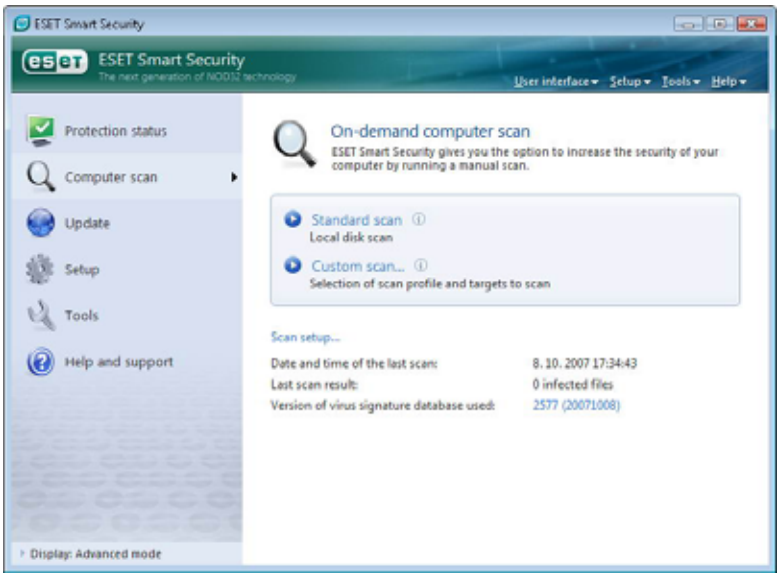

فهرست نرم افزارهایی کـه کـاربر مـی‌توانـد بـه عنوان مرورگر وب تعیـین نمایـد بـا کلیـک بـر روی گزینـه "HTTP" و پـس از آن انتخـاب زیـر منـوی "web browsers" در دسـترس قرار می گیرد. زیر منوی "web browsers" نیـز دارای زیـر منـوی دیگـری بـه نـام "active mode" است که بـا اسـتفاده از آن می‌توان مد کنتـرل مرورگرهـای وب را تعیـین کرد. ویژگی "active mode" از ایـن جهـت که اطلاعات تبادلی را به صورت کلی و جامع مورد بررسی قرار می‌دهد، از جمله امکانات مفید به حساب می‌آید.

همچنین اگر این گزینه فعال نگردد، کنترل ارتباطات نرم‌افزارهای کاربردی کندتر انجام می‌پذیرد. لذا اگرچه ایـن مـورد باعـث کـاهش تاثیر پذیری فرایند تائید اعتبار داده‌ها می‌گردد، باعث افزایش سازگاری نرم افزارهای کاربردی فهرست شـده (بـه عنـوان مرورگـر وب) می‌شود. نکته آخر اینکه اگر در زمان فعال بودن این گزینه مشکلی برای کاربر اتفاق نیفتد، توصیه می‌شود این گزینـه در حالـت فعـال باقی بماند.

### ۴-۱-۴- پویش رایانه

اگر کاربر بر اثر کارکرد ناصحیح و غیر معمول رایانه احساس کند که ممکن است رایانه دچار آلودگی ویروسی شده باشـد، مـی‌توانـد بـا اجرای ماژول پویش دستی رایانه را به لحاظ وجود آلودگی ویروسی مورد پویش قرار دهد. به عنوان یک نقطه نظر امنیتـی مـی‌بایـست رایانه را به طور مرتب و روتین مورد پویش دستی قرار داد، نه صرفا زمانی که رایانه مشکوک به آلودگی ویروسی است. زیرا پویش مرتب رایانه باعث آشکارسازی تهدیداتی می‌شود که در زمان ایجاد توسط گارد نرم افزار شناسایی نشده‌اند. این مورد می‌تواند به دلایلی نظیـر غیرفعال بودن پویشگر "real–time" در زمانی کپی فایل آلوده به حافظه رایانه و یا بروز نبودن بانک اطلاعاتی شناسه ویروسها اتفـاق افتد.

شرکت "ESET" توصیه می‌کند رایانه را حداقل ماهی دوبار به صورت دستی مورد پویش قرار دهید. ضمن اینکه مـی‌توانیـد از برنامـه زمان بندی نرم افزار نیز جهت انجام این مهم استفاده به عمل آورید. جهت دسترسی به این ابزار کافی است از قسمت "tools" گزینـه "schedular" را برگزینید.




### ۱-۴-۱-۴- انواع پویش

پویش رایانه توسط "ESS" بـه دو نـوع تقـسیم می‌شود:

الف) پویش استاندارد

ب) پویش سفارشی یا "custom"

زمانی که کاربر مبادرت به انجام پویش اسـتاندارد مـی‌کنـد، نـرم افـزار بـدون نیـاز بـه هـیچ گونـه پیکربندی پارامترهای پویش مبـادرت بـه پـویش رایانه می‌کند. در حالت پـویش "custom" نیـز همه موارد اعم از انتخاب آیتم‌های مورد نظر جهت پویش، انتخاب پروفایل پویش و ... توسط کاربر انجام می‌پذیرد.

### ۱-۱-۴-۱-۴- پویش استاندارد

ویژگی پویش استاندارد با روش ساده و قابل فهمی به کاربر امکان می‌دهد تا بتواند بدون هرگونه تنظیمات خاصی مبـادرت بـه پـویش رایانه نموده و آلودگی‌های ویروسی را از بین ببرد. مزیت اصلی این روش پویش عبارت از عملکرد ساده آن بدون نیاز به انجام تنظیمات پیچیده می‌باشد. در روش مورد بحث تمامی فایلهای موجود بر روی دیسک سخت رایانه (شامل فایلهای مربوط به نامه‌های الکترونیکـی و فایل‌های آرشیو شده) مورد پویش واقع شده و آیتم‌های آلوده به صورت خودکار مورد پاکسازی قرار گرفته و یا پاک می‌شـوند. ضـمن اینکه در این حالت سطح پاکسازی در حالت پیش فرض قرار می‌گیرد. همچنین پروفایل پویش استاندارد نیز به منظور استفاده کاربرانی طراحی گردیده است که تمایل دارند رایانه خود را با روش سریع و ساده مورد پویش قرار دهند. در این پروفایل تمامی پارامترهای یـک پویش موثر و پاکسازی آیتم‌های آلوده بدون نیاز به انجام پیکربندی خاص لحاظ گردیده است.

### ۲-۱-۴-۱-۴- پویش "custom"

پویش "custom" روش بهینه‌ای است که در آن کاربر می‌تواند پارامترهای پویش از جمله انتخاب آیتم‌های مورد نظر جهـت پـویش و همچنین روشهای پویش را خود مشخص کند. مزیت اصلی روش "custom" نیز عبارت از امکان انجـام تنظیمـات بـا جزئیـات کامـل توسط کاربر است. ضمن اینکه می‌توان ایـن تنظیمـات را در پروفایـل "user–defined" ذخیـره سـازی نمـوده و از آن بـرای انجـام پویش‌های بعدی با پارامترهای تنظیم شده موجود در پروفایل "user–defined" بهره جست.

به منظور مشخص نمودن آیتم مورد نظر جهت پویش کافی است از منوی بازشونده انتخاب سریع آیتم جهت پویش و یا نمودار آیتم‌های قابل پویش موجود در رایانه استفاده شود. به علاوه، امکان انتخاب آیتم‌ها جهت پویش از طریق سطوح پاکسازی نیز امکان پذیر است. بدین منظور کافی است بر روی گزینه "setup..." کلیک کرده و گزینه "cleaning" را برگزینید.

همچنین اگر تمایل دارید صرفا رایانه را بدون پاکسازی آیتم‌های آلوده مورد پویش قرار دهید، می‌توانید گزینه "scan without cleaning" را تیک بزنید.

توصیه می‌شود صرفا کاربران حرفه‌ای که تجربه کار با نرم افزارهای ضدویروس و تنظیمات مربوط به آنها را دارند از گزینه پویش "custom" استفاده به عمل آورند.

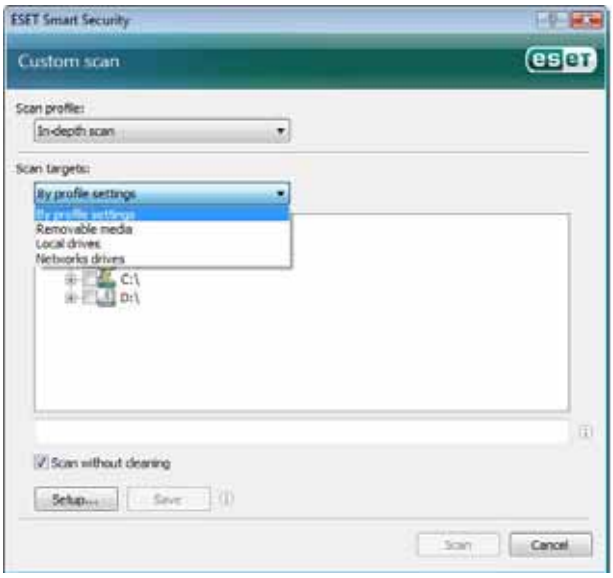
### ۲-۴-۱-۴- آیتم‌های مورد نظر جهت پویش

با استفاده از منوی بازشونده "scan targets" می‌توان فایلها، پوشه‌ها و درایوهای مورد نظرجهت پویش را برگزید. همچنین با استفاده از گزینه منوی انتخاب سریع آیتم‌های مورد نظر جهت پویش می‌توان هر یک از موارد زیر را انتخاب کرد.

الف) "local drives" : برای کنترل تمامی فضاهای دیسک سخت

ب) "removable media" : برای کنترل دیسکت‌ها ، حافظه‌های قابل حمل دارای پورت "USB"، سی‌دی‌ها و دی وی دی‌ها

ج) "network drives" : جهت کنترل تمامی درایوهای شبکه‌ای (mapped drives)




نکته آخر اینکه می‌توان یک فایل یا پوشه خاص را با درج مسیر دقیق آن برای پویش مشخص نمود.

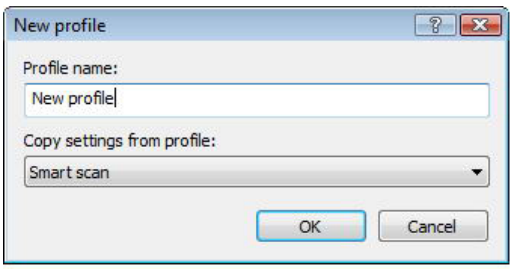
### ۳-۴-۱-۴- پروفایلهای پویش

کاربر می‌تواند پارامترهای تعیین شده جهت پویش رایانه را در پروفایلها ذخیره‌سازی کند. مزیت ایجاد پروفایلهای پویش نیز عبارت از امکان استفاده بعدی از آنها جهت پویش رایانه است.

توصیه شرکت "ESET" این است که کاربران از قبل تعداد متنوعی پروفایل با پارامترها و جزئیات متفاوت برای استفاده‌های آتی خود ایجاد نمایند.

لذا به منظور ایجاد یک پروفایل جهت انجام پویش‌های آتی کافی است کلید "F5" را فشرده تا پنجره تنظیمات پیشرفته گشوده شود. پس از آن به قسمت "on–demand computer scan" رفته و بر روی گزینه "profiles" کلیک کنید تا فهرستی از پروفایلهای پویش و گزینه ایجاد پروفایلهای جدید به نمایش درآید. در مبحث بعدی به توضیحات مرتبط با تنظیمات مربوط به پارامترهای موتور "ThreatSense" جهت انجام تنظیمات پویش رایانه پرداخته شده است. با استفاده از این پارامترها قادر خواهید بود تا پروفایلی ایجاد نمائید که همه نیازهای شما را برآورده سازد.

مثال: تصور کنید که قصد دارید یک پروفایل جدید پویش ایجاد کنید و پروفایل از پیش ایجاد شده "smart scan" تا حدود نسبتا مناسبی با شرائط مورد نظر شما تطابق دارد. لیکن شما قصد ندارید "runtime packer" ها و برنامه‌های کاربردی به صورت بالقوه ناامن را مورد پویش قرار داده و همچنین می‌خواهید از سطح پاکسازی "strict cleaning" استفاده به عمل آورید. بدین منظور کافی است در پنجره "configuration profiles" بر روی دکمه "add..." کلیک کرده و نام پروفایل مورد نظر را در فیلد "profile name" درج نمائید و سپس از منوی بازشونده "copy settings from profile" پروفایل "smart scan" را برگزیده و پس از آن دیگر تنظیمات منطبق با نیاز خود را به انجام رسانید.




### ۵-۱-۴- تنظیمات مربوط به پارامترهای موتور "ThreatSense"

"ThreatSense" مجموعه‌ای از روش‌های شناسایی تهدیدات رایانه‌ای تشکیل یافته است. این فناوری از نوع حفاظت پیش‌گیرانه است. به بیان دیگر با استفاده از این فناوری در ساعات اولیه شیوع یک تهدید رایانه‌ای نیز کاربران دارای نوعی حفاظت پیش‌گیرانه (با استفاده از ابزار هوش مصنوعی) خواهند بود.

همانطور که عنوان گردید در این فناوری از روشهای متعددی نظیر روش بررسی کدها، نمونه‌سازی کدها، شناسه‌های "generic" یا نوعی و همچنین بانک اطلاعاتی شناسه ویروسهای رایانه‌ای استفاده به عمل آمده است تا بتوان با استفاده از این روشها در کنار یکدیگر به یک سطح حفاظت رایانه‌ای بالا دست یافت. ضمن اینکه موتور این فناوری قادر است به طور همزمان چندین رشته از اطلاعات را کنترل نماید و این موضوع باعث افزایش نرخ آشکارسازی تهدیدات رایانه‌ای و تاثیرگذاری می‌گردد. نکته دیگر اینکه می‌توان از فناوری"ThreatSense" جهت مقابله با "rootkit"ها نیز بهره جست.

کاربران با استفاده از گزینه‌های مربوط به تنظیمات فناوری "ThreatSense" قادرند پارامترهای پویش متعددی را مشخص نمایند. این موارد عبارتند از:

الف) انواع فایلها و پسوندهای فایل جهت پویش آنها

ب) ترکیبی از روشهای آشکارسازی متعدد

ج) سطوح پاکسازی و ...

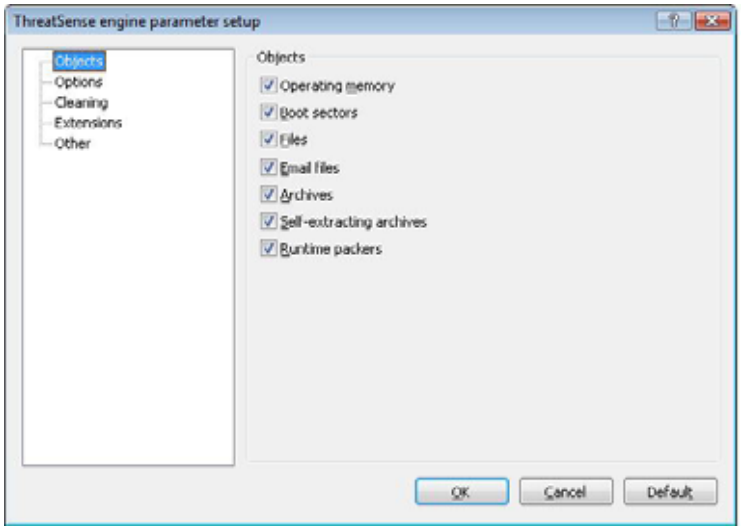
به منظور ورود به پنجره تنظیمات این فناوری کافی است بر روی دکمه "setup..." موجود در پنجره تنظیمات هر یک از ماژولهای نرم افزار که از فناوری "ThreatSense" استفاده می‌کنند، کلیک کنید. لازم به توضیح است که سناریوهای امنیتی متفاوت نیاز به پیکربندی‌های متفاوت دارند. با در نظر داشتن این مورد می‌توان "ThreatSense" را به طور جداگانه برای هر یک از ماژولهای ذیل پیکربندی نمود:

- ماژول حفاظت "real-time"
- ماژول کنترل فایلها در شروع کار رایانه (system startup)
- ماژول حفاظت از نامه‌های الکترونیک
- ماژول حفاظتی مربوط به دسترسی به اینترنت
- ماژول مربوط به پویش دستی رایانه

پارامترهای "ThreatSense" برای هر یک از ماژولها به شکل بسیار خوبی بهینه گردیده‌اند و تغییر و اصلاح هر یک از آنها تاثیر قابل توجهی بر روی عملکرد سیستم خواهد داشت. به عنوان مثال، تغییر پارامترها به منظور پویش همیشگی "runtime packer" ها و یا فعال ساختن ویژگی استفاده از هوش مصنوعی پیشرفته (advanced heuristics) در ماژول حفاظت "real–time" از فایل سیستم‌ها باعث کاهش سرعت سیستم می‌گردد. چرا که در حالت عادی، صرفا فایلهایی که اخیرا ایجاد گردیده اند، با استفاده از این متدها پویش می‌شوند (نه همه فایلهای رایانه‌ای). بنابراین توصیه می‌گردد که از پارامترهای "ThreatSense" به صورت پیش فرض برای تمامی ماژولها مگر ماژول پویش رایانه استفاده کنید.

### ۱-۵-۱-۴- تنظیمات مربوط به آیتم‌های مورد نظر جهت پویش

با استفاده از قسمت "objects" این امکان برای کاربران فراهم می‌آید تا بتوانند اجزا و فایلهای متعددی را جهت پویش انتخاب نمایند.




این اجزا و گزینه‌ها عبارتند از:

الف) حافظه اصلی (operating memory): در زمان انتخاب این گزینه حافظه در حال کارکرد (منظور RAM است) سیستم مورد پویش قرار می‌گیرد.

ب) سکتورهای راه‌اندازی: با انتخاب این گزینه سکتورهای راه‌اندازی به لحاظ وجود آلودگی در رکورد راه‌اندازی اصلی (master boot record) مورد پویش قرار می‌گیرند.

ج) فایلها: جهت پویش انواع فایلهای رایج نظیر برنامه‌ها، تصاویر، فایلهای صوتی، فایلهای ویدئویی، فایلهای بانک اطلاعاتی و ... لازم است این گزینه تیک خورده باشد.

د) فایلهای موجود در نامه‌های الکترونیک: جهت پویش فایلهای موجود در نامه‌های الکترونیک از این گزینه استفاده می‌گردد.

هـ) فایلهای آرشیو شده (فشرده شده): لازم است این گزینه جهت پویش انواع فایلهای آرشیو شده نظیر فایلهای ".rar" ، ".zip" ، ".tar" و ... فعال گردد.

و) فایلهای آرشیو شده خود اجرا: جهت پویش فایلهای آرشیو شده دارای پسوند ".exe" نیز از این گزینه استفاده می‌شود.

ز) "runtime packer" ها: جهت پویش "runtime packer" ها لازم است این گزینه انتخاب گردد.

### ۲-۵-۱-۴- گزینه‌ها

کاربر می‌تواند در قسمت "options" روش‌های مورد نظر جهت پویش سیستم را انتخاب نماید. گزینه‌های موجود عبارتند از:

الف) بانک اطلاعاتی شناسه ویروسها:

جهت پویش تهدیدات رایانه‌ای با استفاده از بانک اطلاعاتی شناسه ویروسهای رایانه‌ای از این گزینه استفاده می گردد.

ب) هوش مصنوعی:

"Heuristics" یا ابزار هوش مصنوعی الگوریتمی است که عملکردهای فرایندهای مشکوک به آلودگی و مخرب را مورد پویش قرار می‌دهد. مزیت اصلی استفاده از این ابزار این است که به کمک آن تهدیدات رایانه‌ای جدید که قبلا موجود نبوده‌اند و یا شناسه آنها در بانک اطلاعاتی شناسه ویروسهای رایانه‌ای نرم افزار ضدویروس موجود نیست مورد شناسایی قرار می‌گیرد.

ج) هوش مصنوعی پیشرفته:

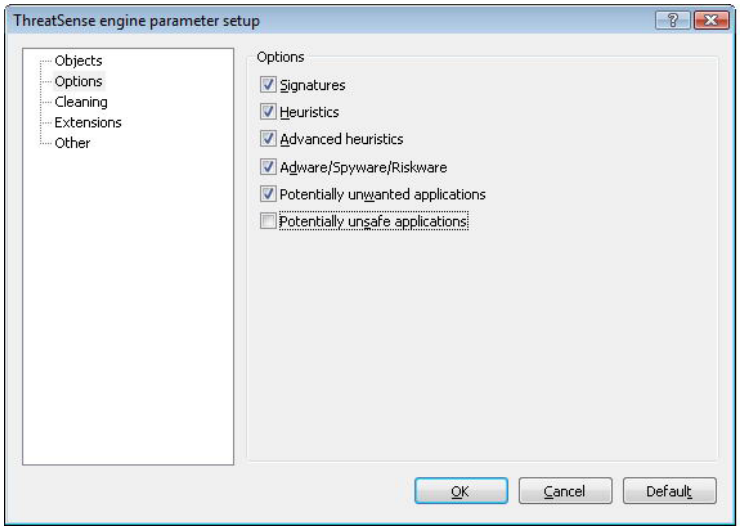
ابزار هوش مصنوعی پیشرفته از الگوریتم منحصر به فرد و بهینه شده شرکت "ESET" جهت آشکارسازی کرم‌های رایانه‌ای و اسبهای تروا که با استفاده از زبانهای برنامه‌نویسی سطح بالا نوشته شده‌اند، تشکیل یافته است. بر اساس هوش مصنوعی پیشرفته، قابلیت شناسایی تهدیدات ناشناخته جدید در نرم افزار بسیار بالا است.

د) جاسوس افزارها، "riskware" ها و "adware" ها:

جاسوس افزارها، "riskware" ها و "adware" ها ازجمله کدهایی هستند که می‌توان با استفاده از آنها اطلاعات محرمانه و حساس یک کاربر را سرقت نمود. لذا جهت پویش رایانه به جهت وجود این نوع کدهای مخرب لازم است این گزینه تیک بخورد. ضمن اینکه

کدهایی که موجب نمایش تصاویر تبلیغاتی در رایانه کاربرمی‌شوند نیز جزء همین دسته از تهدیدات به شمار رفته و با انتخاب گزینه مورد بحث، رایانه به لحاظ وجود این نوع کدها نیز پویش می‌شود.

هـ) برنامه‌هایی که به صورت بالقوه ناامن هستند:

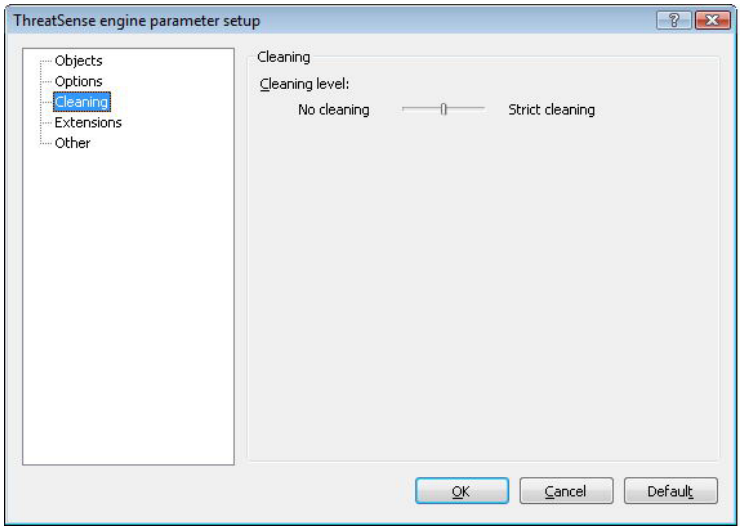



منظور از نرم افزارهای به صورت بالقوه ناامن عبارت از نرم افزارهایی است که جزء کدهای مخرب محسوب نمی‌شوند ولی وجود آنها می‌تواند ناامن باشد. به عنوان مثال می‌توان به نرم افزارهای دسترسی از راه دور اشاره کرد. لذا این گزینه به صورت پیش فرض انتخاب نگردیده است تا کاربر خود نسبت به انتخاب یا عدم انتخاب آن تصمیم بگیرد.

و) برنامه‌هایی که به صورت بالقوه ناخواسته هستند:

این برنامه‌ها نیز اگرچه لزوما از جمله کدهای مخرب محسوب نمی‌شوند، ولی می‌توانند اثرات نامطلوبی بر روی کارایی رایانه داشته باشند. این نرم افزارها به خودی خود نصب نمی‌شوند و معمولا کاربر آنها را نصب می‌کند. از جمله اثرات نامطلوب این برنامه‌ها می‌توان به گشوده شدن پنجره‌های "pop–up" متعدد، فعال شدن و اجرای فرایندهای مخفی، افزایش چشمگیر استفاده از منابع رایانه، تغییر در نتایج کاوشها و ارتباط با سرورهای راه دور (بصورت نامحسوس) اشاره کرد.

### ۳-۵-۱-۴- پاکسازی فایلهای آلوده




تنظیمات مربوط به پاکسازی فایلهای آلوده تعیین کننده رفتار پویشگر در زمان پاکسازی فایلهای دارای آلودگی ویروسی است. در "ESS" سه سطح پاکسازی وجود دارد.

الف) حالت "no cleaning":

در زمان انتخاب این حالت فایلهای آلوده به صورت خودکار پاکسازی نمی‌گردند و نرم افزار طی پنجره‌ای از کاربر نسبت به روش مقابله با تهدید شناسایی شده سوال می‌نماید.

ب) حالت پیش فرض (default level):

در این حالت نرم افزار به صورت خودکار مبادرت به پاکسازی فایل آلوده و یا پاک کردن آن می‌نماید. همچنین اگر امکان انجام مقابله با تهدید آشکار شده به صورت خودکار برای نرم افزار فراهم نباشد، نرم افزار روشهای تکمیلی دیگری را به کاربر پیشنهاد می‌دهد. این

روشهای تکمیلی در صورت عدم کارکرد روش پیش فرض تعیین شده جهت مقابله با آلودگی ویروسی شناسایی شده از طریق نرم افزار طی پنجره‌ای به کاربر پیشنهاد می‌گردند.

ج) حالت "strict cleaning":

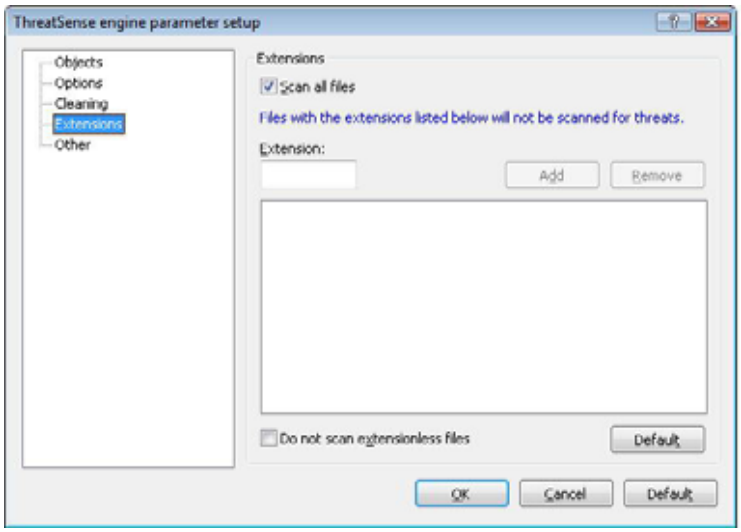
در این حالت نرم افزار به صورت خودکار مبادرت به پاکسازی و یا پاک کردن آیتم آلوده – حتی فایلهای آرشیو شده – می‌نماید. تنها استثنا در این حالت فایلهای سیستمی آلوده هستند. در این حالت اگر فایل سیستمی آلوده قابل پاکسازی نباشد، نرم افزار طی پنجره‌ای گزینه‌های مقابله ای دیگری را به کاربر پیشنهاد می‌دهد.

*هشدار:*

*در مد یا حالت پیش فرض، فایل‌های آرشیو شده آلوده صرفا زمانی پاک می‌شوند که تمامی فایلهای موجود در آنها آلوده باشند. اگر آرشیو آلوده دارای فایل‌های غیر آلوده بوده و به عنوان مثال از ۱۰ فایل موجود در آن ۲ مورد دارای آلودگی ویروسی باشند، فایل آرشیو به صورت خودکار پاک نخواهد شد. اما اگر همین فایل آرشیو حاوی ۱۰ فایل در زمان فعال بودن حالت "strict cleaning" شناسایی گردد، اگر قابل پاکسازی نباشد به صورت خودکار پاک خواهد شد.*

### ۴-۵-۱-۴- پسوندها

همانطور که می‌دانید هر فایل رایانه‌ای دارای یک پسوند خاص است که این پسوند بیانگر نوع و محتوای آن فایل می‌باشد. این قسمت از تنظیمات مربوط به پارامترهای "ThreatSense" کاربر را قادر می‌سازد تا بتواند انواع فایلهای مختلف را جهت پویش مشخص نماید.




به صورت پیش فرض، تمامی فایلها صرف نظر از پسوندشان مورد پویش قرار می‌گیرند. همچنین در فهرست مشخص شده در شکل اخیر می‌توان با افزودن هر پسوند دلخواهی، آن پسوند را از فهرست پسوندهایی که مورد پویش قرار می‌گیرند حذف نمود. همچنین اگر گزینه "scan all files" تیک نخورده باشد، پسوندهای موجود در فهرست زیر آن تبدیل به گزینه هایی می‌شوند که توسط نرم افزار

مورد پویش قرار خواهند گرفت. به بیان دیگر کاربر با استفاده از دکمه‌های "add" و "remove" موجود در این پنجره می‌تواند پسوندهای مورد نظر خود جهت پویش و یا عدم پویش را مشخص کند.

اگر پویش برخی از انواع فایلها باعث شود که نرم افزار مربوط به آنها نتواند به طور صحیح وظیفه خود را انجام دهد، می‌توان آن نوع فایلها (پسوند فایلها) را در فهرست " حذف از پویش" اضافه نمود. به عنوان مثال اگر از نرم افزار "MS exchange server" بر روی رایانه استفاده می‌شود، بهتر است که فایلهای دارای پسوندهای ".edb" ، ".eml" و ".tmp" را در فهرست "حذف از پویش" اضافه نمائید.

### ۶-۱-۴- اقدامات لازم در زمان شناسایی یک تهدید رایانه‌ای

تهدیدات رایانه ای از طرق مختلف نظیر صفحات اینترنتی، پوشه‌های به اشتراک گذاشته شده، نامه‌های الکترونیک و حافظه‌های قابل حمل اعم از دیسکتها، سی‌دی‌ها، حافظه‌های دارای پورت "USB" و ... می‌توانند رایانه را آلوده نمایند.

اگر رایانه علائمی از آلودگی نظیر کند شدن سرعت سیستم و یا هنگ کردن‌های مداوم را نشان می‌دهد، بهتر است مراحل ذیل توسط کاربر انجام شود:

الف) نرم افزار "ESS" را اجرا کرده و بر روی گزینه "computer scan" کلیک نماید.

ب) بر روی گزینه "standard scan" کلیک کند.

ج) پس از پایان فرایند پویش، فایل ثبت رخدادها را مشاهده کرده و از تعداد فایلهای پویش شده، تعداد فایلهای آلوده و همچنین تعداد فایلهای پاکسازی شده اطلاع حاصل نماید.

همچنین اگر کاربر قصد دارد صرفا آیتم خاصی را پویش کند، می‌تواند بر روی گزینه "custom scan" کلیک کرده و آیتم‌های مورد نظر جهت پویش را برگزیند.

به عنوان یک مثال از چگونگی عملکرد "ESS" در زمان شناسایی یک تهدید رایانه ای تصور کنید که پویشگر خودکار فایل‌های سیستمی "real–time" یک آلودگی ویروسی را شناسایی می‌کند و حال آنکه سطح پاکسازی نرم افزار "ESS" بر روی سطح پیش فرض (default cleaning level) قرار دارد.


در این زمان "ESS" مبادرت به پاکسازی و یا پاک نمودن فایل آلوده به صورت خودکار می‌نماید. همچنین اگر هیچ روش از پیش تعیین شده‌ای برای ماژول حفاظت "real–time" تعریف نشده باشد، "ESS" طی پنجره‌ای از کاربر جهت اتخاذ تصمیم مبنی بر چگونگی مقابله با تهدید شناسایی شده سوال خواهد کرد. معمولا گزینه‌های مقابله‌ای پیشنهاد شده عبارت از "clean" ، "delete" و "leave" هستند.

توصیه می‌شود از گزینه "leave" استفاده نشود، چرا که با انتخاب این گزینه فایل آلوده دست نخورده باقی می‌ماند. تنها استثنا در انتخاب گزینه "leave" زمانی است که کاربر مطمئن است که فایل شناسایی شده به عنوان تهدید رایانه‌ای بی خطر بوده و اشتباها شناسایی گردیده است.

از گزینه "clean" نیز زمانی استفاده می‌گردد که قصد دارید فایل آلوده را به لحاظ وجود آلودگی ویروسی پاکسازی نمائید. با انتخاب این گزینه فایل آلوده پاکسازی می‌شود و اگر آلودگی به گونه‌ای باشد که تمامی فایل آلوده شده باشد، در نهایت فایل آلوده پاک خواهد شد.

نکته دیگر اینکه اگر فایل آلوده قفل باشد (locked) و یا از آن توسط فرایندهای سیستمی استفاده به عمل می‌آید، معمولا پس از آزاد شدن از فرایند سیستمی (در اکثر مواقع منظور زمانی است که رایانه راه‌اندازی مجدد می‌شود) پاک خواهد شد.

همچنین در مد یا حالت پیش فرض، فایل‌های آرشیو شده آلوده صرفا زمانی پاک می‌شوند که تمامی فایلهای موجود در آنها آلوده باشند. اگر آرشیو آلوده دارای فایل‌های غیر آلوده بوده و به عنوان مثال از ۱۰ فایل موجود در آن ۲ مورد دارای آلودگی ویروسی باشند، فایل آرشیو به صورت خودکار پاک نخواهد شد. اما اگر همین فایل آرشیو حاوی ۱۰ فایل در زمان فعال بودن حالت "strict cleaning" شناسایی گردد، اگر قابل پاکسازی نباشد به صورت خودکار پاک خواهد شد.

### ۴-۲- دیواره آتش شخصی

دیواره آتش شخصی تمامی ترافیک ورودی و خروجی رایانه را مورد کنترل قرار می‌دهد. کنترل هر یک از ارتباطات شبکه‌ای بر اساس قوانین فیلترسازی تعیین شده انجام می‌پذیرد تا رایانه از حملات رایانه‌های راه دور حفاظت شده و سرویس‌های تهدید آمیز بلوکه گردند. همچنین این ماژول کنترلی موجب حفاظت ضدویروس پروتکل‌های "HTTP" و "POP3" نیز می‌شود. لذا پر واضح است که یکی از المانهای اصلی و مهم در زمینه حفاظت رایانه‌ای وجود دیواره آتش شخصی است.

#### ۴-۲-۱- مدهای فیلترسازی

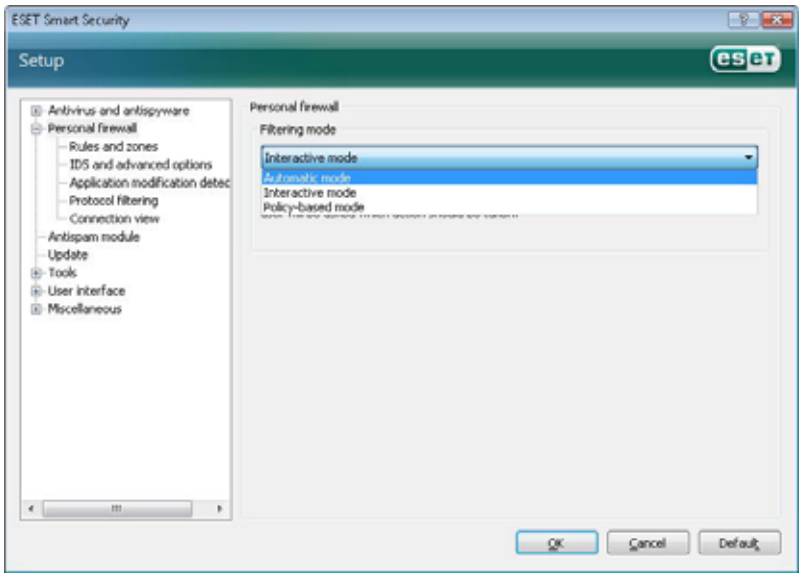
دیواره آتش شخصی "ESS" دارای ۳ مد فیلترسازی است و رفتار این دیواره آتش بر اساس هر یک از این مدها متفاوت است. همچنین انتخاب هر یک از این مدها تاثیر مستقیمی بر سطح تعاملی کاربر رایانه دارد.

این ۳ مد فیلترسازی عبارتند از:

الف) مد فیلترسازی خودکار که حالت پیش فرض است. این حالت مناسب کاربرانی است که ترجیح می‌دهند با استفاده از روشی ساده و راحت از دیواره آتش استفاده کرده و تمایلی به تعریف قوانین ندارند. در این مد فیلترسازی عبور ترافیک خروجی مجاز بوده و تمامی ارتباطات جدید از سمت شبکه بلوکه می‌گردند.

ب) مد فیلترسازی تعاملی به کاربر امکان می‌دهد تا بهترین پیکربندی را جهت استفاده از دیواره آتش شخصی به انجام رساند.

زمانی که یک ارتباط رایانه‌ای جدید و فاقد قانونی جهت کنترل آن شناسایی می‌گردد، یک پنجره محاوره‌ای حاوی اطلاعاتی در مورد ارتباط ایجاد شده جدید گشوده می‌شود که حاوی گزینه‌هایی جهت عبور و یا بلوکه کردن ترافیک مورد بحث می‌باشد. ضمن اینکه هر گزینه که کاربر در این لحظه انتخاب می‌کند (عبور و یا بلوکه کردن ترافیک مربوط به اتصال جدید) توسط دیواره آتش شخصی می تواند به عنوان یک قانون به خاطر سپرده می‌شود. به بیان دیگر اگر در همین حین کاربر گزینه ایجاد یک قانون جدید را بر گزیند، با تمامی ارتباطات بعدی از نوع ارتباط شناسایی شده جدید بر اساس قانون تعریف شده برخورد خواهد شد.




ج) در حالت مبتنی بر سیاست (policy–based) نیز تمامی ارتباطاتی که فاقد قانونی برای عبور هستند، بلوکه می‌گردند. کاربران حرفه‌ای با استفاده از این مد می‌توانند قوانینی تبیین کنند تا صرفا ترافیک مورد نظر آنها بر اساس آن قوانین عبور داده شود و دیگر ارتباطات نامعلوم توسط دیواره آتش شخصی بلوکه گردند.

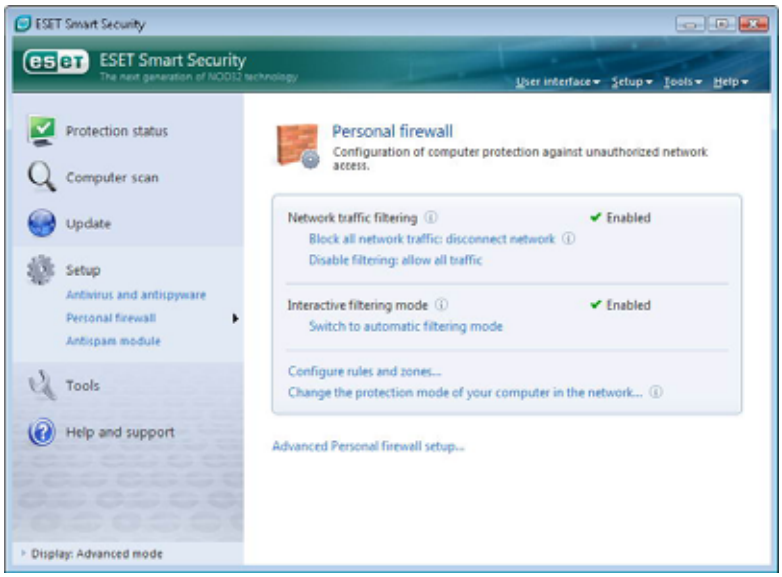
### ۲-۲-۴- بلوکه شدن تمامی ترافیک: قطع شبکه

تنها گزینه‌ای که تمامی ترافیک شبکه را بلوکه می‌کند عبارت از گزینه

"block all network traffic:disconnect network"

است. در این حالت تمامی ترافیک ورودی و خروجی به صورت خودکار و بدون نمایش پنجره هشدار توسط دیواره آتش شخصی بلوکه می‌گردد.

این گزینه را صرفا زمانی لازم است انتخاب کنید که نسبت به مسائل امنیتی شبکه مشکوک هستید و ممکن است رایانه شما از جانب چنین شبکه‌ای تهدید شود.




### ۳-۲-۴- غیر فعال کردن فیلترسازی: عبور تمامی ترافیک

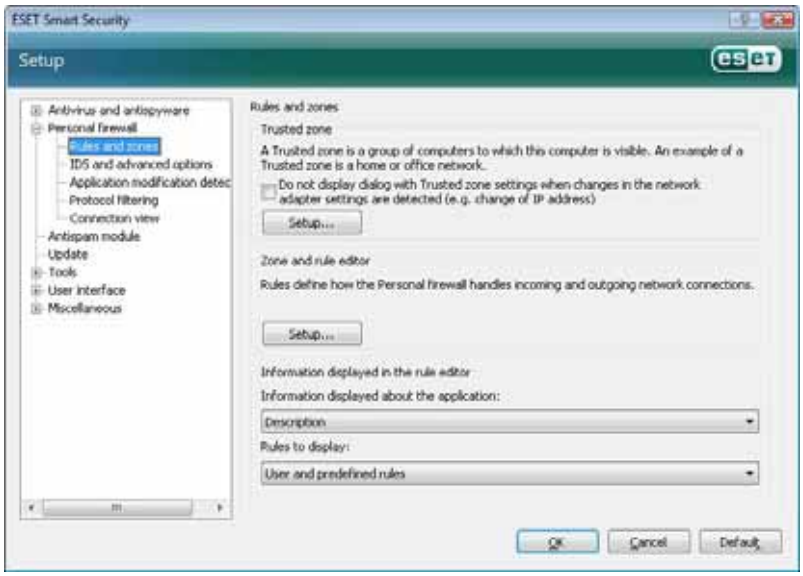
این گزینه دقیقا متضاد گزینه‌ای است که در بند ۲-۲-۴ مورد بررسی قرار گرفت. به بیان دیگر با انتخاب این گزینه تمامی تنظیمات فیلترسازی توسط دیواره آتش شخصی غیر فعال شده و تمامی ترافیک ورودی و خروجی عبور داده خواهد شد. در واقع زمانی که شبکه دارای امنیت کامل باشد، نیازی به وجود دیواره آتش وجود ندارد.

### ۴-۲-۴- پیکربندی و استفاده از قوانین

قوانین نمایانگر مجموعه‌ای از شرائط هستند که با استفاده از آنها تمامی ارتباطات شبکه‌ای کنترل شده و عکس العمل‌های از پیش تعریف شده در مقابل این ارتباطات انجام می‌پذیرد. در دیواره آتش شخصی "ESS" کاربر می‌تواند مشخص کند که چه عکس العملی در مقابل برقراری ارتباطی که توسط یک قانون مشخص شده است به انجام رسد.

به منظور دسترسی به تنظیمات مربوط به قوانین فیلترسازی کافی است با استفاده از دکمه "F5" پنجره "advanced setup" را گشوده و از نمودار درختی سمت چپ آن گزینه "personal firewall" را برگزینید و پس از آن زیر منوی "rules and zones" را برگزینید. سپس به جهت نمایش پیکربندی جاری کافی است که گزینه "setup..." موجود در قسمت "zone and rule editor" را کلیک کنید.

توجه داشته باشید که اگر دیواره آتش شخصی در حالت فیلترسازی خودکار (automatic filtering mode) قرار داشته باشید، به قسمت "zone and rule editor" دسترسی نخواهید داشت.



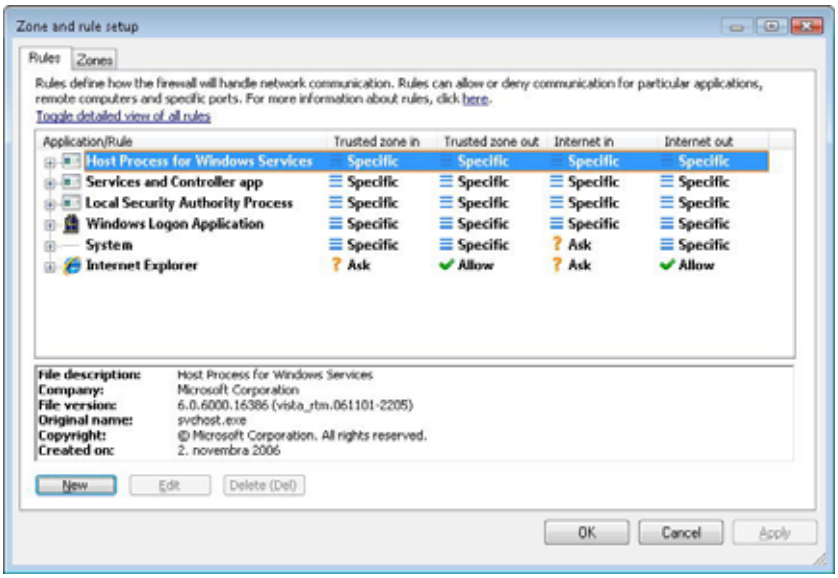

سپس در پنجره "zone and rule setup" می‌توانید یک نگاه کلی به قوانین و ناحیه‌ها (بر اساس برگ نشان انتخاب شده) داشته باشید. پنجره مورد بحث به دو قسمت تقسیم شده است. در قسمت بالایی می‌توانید یک نگاه اجمالی به قوانین داشته باشید. در قسمت پائین نیز جزئیات کامل مربوط به قانون انتخاب شده در قسمت بالایی نمایش داده می‌شود. در قسمت پائین پنجره نیز دکمه‌های "new"، "edit" و "delete" جهت ایجاد، ویرایش و یا حذف یک قانون در اختیار کاربر قرار گرفته اند.

با در نظر گرفتن جهت حرکت ترافیک شبکه‌ای می‌توان گفت که دارای دو نوع ترافیک ورودی و خروجی هستیم. ترافیک ورودی از سمت رایانه راه دور است که قصد دارد ارتباطی را با رایانه کاربر برقرار نماید. ترافیک خروجی عکس ترافیک ورودی است. به بیان دیگر ارتباط از رایانه کاربر به سمت رایانه راه دور برقرار می‌گردد.

همچنین اگر یک ارتباط نامعلوم توسط دیواره آتش شخصی شناسایی گردد، لازم است کاربر نسبت به عبور و یا بلوکه نمودن آن اتخاذ تصمیم نماید. ارتباطات ناامن، ناخواسته و یا ارتباطاتی که به طور کامل نامعلوم هستند جزء مواردی به حساب می‌آیند که می‌توانند برای رایانه کاربر نوعی خطر امنیتی تلقی شوند. بنابراین اگر چنین ارتباطاتی برقرار شود، توصیه می‌شود به رایانه راه دور و همچنین نرم افزاری که از رایانه راه دور قصد اتصال به رایانه کاربر را دارد توجه ویژه‌ای معطوف گردد. چرا که بسیاری از تهدیدات رایانه‌ای پس از دسترسی و جمع‌آوری اطلاعات محرمانه کاربران مبادرت به ارسال آنها برای افراد غیرمجاز نموده و یا سبب می‌شوند کدهای مخرب دیگری در ایستگاه‌های کاری کاربران بارگذاری گردند. با استفاده از دیواره آتش شخصی "ESS" کاربران قادر به شناسایی و متوقف نمودن چنین ارتباطی خواهند بود.

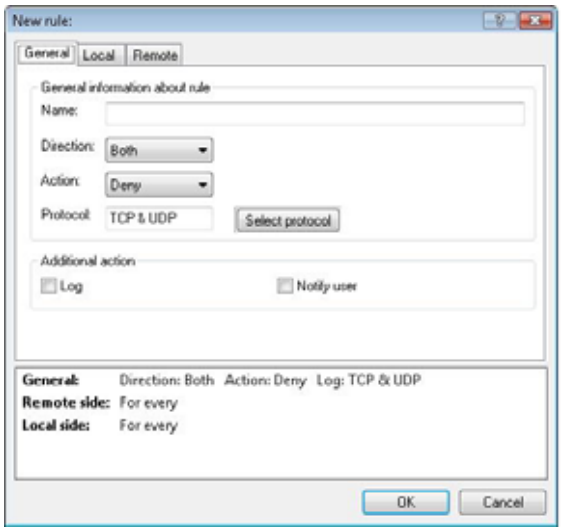
### ۱-۴-۲-۴- ایجاد قوانین جدید

زمانی که یک برنامه کاربردی جدید نصب می‌کنید که هدف از آن دسترسی به منابع شبکه‌ای است و یا در زمان تغییر و اصلاح یک ارتباط موجود (به عنوان مثال رایانه راه دور، شماره پورت ارتباطی و ...) لازم است یک قانون جدید تعریف نمائید.




به منظور ایجاد یک قانون جدید اطمینان حاصل کنید که برگ نشان "rules" انتخاب گردیده است. پس از آن بر روی دکمه "new" موجود در پنجره "zone and rule setup" کلیک کنید تا یک پنجره محاوره‌ای جدید جهت تعیین پارامترهای قانون جدید گشوده شود. در قسمت بالایی پنجره اخیر ۳ برگ نشان وجود دارد.

- ✓ برگ نشان "general": در این قسمت می‌توان نام قانون، جهت حرکت ترافیک، عکس العمل مناسب و پروتکل‌های مورد نظر را مشخص نمود. در اینجا منظور از عکس العمل عبور ترافیک و یا بلوکه کردن آن است.
- ✓ برگ نشان "local": در این قسمت اطلاعات مربوط به سمت رایانه محلی (رایانه کاربر) از قبیل شماره پورت محلی و یا بازه پورت‌های ارتباطاتی و همچنین نام برنامه کاربردی برقرار کننده ارتباط قابل مشاهده است.
- ✓ برگ نشان "remote": این قسمت نیز حاوی اطلاعاتی در مورد پورت راه دور و یا بازه پورتهای ارتباطی راه دور است. همچنین در این قسمت امکانی فراهم آمده است تا کاربر بتواند فهرستی از آدرس‌های "IP" راه دور و یا ناحیه‌های مورد نظر مرتبط با قانون جدید را تعیین کند.



یک مثال خوب در مورد ایجاد یک قانون جدید عبارت از دسترسی برنامه مرورگر وب "internet explorer" به شبکه است. در این حالت مراحل ذیل انجام می‌شود.

۱- در برگ نشان "general" ترافیک خروجی از طریق پروتکل "TCP & UDP" را فعال نمائید.

۲- در برگ نشان "local"پروسه‌ای که مبین نرم افزار مرورگر وب است را اضافه کنید. پروسه مربوط به نرم افزار "internet explorer" عبارت از "iexplorer.exe" می‌باشد.

۳- در برگ نشان "remote" و در صورتی که صرفا تمایل به مجاز نمودن سرویس‌های استاندارد شبکه جهانی اینترنت دارید، پورت ۸۰ را فعال کنید.

### ۴-۲-۴-۲- ویرایش قوانین

به منظور ویرایش یک قانون موجود کافی است بر روی دکمه "edit" کلیک کنید. با این کار قادر خواهید بود تمامی پارامترهای ذکر شده در مبحث ۴-۲-۴-۱ را مورد ویرایش قرار دهید.

تغییر و اصلاح قانون در هر زمانی که پارامترهای کنترل شده تغییر می‌کنند، لازم و ضروری است. چرا که اگر این اصلاح انجام نشود، قانون در شناسایی شرائط ناتوان مانده و عکس العمل مناسبی را در مورد ترافیک مورد نظر نشان نخواهد داد و در آخر اشکالاتی در ارتباطات سیستم کاری نرم افزار کاربردی رخ خواهد داد.

به عنوان یک مثال در این زمینه می‌توان به تغییرات آدرس‌ها و شماره پورتهای رایانه‌های راه دور اشاره کرد. اگر این تغییرات در قوانین رایانه کاربر اصلاح نگردند، مشکلات عدیده‌ای رخ خواهد داد.

### ۴-۲-۵- پیکربندی ناحیه‌ها

یک ناحیه (zone) نمایانگر مجموعه‌ای از آدرس‌های شبکه‌ای است که یک گروه منطقی را تشکیل داده‌اند. در یک ناحیه برای تمامی آدرس‌ها همان قوانینی که برای مجموعه آنها در قالب ناحیه تعریف گردیده است اجرا می‌گردد. یکی از مثالها در مورد یک ناحیه عبارت از ناحیه قابل اعتماد یا "trusted zone" است. این ناحیه مبین گروهی از آدرسهایی (آدرسهای شبکه‌ای) است که کاربر به آنها اطمینان داشته و ترافیک مربوط به آنها به هیچ وجه از طرف دیواره آتش شخصی بلوکه نمی‌گردد.

ناحیه‌ها را می‌توان با کلیک بر روی برگ نشان "zones" موجود در پنجره "zone and rule setup" پیکربندی کرد. ضمن اینکه با کلیک بر روی دکمه "new" نیز می‌توان یک ناحیه جدید تعریف نمود. جهت این کار کافی است پس از کلیک بر روی دکمه "new" یک نام به ناحیه جدید اطلاق نموده و آدرسهای مورد نظر شبکه‌ای را در پنجره باز شده درج کنید.

### ۴-۲-۶- ایجاد یک ارتباط- آشکارسازی

دیواره آتش شخصی "ESS" هر ارتباط شبکه‌ای جدیدی را شناسایی می‌کند. همچنین با استفاده از مد فعال دیواره آتش (حالت خودکار، تعاملی و حالت مبتنی بر سیاست) عکس العمل مناسب برای قانون جدید اتخاذ می‌گردد. به بیان دیگر اگر هر یک از دو حالت خودکار و یا "policy–based" فعال گردیده باشد، دیواره آتش شخصی بدون دخالت کاربر مبادرت به انجام عکس العمل از پیش

تعریف شده می‌نماید. در حالتی نیز که حالت تعاملی فعال باشد، یک پنجره آگاهی رسانی گشوده شده و شناسایی یک ارتباط شبکه‌ای جدید را به همراه جزئیات مربوط به آن به اطلاع کاربر می‌رساند. در این زمان است که کاربر در مورد عبور و یا بلوکه کردن این ارتباط تصمیم‌گیری لازم را به عمل می آورد.


بنابراین اگر همواره تصمیم کاربر در مورد یک نوع ارتباط خاص مبنی بر عبور و مجاز بودن آن ارتباط است، توصیه می‌شود برای آن ارتباط خاص یک قانون جدید تعریف شود. بدین منظور کافی است گزینه "remember action (create rule)" را تیک زده و عکس العمل "ESS" در رابطه با ارتباط مورد نظر را در قالب یک قانون جدید برای دیواره آتش شخصی ذخیره سازی نمائید. در نتیجه اگر دیواره آتش شخصی مجددا ارتباط خاص مورد نظر را شناسایی کند، طبق قانون مشخص شده عکس العمل مناسبی از خود نشان خواهد داد.

لازم است کاربران در زمان ایجاد قوانین جدید دقت نظر کافی مبذول داشته و صرفا در قوانین جدید ارتباطات امن و معتبر را مجاز به عبور نمایند. اگر تمامی ارتباطات اعم از معتبر و غیر معتبر مجاز به عبور از دیواره آتش شخصی باشند، دیواره آتش شخصی معنی خود را از دست می‌دهد. لذا پارامترهای مهم در رابطه با ارتباطات به قرار زیر هستند:

۱- سمت راه دور (remote side)

صرفا ارتباطات با آدرس‌های معلوم و امن را مجاز شمارید

۲- نرم افزار کاربردی محلی (local application)

بهتر است از ایجاد ارتباط توسط نرم افزارها و فرایندهای موجود در رایانه محلی که آنها را نمی‌شناسید جلوگیری به عمل آورید.

۳- شماره پورتها (port number)

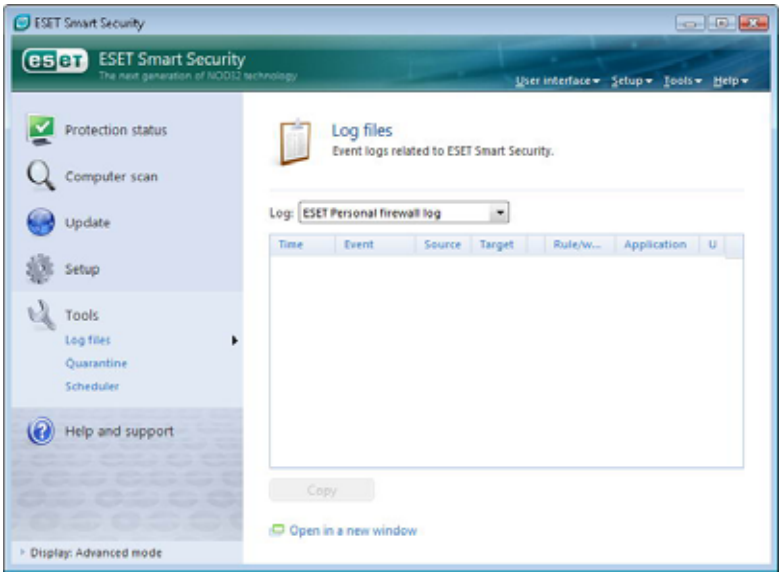
در نظر داشته باشید که ارتباطات برقرار شده توسط پورتهای رایج معمولا ایمن هستند. از این پورتها می‌توان به پورت ۸۰ جهت ارتباطات اینترنتی اشاره کرد.

تهدیدات رایانه‌ای معمولا به جهت گسترش از بستر اینترنت و ارتباطات مخفی استفاده می‌کنند تا بتوانند رایانه‌های راه دور را آلوده نمایند. بنابراین اگر قوانین به درستی پیکربندی شوند، دیواره آتش شخصی تبدیل به ابزار بسیار مفیدی جهت دفع حملات کدهای مخرب می‌شود.

### ۴-۲-۷- ثبت وقایع و رخدادها

دیواره آتش شخصی "ESS" تمامی رخدادهای مهم را در یک فایل ثبت رخدادها (log file) ذخیره سازی می‌نماید. برای مشاهده این فایل می‌توان مستقیما از منوی اصلی نرم افزار بر روی گزینه "tools" و پس از آن بر روی گزینه "log files"کلیک نموده و از منوی بازشونده سمت راست پنجره اصلی نرم افزار گزینه "ESET personal firewall log" را انتخاب نمود.

فایلهای ثبت رخدادها ابزار بسیار مناسبی جهت شناسایی خطاها و مشاهده تهدیدات شناسایی شده هستند و لذا باید به آنها توجه ویژه‌ای نمود. در فایلهای ثبت رخدادهای دیواره آتش شخصی "ESS" اطلاعات ذیل قابل مشاهده می‌باشد:




۱- زمان و تاریخ رخداد

۲- نام رخداد

۳- آدرسهای شبکه‌ای منبع تهدید و هدف آن

۴- پروتکل ارتباطی شبکه

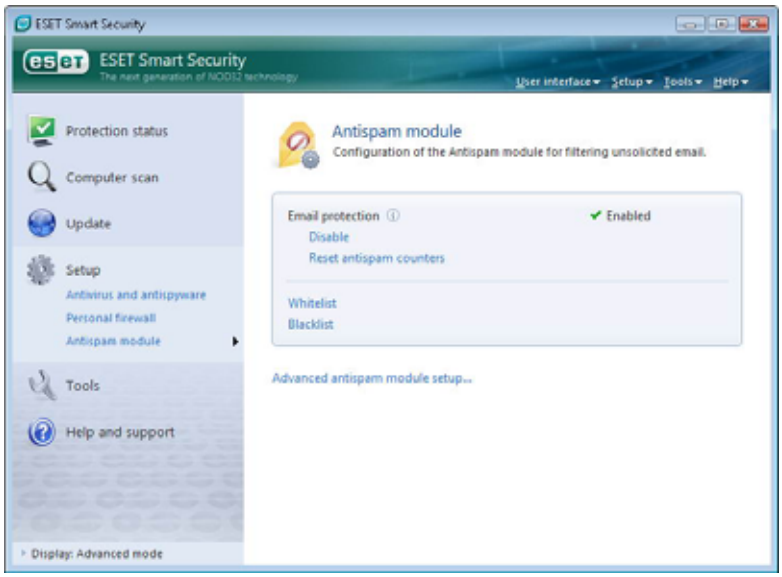
۵- قانون اعمال شده و یا نام کد مخرب (در صورت شناسایی آن)

۶- نرم افزاری که با تهدید شناسایی شده مرتبط بوده است.

تحلیل عمیق‌تر این اطلاعات می‌تواند در شناسایی عوامل دیگری که امنیت سیستم را تهدید نموده‌اند، کاربران را یاری نماید. به بیان دیگر فاکتورهای بسیار دیگری در فایل ثبت رخدادها وجود دارند که می‌توانند به صورت بالقوه تهدیدی برای سیستم به شمار آیند و تحلیل عمیق این فاکتورها گام موثری در کاهش اثر آنها خواهد بود. از جمله این فاکتورها می‌توان به برقراری ارتباطات مستمر از طرف آدرس‌های نامعلوم، ارتباطات نامعلوم نرم افزارهای کاربردی و همچنین پورتهای مورد استفاده قرار گرفته نامعمول اشاره کرد.

### ۴-۳- حفاظت در برابر هرزنامه‌ها

امروزه نامه‌های الکترونیک ناخواسته که از آنها به هرزنامه یاد می‌شود،رتبه بالایی را در میان مشکلات و معضلات مربوط به ارتباطات الکترونیک به خود اختصاص داده‌اند. به بیان دیگر بیش از ۸۰ درصد نامه‌های الکترونیک را هرزنامه‌ها تشکیل می‌دهند. وظیفه ماژول حفاظت در برابر هرزنامه‌ها نیز حفاظت در برابر همین معضل است. به بیان دیگر این ماژول با استفاده از مجموعه‌ای از روشهای موثر باعث فیلترسازی این نوع تهدیدات رایانه‌ای می‌گردد.




یکی از روشهای مهم در شناسایی هرزنامه‌ها عبارت از شناسایی نامه‌های ناخواسته بر اساس فهرست‌های از پیش تعیین شده معتبر (white list) و نامعتبر (blacklist) است. در واقع تمامی آدرس‌های موجود در نرم‌افزار مدیریت پست الکترونیک کاربر به صورت خودکار و همچنین تمامی آدرس‌هایی که توسط کاربر به عنوان آدرس‌های معتبر تعیین گردیده‌اند به فهرست سفید (معتبر) افزوده می‌گردند.

روش اصلی در شناسایی یک هرزنامه عبارت از پویش خصوصیات نامه الکترونیک مورد نظر است. به بیان دیگر نامه‌های دریافتی بر اساس شرائط پایه‌ای مربوط به ضد هرزنامه‌ها از قبیل توضیحات مربوط به پیام، اطلاعات آماری مربوط به هوش مصنوعی، شناسایی الگوریتم‌ها و دیگر روش‌های منحصر به فرد مورد پویش قرار گرفته و مقادیر بدست آمده موجود در ایندکس بدست آمده مشخص می‌کنند که آیا نامه مورد نظر یک هرزنامه است و یا خیر.

یکی دیگر از روش‌های فیلترسازی مورد استفاده عبارت از فیلتر بایسیان است که مورد استفاده قرار می‌گیرد. در این روش کاربر با علامت زدن نامه‌ها به عنوان هرزنامه و یا نامه الکترونیکی عادی یک بانک اطلاعاتی از لغات ایجاد می‌نماید که لغات مربوط به دسته هرزنامه ها و دسته نامه‌های عادی را شامل می‌شود. هر چقدر این بانک اطلاعاتی حاوی اطلاعات بیشتری باشد، دقت ماژول ضد هرزنامه در تشخیص هرزنامه‌ها افزایش می‌یابد.

ترکیب روشهای ضد هرزنامه مطرح شده در این بخش باعث افزایش نرخ آشکارسازی هرزنامه‌ها می‌گردد. ضمن اینکه ماژول ضد هرزنامه "ESS" حفاظت نرم افزارهای مدیریت پست الکترونیک "Microsoft Outlook"، "Outlook Express" و "Windows Mail" را پشتیبانی می‌کند.

### ۱-۳-۴- ضد هرزنامه به صورت خودآموز

مسائل مربوط به خودآموز ضد هرزنامه بیشتر در ارتباط با فیلتر بایسیان است. در واقع اهمیت هر یک از لغات در طول فرایند آموزش اینکه چه نامه‌ای یک هرزنامه و چه نامه‌ای یک نامه عادی است، متفاوت است. بنابراین هرچه تعداد نامه‌های طبقه بندی شده (به لحاظ هرزنامه و یا نامه عادی بودن) بیشتر باشد، نتایج بدست آمده از طریق روش فیلتر بایسیان دقیقتر خواهد بود.

ضمن اینکه لازم است آدرس‌های معتبر را در فهرست سفید (مجاز) اضافه نمائید تا این آدرس‌ها مورد فیلترسازی قرار نگیرند.

### ۱-۱-۳-۴- افزودن آدرس‌ها به فهرست سفید

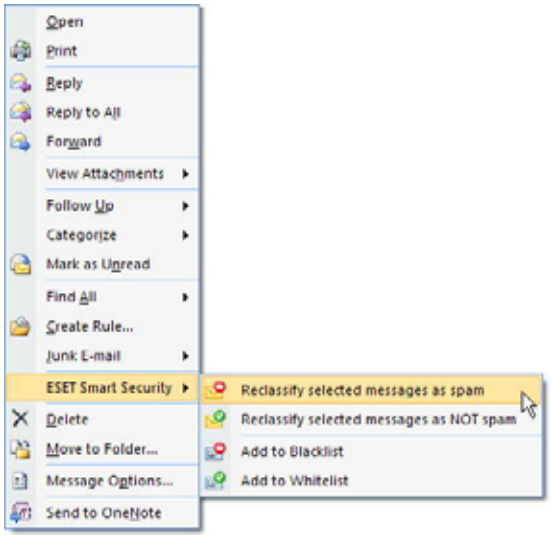
کاربران می‌توانند آدرس‌های پست الکترونیک اشخاصی که با آنها ارتباط الکترونیکی دارند را در فهرست مجاز (فهرست سفید) درج نمایند.

با درج آدرس در فهرست سفید هیچ نامه‌ای از آن آدرس به عنوان هرزنامه تلقی نخواهد شد. برای افزودن یک آدرس جدید به این فهرست کافی است بر روی نامه الکترونیکی مورد نظر راست کلیک کرده و سپس گزینه "ESET smart security" را برگزینید و پس از آن زیر منوی "add to whitelist" را انتخاب کنید. روش دیگر عبارت از کلیک بر روی گزینه "trusted address" موجود در نوار ابزار ضد هرزنامه "ESS" در قسمت بالایی پنجره نرم افزار مدیریت پست الکترونیکی است. به طور مشابه می‌توان از این روش برای هرزنامه‌ها استفاده نمود. اگر آدرسی در فهرست سیاه (غیرمجاز) درج گردد، هر نامه‌ای که از آن آدرس ارسال شده باشد به عنوان هرزنامه تلقی می‌شود.

### ۲-۱-۳-۴- نشانه گذاری یک نامه به عنوان هرزنامه

هر یک از نامه‌های موجود در صندوق پستی نرم افزار مدیریت پست الکترونیک را می‌توان به عنوان یک هرزنامه نشانه‌گذاری کرد. بدین منظور کافی است بر روی نامه مورد نظر راست کلیک کرده و از منوی ایجاد شده گزینه "ESET smart security" و پس از آن زیر منوی "reclassify selected messages as spam" را انتخاب نمائید.

روش دوم عبارت از کلیک بر روی گزینه "spam" موجود در نوار افزار ضد هرزنامه "ESS" در قسمت بالایی پنجره نرم افزار مدیریت پست الکترونیک است.



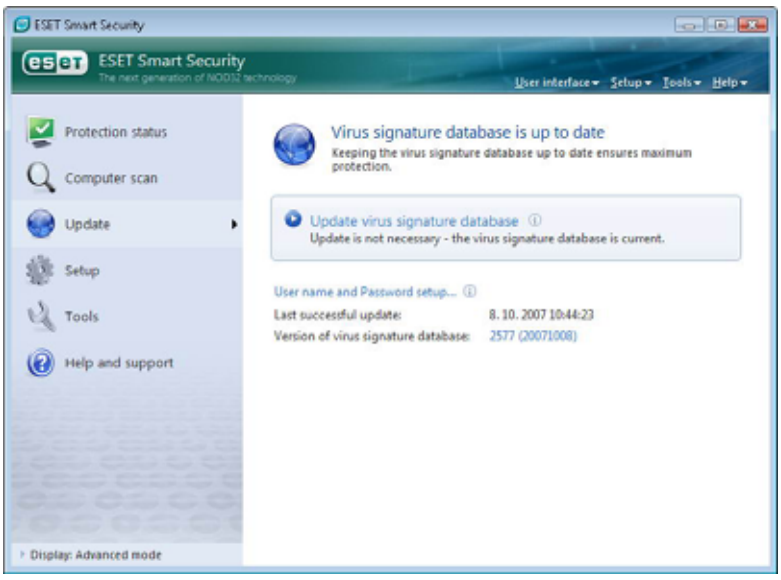

نامه‌های طبقه بندی شده مجدد (reclassified) به طور خودکار به پوشه "spam" انتقال داده می‌شوند، اما آدرس شخص ارسال کننده آنها به فهرست سیاه افزوده نمی‌شود. به طور مشابه می توان نامه‌های دریافتی را در گروه نامه‌های عادی (not spam) طبقه کرد. همچنین اگر نامه‌هایی از پوشه "junk e-mail" را در گروه نامه‌های عادی طبقه بندی نمائید، این نامه‌ها به پوشه اصلی

خودشان انتقال پیدا می‌کنند. ضمن اینکه توجه داشته  که با مشخص کردن یک نامه به عنوان یک نامه عادی، آدرس فرستنده آن به صورت خودکار به فهرست سفید اضافه نخواهد شد.

### ۴-۴- بروزرسانی برنامه

بروزرسانی مستمر سیستم پایه اصلی در دستیابی به حداکثر سطح حفاظتی "ESS" است. با استفاده از ماژول بروزرسانی نرم افزار همواره برنامه بروز می‌ماند. دو روش برای بروزرسانی نرم افزار وجود دارد که عبارت از بروزرسانی بانک اطلاعاتی شناسه ویروسهای رایانه‌ای و بروزرسانی تمامی اجزای نرم افزار می باشند.

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 از نگارش فعلی بانک اطلاعاتی شناسه ویروسهای رایانه‌ای و نیاز و یا عدم نیاز به بروزسانی نرم افزار می باشد. همچنین در این قسمت گزینه‌ای وجود دارد که با کلیک بر روی آن می‌توانید فورا فرایند بروزسانی را آغاز کنید. این گزینه  عبارت از "update virus signature database" می‌باشد. از دیگر قسمت‌های قابل دسترسی می‌توان به لینک "user name and password setup" جهت درج شناسه کاربری و کلمه عبور به منظور دسترسی به سرورهای بروزرسانی "ESET" اشاره نمود. اطلاعات دیگر مفید موجود در این پنجره عبارت از تاریخ و زمان آخرین بروزرسانی نرم افزار و همچنین شماره بانک اطلاعاتی شناسه ویروسها است. با کلیک بر روی شماره بانک اطلاعاتی شناسه ویروسها پنجره ای گشوده شده و کاربر به صورت دینامیکی به صفحه‌ای از وب سایت "ESET" دسترسی پیدا می‌کند که نمایانگر شناسه‌های موجود در بسته بروزرسانی فعلی نرم افزار نصب شده بر روی رایانه کاربر است.

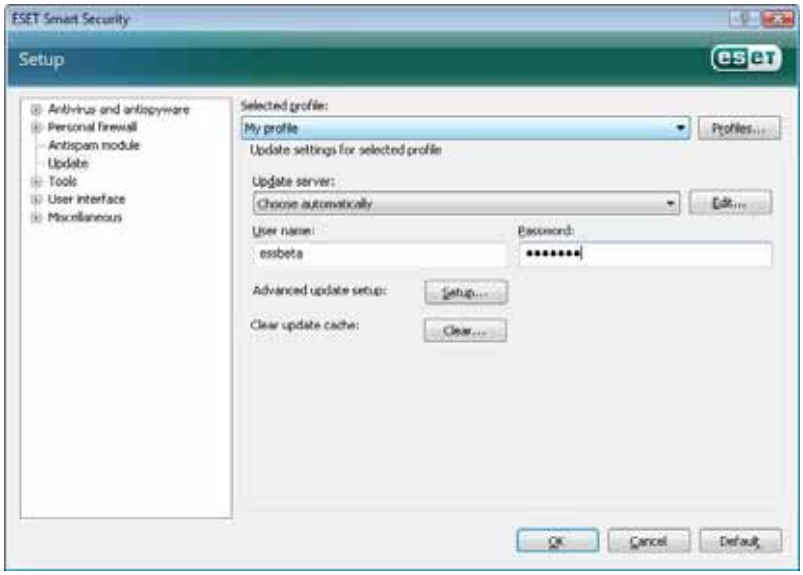



*توجه: شناسه کاربری و کلمه عبور پس از خرید نرم افزار از طرف شرکت "ESET" در اختیار کاربر قرار می‌گیرند.*

### ۴-۴-۱- تنظیمات مربوط به بروزرسانی

قسمت مربوط به تنظیمات بروزرسانی حاوی اطلاعاتی چون منبع بروزرسانی نرم افزار نظیر نام سرورهای بروزرسانی و اطلاعات مربوط به تائید اعتبار جهت دسترسی به فایلهای بروزرسانی از طریق این سرورها است.

به صورت پیش فرض، فیلد "update server" بر روی گزینه "choose automatically" تنظیم گردیده است. در این حالت فایلهای بروزرسانی نرم افزار از سرورهایی دانلود می‌شود که دارای بار ترافیکی کمتری هستند. برای دسترسی به پنجره تنظیمات بروزرسانی نرم افزار کافی است پس از فشردن کلید "F5" صفحه کلید، بر روی گزینه "update" کلیک کنید.




برای دسترسی به فهرست سرورهای بروزرسانی کافی است از منوی بازشونده "update server" استفاده نمائید. ضمن اینکه جهت افزودن یک سرور جدید می‌توانید با کلیک بر روی دکمه "edit..." موجود در قسمت

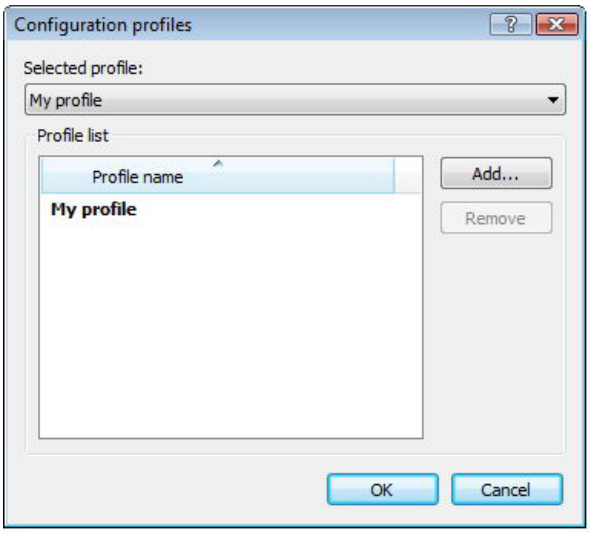
"update settings for selected profile"

کلیک کرده و پس از آن گزینه "add" را انتخاب کنید.

همانطور که قبلا نیز اشاره شد، اطلاعات مربوط به تائید اعتبار کاربر جهت دانلود فایلهای بروزرسانی نرم افزار از سرورهای شرکت "ESET" همان شناسه کاربری و کلمه عبوری است که شرکت "ESET" پس از خرید نرم افزار به کاربر ارائه می‌کند.

### ۱-۱-۴-۴- پروفایلهای بروزرسانی

کاربران می‌توانند با ایجاد پروفایلهای بروزرسانی متعدد از تنظیمات و پیکربندی‌های 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 نموده‌اند، بسیار بهتر و موثرتر است. زیرا پیکربندی تنظیمات اینترنت این نوع کاربران دائما از نقطه ای به نقطه دیگر تغییر می‌کند 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 نمائید. در زمان ایجاد یک پروفایل جدید قادر خواهید 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.

در زمان انجام تنظیمات مربوط به یک پروفایل می‌توان سرور مورد نظر جهت دانلود فایلهای بروزرسانی را نیز مشخص نمود. به بیان دیگر کاربران هم می‌توانند هر یک از سرورهای موجود در فهرست سرورها را انتخاب کنند و هم امکان افزودن سرور جدید برای آنها فراهم آمده است. جهت دسترسی به فهرست سرورهای موجود می‌توانید از فهرست بازشونده "update server" استفاده کنید.

به منظور افزودن یک سرور جدید نیز می‌توانید بر روی گزینه "edit..." موجود در قسمت

"update settings for selected profile"

کلیک کرده و پس از آن گزینه "add"را انتخاب نمائید.

### ۲-۱-۴-۴- تنظیمات پیشرفته بروزرسانی

جهت مشاهده تنظیمات پیشرفته بروزرسانی کافی است بر روی دکمه "setup..." کلیک نمائید. با انجام این کار پنجره‌ای گشوده می‌شود که حاوی برگ نشان‌های مد یا حالت بروزرسانی(update mode)، "HTTP proxy" ، "lan" و "Mirror" می‌باشد.

### ۱-۲-۱-۴-۴- برگ نشان "update mode"

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

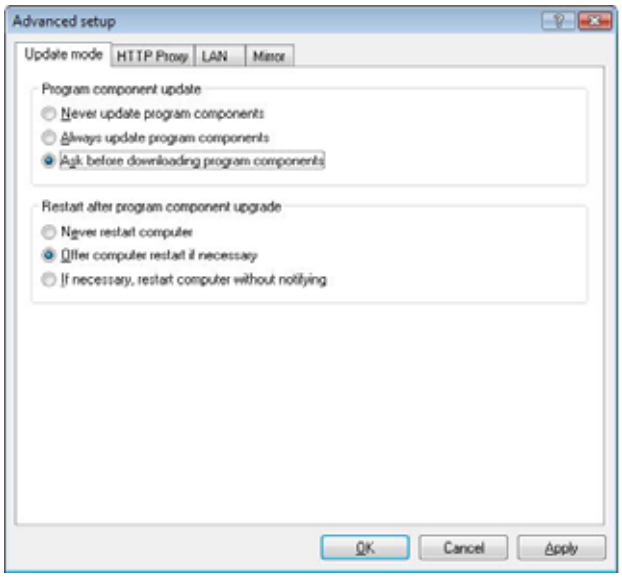
الف: عدم بروزرسانی اجزای نرم افزار

ب: بروزرسانی همیشگی اجزای نرم افزار

ج: اخذ نظر کاربر در مورد دانلود اجزای نرم افزار

انتخاب گزینه اول به کاربر اطمینان می‌دهد که در صورت وجود فایل‌های بروزرسانی اجزای "ESS" بر روی سرورهای "ESET"، این فایلها دانلود نشوند و لذا اجزای نرم افزار مورد بروزرسانی قرار نخواهند گرفت. گزینه دوم عکس گزینه اول است. یعنی زمانی که فایلهای بروزرسانی بر روی سرورهای بروزرسانی "ESET" قرار گیرند، توسط نرم افزار دانلود شده و اجزای نرم افزار به نگارش جدید دانلود شده ارتقاء می‌یابند.

با انتخاب گزینه سوم نیز نرم افزار در صورت وجود فایلهای بروزرسانی اجزای "ESS" بر روی سرورهای "ESET" نسبت به دانلود آنها از کاربر سوال می‌کند. در این حالت پنجره‌ای که حاوی اطلاعات در زمینه فایلهای بروزرسانی موجود بر روی سرورهای "ESET" است، گشوده شده و کاربر می‌تواند نسبت به دانلود و یا عدم دانلود آنها اتخاذ تصمیم نماید. در صورت دانلود این فایلها نیز اجزای نرم افزار مورد بروزرسانی قرار می‌گیرند. توجه داشته باشید که در اینجا حالت پیش فرض گزینه سوم است.




پس از بروزرسانی اجزای نرم افزار لازم است تا سیستم راه‌اندازی مجدد گردد تا ماژولهای بروز شده بتوانند به صورت کامل وظایف خود را به انجام رسانند. بنابراین گزینه‌هایی در این ارتباط در قسمت

"restart after program component upgrade"

پیش بینی شده است تا کاربر بتواند هر یک از آنها را انتخاب نماید. این گزینه‌ها عبارتند از:

الف: عدم راه‌اندازی مجدد رایانه

ب: ارائه پیشنهاد به راه‌اندازی مجدد رایانه در صورت نیاز

ج: راه‌اندازی مجدد رایانه در صورت نیاز بدون اطلاع قبلی به کاربر.

در این جا نیز حالت پیش فرض گزینه دوم است. انتخاب گزینه‌های مناسب در رابطه با بروزرسانی اجزای نرم افزار در برگ نشان "update mode" بستگی به هر یک از ایستگاه‌های کاری دارد و با توجه به نیازهای هر یک از ایستگاه‌ها لازم است از گزینه‌های متناسب با آن نیازها استفاده به عمل آید.

لذا لازم است توجه داشته باشید که تفاوتهای زیادی بین سرورها و ایستگاه‌های کاری وجود دارد. به عنوان مثال راه‌اندازی مجدد (restart) و به صورت خودکار یک سرور پس از بروزرسانی اجزای نرم افزاری نصب شده بر روی آن می‌تواند اثرات نامطلوبی در کارکرد شبکه داشته باشد.

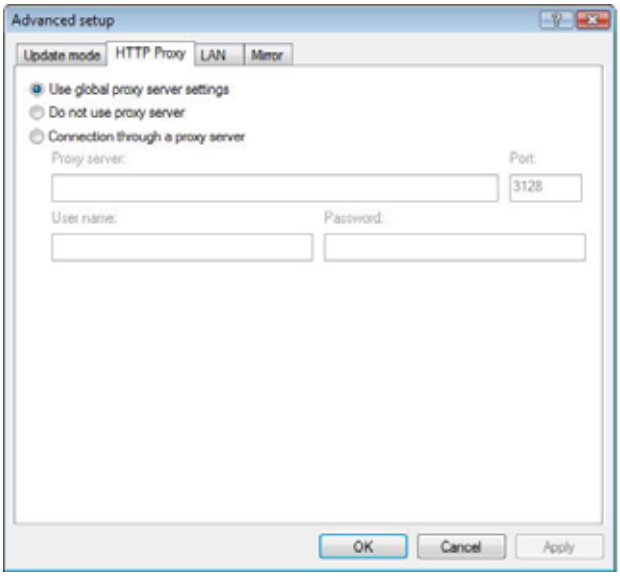
### ۲-۲-۱-۴-۴- سرور "proxy"

جهت دسترسی به گزینه‌های تنظیمات سرور "proxy" برای هر یک از پروفایلهای انتخاب شده کافی است پس از فشردن کلید "F5" صفحه کلید بر روی گزینه "update" کلیک کرده و سپس برگ نشان "HTTP proxy" را برگزینید. گزینه‌های موجود در این قسمت عبارتند از:

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

- اتصال از طریق یک سرور "proxy"

با انتخاب گزینه اول از گزینه‌های مربوط به پیکربندی سرور "proxy" در قسمت "proxy server" پنجره تنظیمات پیشرفته استفاده به عمل خواهد آمد. توجه داشته باشید که برای رسیدن به گزینه "proxy server" در پنجره تنظیمات پیشرفته لازم است که در ابتدا گزینه "miscellaneous" را برگزینید.




همچنین اگر از سرور "proxy" استفاده به عمل نمی‌آورید نیز می‌توانید گزینه دوم را برگزینید. از گزینه سوم نیز زمانی استفاده می‌شود که کاربر برای بروزرسانی "ESS" از یک سرور "proxy" متفاوت از آن سروری که در پنجره تنظیمات پیشرفته نرم افزار مشخص کرده است، استفاده می‌نماید. لذا اگر چنین باشد، باید کاربر اطلاعات مربوط به این سرور "proxy" از جمله آدرس، پورت ارتباطی و در صورت نیاز شناسه کاربری و کلمه عبور مرتبط را در فیلدهای مربوطه درج نماید.

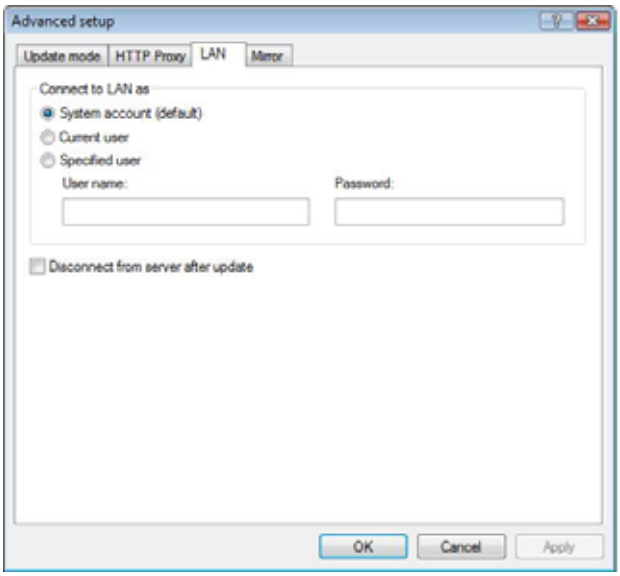
یکی دیگر از حالاتی که در آن شرائط می‌توان گزینه سوم را برگزید این است که تنظیمات سرور "proxy" به صورت جامع (globally) در پنجره تنظیمات پیشرفته لحاظ نشده باشد و لازم باشد "ESS" برای بروزرسانی از یک سرور "proxy" استفاده کند.

نکته آخر اینکه توجه داشته باشید که گزینه پیش فرض نرم افزار عبارت از گزینه اول است.

### ۳-۲-۱-۴-۴- اتصال به شبکه "LAN"

همانطور که می‌دانید اگر عملیات بروزرسانی از روی یک سرور محلی دارای سیستم عامل مبتنی بر شبکه (NT–based) انجام پذیرد، به صورت پیش فرض تمامی ارتباطات ایستگاه‌های کاری با سرور پس از تائید اعتبار برقرار می‌گردند. در اکثر مواقع شناسه کاربری محلی فاقد مجوزهای لازم جهت دسترسی به پوشه "Mirror" که حاوی اطلاعات بروزرسانی نرم افزار است می‌باشد. در چنین شرائطی کافی است شناسه کاربری و کلمه عبور خود را در قسمت تنظیمات بروزرسانی وارد نمائید و یا از حساب کاربری‌ای استفاده کنید که بر اساس آن دسترسی برنامه به فایلهای بروزرسانی مقدور باشد.

به منظور درج چنین حساب کاربری‌ای کافی است بر روی برگ نشان "LAN" کلیک کرده و یکی از گزینه‌های قسمت "connect to LAN as" را انتخاب کنید. این گزینه‌ها عبارت از حساب کاری سیستمی که گزینه پیش فرض است، حساب کاربری جاری و حساب کاربری خاص هستند.




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

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 می‌توان گزینه "current user" را برگزید. ایراد این روش آن است که نرم افزار نصب شده بر روی ایستگاه کاری در صورتی که هیچ کاربری از طریق آن ایستگاه به شبکه وصل نشده باشد، قادر به اتصال و دریافت فایلهای بروزرسانی نخواهد بود.

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

نکته آخر اینکه گزینه پیش فرض در اینجا گزینه "system account" است.

*هشدار:*

*زمانی که هر یک از گزینه‌های "current user" و یا "specified user" انتخاب شده باشند، ممکن است خطایی در زمان تغییر اطلاعات مورد استفاده جهت تائید اعتبار به اطلاعات کاربر مورد نظر رخ دهد. لذا دلیل اصلی توصیه شرکت "ESET" مبنی بر درج اطلاعات مربوط به تائید اعتبار شبکه محلی (LAN) در قسمت اصلی تنظیمات بروزرسانی نیز همین مورد است. در قسمت اصلی تنظیمات بروزرسانی، اطلاعات مربوط به تائید اعتبار به شکل زیر درج می‌گردند:*

الف) "domain–name\user" به همراه کلمه عبور کاربر در شبکه دامین

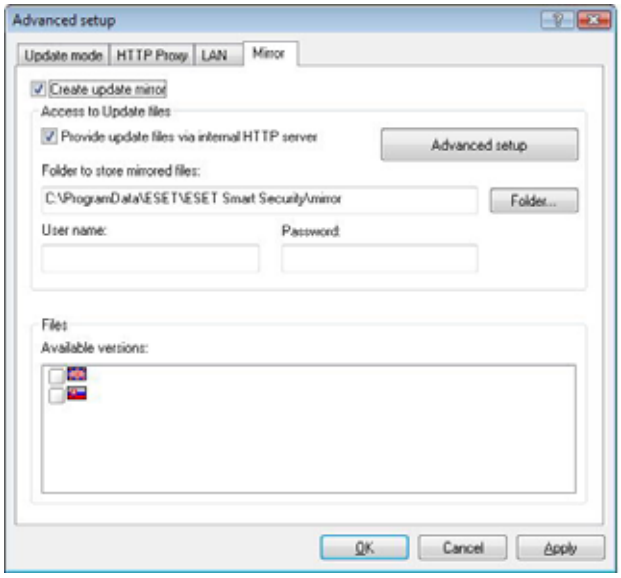
ب) "workgroup–name\user" به همراه شناسه کاربری در شبکه "workgroup"

همچنین در صورتی که از نگارش "HTTP" سرور محلی استفاده می‌شود، نیازی به تائید اعتبار وجود ندارد.

### ۴-۲-۱-۴-۴- ایجاد پوشه بروزرسانی "Mirror"

نسخه تجاری "ESS" امکان ایجاد پوشه بروزرسانی "Mirror"بر روی یک رایانه جهت استفاده دیگر ایستگاه‌های کاری موجود در شبکه از روی اطلاعات آن به منظور بروزرسانی را فراهم آورده است. استفاده از پوشه "Mirror" جهت بروزرسانی ایستگاه‌های کاری

موجود در شبکه علاوه بر اینکه تعادل بار شبکه را بهینه می‌کند، باعث می‌شود تا بتوان از پهنای باند بستر اینترنتی استفاده‌های دیگری نمود.




جهت دسترسی به تنظیمات مربوط به سرور محلی "Mirror" کافی است پس از فشردن کلید "F5" و نمایان شدن پنجره تنظیمات پیشرفته بر روی گزینه "update" کلیک کرده و سپس در قسمت سمت راست پنجره گزینه "setup..." را برگزینید و پس از آن بر روی برگ نشان "Mirror" کلیک نمائید.

اولین قدم جهت پیکربندی "Mirror" عبارت از تیک زدن گزینه "create update Mirror" است. انتخاب این گزینه باعث فعال شدن دیگر گزینه‌های موجود در پنجره جاری می‌گردد.

روش‌های فعال سازی "Mirror" در بخش "متغیرهای دسترسی به Mirror " به صورت کامل تشریح می‌شوند. صرفا در اینجا لازم است توجه داشته باشید که دو روش پایه‌ای برای دسترسی به "Mirror" وجود دارد. به بیان دیگر می‌توان "Mirror" را هم در قالب یک پوشه به اشتراک گذاشته شده و هم به صورت یک سرور "HTTP" مورد استفاده قرار داد.

لازم است مسیر پوشه حاوی اطلاعات بروزرسانی را در قسمت "folder to store Mirrored files" درج کنید. با کلیک بر روی دکمه "folder..." نیز می‌توانید پوشه مورد نظر را در رایانه محلی و یا شبکه رایانه‌ای جستجو کرده و آدرس آن را به صورت خودکار درج نمائید.

همچنین اگر دسترسی به پوشه مورد نظر مستلزم وجود شناسه کاربری و کلمه عبور است، می‌بایست این اطلاعات را در فیلدهای "user name" و "password" درج نمائید. ضمن اینکه توجه داشته باشید که درج شناسه کاربری در اینجا باید در قالب "domain\user" و یا "workgroup\user" انجام شود.

در زمان انجام دیگر پیکربندی‌های "Mirror" می‌توان با توجه به زبان نگارش "ESS" فایلهای بروزرسانی مورد نظر جهت دانلود را مشخص نمود. بدین منظور کافی است در قسمت "available versions" زبانهای مورد نظر را انتخاب کنید.

### ۱-۴-۲-۱-۴-۴- بروزرسانی از طریق "Mirror"

از "Mirror" در دو قالب پوشه به اشتراک گذاشته شده و یا سرور "HTTP" می‌توان جهت بروزرسانی ایستگاه های کاری استفاده به عمل آورد.

۱) دسترسی به "Mirror" با استفاده از سرور "HTTP" داخلی

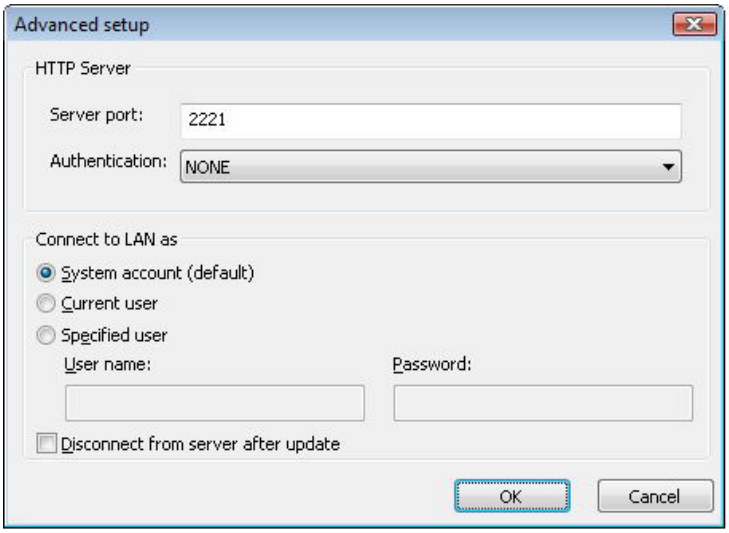
این پیکربندی گزینه پیش فرض برنامه است. به منظور مجاز نمودن دسترسی به "Mirror" با استفاده از سرور "HTTP" کافی است بر روی برگ نشان "Mirror" موجود در پنجره تنظیمات پیشرفته بروزرسانی کلیک کرده و سپس گزینه

"create update Mirror" را تیک بزنید. سپس بر روی دکمه "advanced setup" کلیک کرده تا پنجره حاوی تنظیمات سرور "HTTP" گشوده شود. در این پنجره می‌توان علاوه بر درج شماره پورت سرور، نوع تائید اعتبار مورد استفاده سرور "HTTP" را مشخص کرد. به صورت پیش فرض گزینه "server port" بر روی شماره ۲۲۲۱ تنظیم گردیده است. در قسمت "authentication" نیز روشهای مختلف تائید اعتبار برای دسترسی به فایلهای بروزرسانی ارائه گردیده‌اند.

این گزینه‌ها عبارت از "none" ، "basic" و "NTLM" هستند. با انتخاب گزینه "basic" از روش کدگذاری "base 64" جهت تائید اعتبار شناسه کاربری و کلمه عبور استفاده کنید. گزینه "NTLM" نیز یک روش کدگذاری ایمن را برای کاربر به ارمغان می‌آورد. توجه داشته باشید که در فرایند تائید اعتبار از حساب کاربری ایجاد شده بر روی رایانه حاوی پوشه "Mirror" استفاده می‌شود. گزینه پیش فرض مربوط به فرایند تائید اعتبار نیز گزینه "none" است. با انتخاب این گزینه دسترسی به فایلهای بروزرسانی بدون انجام فرایند تائید اعتبار به انجام می‌رسد.

*هشدار:*

*اگر قصد دارید از طریق سرور "HTTP" به فایلهای بروزرسانی دسترسی داشته باشید، می‌بایست پوشه "Mirror" بر روی همان رایانه‌ای که "ESS" آن را ایجاد کرده است قرار داشته باشد .*




پس از پایان پیکربندی "Mirror" به ایستگاه‌های کاری رفته و یک سرور بروزرسانی را در "ESS" نصب شده بر روی آنها و در قالب "HTTP://IP-ADDRESS-OF-YOUR-SERVER:2221" اضافه کنید.

بدین منظور کافی است مراحل ذیل را انجام دهید :

الف) کلید F5 را بزنید تا پنجره تنظیمات پیشرفته گشوده شود و پس از آن بر روی گزینه "update" کلیک کنید.

ب) بر روی دکمه "edit" واقع شده در سمت راست منوی بازشونده "update server" کلیک کرده و یک سرور جدید در قالب ذکر شده را به فهرست سرورها اضافه کنید.

ج) سرور جدید را از فهرست سرورهای بروزرسانی انتخاب کنید.

۲) دسترسی به "Mirror" از طریق به اشتراک گذاشتن پوشه آن

در این حالت ابتدا لازم است یک پوشه به اشتراک گذاشته شده بر روی رایانه محلی و یا یکی از رایانه‌های موجود در شبکه ایجاد کنید. توجه داشته باشید که در زمان ایجاد این پوشه لازم است به کاربری که اطلاعات بروزرسانی را در این پوشه قرار می‌دهد مجوز "نوشتن" و به دیگر کاربران که از این پوشه استفاده می‌کنند، مجوز "خواندن" ارائه گردد.

در گام بعدی لازم است تنظیمات دسترسی به "Mirror" را انجام دهید. بدین منظور ابتدا دکمه "F5" را فشرده و سپس بر روی گزینه "update" کلیک نمائید و پس از آن برگ نشان "Mirror" را برگزینید. سپس می‌بایست گزینه

"provide update files via internet HTTP server"

را که در حالت پیش فرض فعال است، غیر فعال نمائید.

توجه داشته باشید که اگر پوشه به اشتراک گذاشته شده بر روی هر یک از رایانه‌های شبکه باشد لازم است شناسه کاربری و کلمه عبور جهت دسترسی به آن رایانه درج شود. بدین منظور کافی است بر روی برگ نشان "LAN" کلیک کرده و تنظیمات مربوطه را که قبلا مورد بررسی قرار گرفتند را به انجام رسانید.

پس از پایان پیکربندی "Mirror" به ایستگاه‌های کاری رفته و آدرس سرور بروزرسان را در قالب آدرس "UNC PATH" درج نمائید.

بدین منظور مراحل ذیل انجام می‌پذیرد:

- به ایستگاه کاری مورد نظر مراجعه کرده و پنجره تنظیمات پیشرفته "ESS" را بازکنید و پس از آن بر روی گزینه "update" کلیک نمائید.
- بر روی دکمه "edit..." مجاور گزینه "update server" کلیک کرده و یک سرور را در قالب "UNC PATH" به فهرست سرورها اضافه کنید.
- سرور جدید را به عنوان سرور بروزرسان از فهرست سرورها انتخاب نمائید.

*توجه:*

به منظور انجام فرایند بروزرسانی به طور صحیح لازم است که مسیر "Mirror" در قالب مسیر "UNC" درج شود. زیرا در صورت استفاده از آدرس درایو های "map" شده ممکن است فرایند بروزرسانی به طور صحیح انجام نپذیرد.

### ۲-۴-۲-۱-۴-۴- رفع اشکالات مربوط به بروزرسانی از طریق "Mirror"

گاهی اوقات کاربران با توجه به روش اتصال به پوشه "Mirror" با خطاهای متفاوتی روبرو می‌گردند. در اکثر این موارد، خطای اتفاق افتاده در زمان بروزرسانی نرم افزار از طریق "Mirror" به یکی از دلایل زیر می‌باشد:

۱- انجام تنظیمات پوشه "Mirror" به طور ناصحیح

۲- درج اطلاعات تائید اعتبار غیر صحیح

۳- پیکربندی اشتباه ایستگاه‌های کاری جهت دانلود فایلهای بروزرسانی

۴- ترکیبی از موارد ذکر شده

در ادامه به تشریح چند مورد از خطاهای رایج پرداخته می‌شود:

الف) "ESS" خطایی را در زمان اتصال به سرور "Mirror" به کاربر اعلام می‌کند:

این خطا معمولا زمانی اتفاق می‌افتد که تنظیمات مربوط به پوشه "Mirror" از قبیل مسیر شبکه‌ای آن صحیح نبوده و ایستگاه‌های کاری قادر به دانلود فایلهای بروزرسانی از این سرور نمی باشند.

به منظور مشخص شدن صحت مسیر درج شده کافی است بر روی دکمه "start" کلیک کرده، گزینه "run" را انتخاب نموده، مسیر مشخص شده تنظیمات "ESS" را درج کرده و "OK" نمائید. اگر آدرس پوشه صحیح باشد باید پنجره مربوط به این پوشه گشوده شده و کاربر بتواند فایلهای بروزرسانی را مشاهده کند.

ب) "ESS" نیاز به شناسه کاربری و کلمه عبور دارد:

این خطا نیز معمولا زمانی رخ می‌دهد که اطلاعات مربوط به تائید اعتبار کاربر به صورت ناصحیح درج گردیده است. به بیان دیگر شناسه کاربری و کلمه عبور جهت دسترسی به پوشه "Mirror" در قسمت تنظیمات مربوط به بروزرسانی به طور اشتباه درج گردیده‌اند. لذا لازم است کاربر صحت اطلاعات درج شده را بررسی نماید. به عنوان مثال، می‌بایست شناسه کاربری در قالب "domain\user name" و یا "workgroup\user name" درج شده باشد. همچنین اگر سرور "Mirror" برای شناسه کاربری "everyone" قابل دسترسی باشد، بدین معنا نیست که همه افراد به این پوشه دسترسی دارند. بلکه معنی اصلی آن است که تمامی کاربران شبکه دامین مجاز به دسترسی به این پوشه هستند. بنابراین اگر این پوشه برای شناسه کاربری "everyone" در دسترس باشد، باز هم لازم است تا شناسه کاربری و کلمه عبور کاربر شبکه دامین در قسمت تنظیمات بروزرسانی درج گردد.

ج) "ESS" خطایی را در زمان اتصال به یک سرور "Mirror" مشخص (منظور این است که مسیر سرور صحیح است) به کاربر اعلام می‌کند:

در این حالت ارتباط از طریق پورت دسترسی به نگارش "HTML" پوشه بروزرسانی (Mirror) بلوکه گردیده است.

### ۲-۴-۴- چگونگی ایجاد "task"های بروزرسانی

بروزرسانی به دو روش انجام می‌پذیرد : روش دستی و روش خودکار

در حالت روش دستی کافی است از منوی اصلی نرم افزار گزینه "update" را انتخاب کنید و پس از آن بر روی گزینه "update virus signature database" کلیک نمائید.

در حالت خودکار می‌توان از برنامه زمان بندی جهت بروزرسانی نرم افزار استفاده کرد. بدین منظور کافی است از منوی "tools" گزینه "scheduler" را بر گزینید. به صورت پیش فرض "task" های زیر در "ESS" فعال هستند.

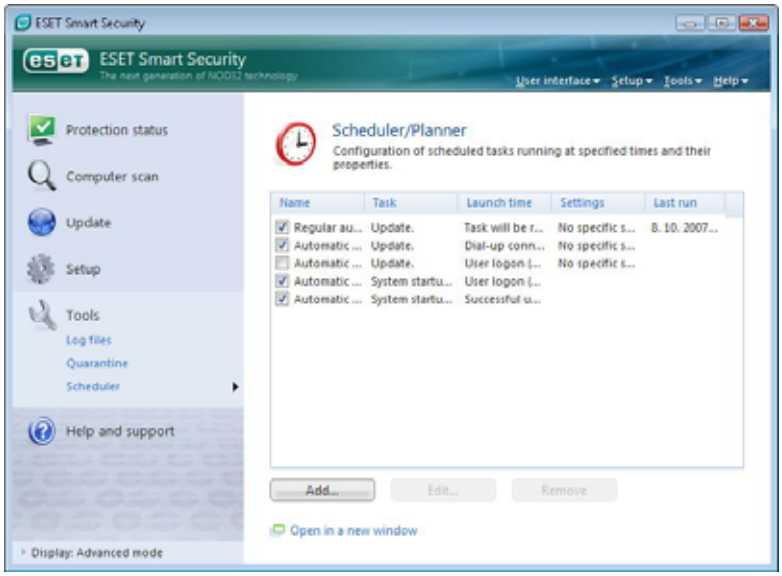
الف) بروزرسانی خودکار عادی

ب) بروزرسانی خودکار پس از ارتباط "dial–up"

ج) بروزرسانی خودکار پس از ورود کاربر به شبکه (logon)

هر یک از این سه روش را می‌توان مطابق با نیازها مورد ویرایش قرار داد. علاوه بر این "task" های بروزرسانی خودکار، کاربران می‌توانند "task" های بروزرسانی جدیدی را به همراه پیکربندی مورد نظر ایجاد نمایند. جهت کسب اطلاعات بیشتر در این خصوص می‌توانید به بخش ۵-۴ مراجعه کنید.

### ۵-۴- برنامه زمان بندی




اگر مد پیشرفته "ESS" فعال شود، برنامه زمان بندی (scheduler) قابل مشاهده خواهد بود. برای اجرای آن نیز کافی است بر روی گزینه "tools" کلیک کرده و سپس گزینه "scheduler" را انتخاب نمائید. با کلیک بر روی این ماژول خلاصه فهرستی از "task" های زمان بندی شده و همچنین خصوصیات آنها از قبیل تاریخ از پیش تعیین شده آنها، زمان اجرای آنها و همچنین پروفایل پویش هر یک از آنها مشاهده خواهد شد.

به صورت پیش فرض "task" های زمان بندی شده زیر در قسمت "scheduler" قابل مشاهده هستند:

۱- بروزرسانی خودکار عادی

۲- بروزرسانی خودکار پس از ارتباط "dial – up"

۳- بروزرسانی خودکار پس از ورود به شبکه

۴- پویش خودکار فایلهای "startup" پس از ورود کاربر به شبکه

۵- پویش خودکار فایلها پس از بروزرسانی بانک اطلاعاتی شناسه ویروسها

جهت ویرایش پیکربندی هر یک از "task" ها اعم از "task" های پیش فرض و یا "task" های تعریف شده توسط کاربر کافی است بر روی "task" مورد نظر راست کلیک کرده و از منوی ایجاد شده گزینه "edit..." را برگزینید. ضمن اینکه می‌توانید "task" مورد نظر را انتخاب کرده و جهت ویرایش آن بر روی دکمه "edit..." کلیک نمائید.

#### ۵-۴-۱- هدف از "task" های زمان بندی شده

با استفاده از "scheduler" می‌توان "task" های زمان بندی شده را مدیریت و یا اجرا نمود. خصوصیات و پیکربندی هر یک از این "task" ها به معنی اطلاعاتی در خصوص تاریخ و زمان اجرای آنها و همچنین پروفایل مورد استفاده در طول اجرای آنها است.

### ۲-۵-۴- ایجاد "task" های جدید

به منظور ایجاد یک "task" جدید در "scheduler" کافی است بر روی دکمه "..add"کلیک کرده و یا راست کلیک نموده و از منوی ظاهر شده گزینه "...add" را برگزینید. ۵ نوع از "task" های زمان بندی شده عبارت اند از :

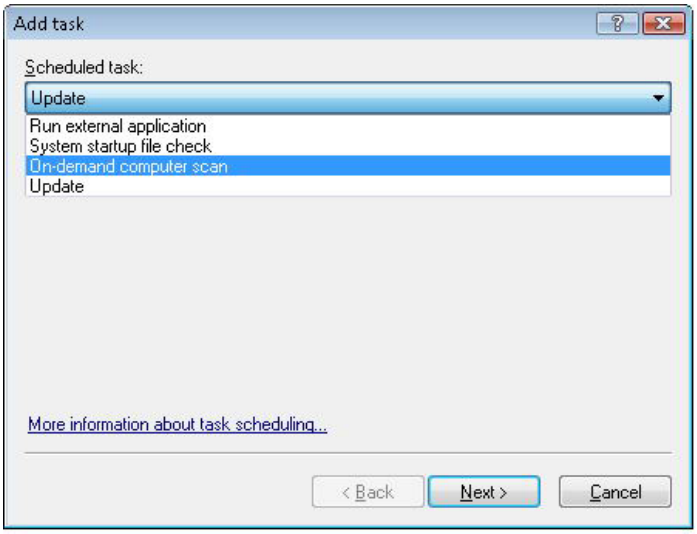
۱- اجرای برنامه کاربردی خارجی

۲- ثبت و نگهداری رخدادها

۳- بررسی فایلهای "startup"

۴- پویش دستی رایانه

۵- بروزرسانی نرم افزار




با توجه به اینکه "task" های بروزرسانی و پویش دستی رایانه بیشتر توسط کاربران مورد استفاده قرار می‌گیرند، در ادامه چگونگی افزودن یک "task" بروزرسانی مورد بررسی قرار خواهد گرفت.

ابتدا لازم است از منوی بازشونده "scheduler task" گزینه "update" را برگزینید. سپس بر روی "next" کلیک کرده و در فیلد "task name" یک نام برای "task" جدید درج کنید. پس از آن لازم است تعدد اجرای "task" را تعیین نمائید. گزینه‌های موجود در این زمینه عبارت از انجام "task" برای یکبار (once) ، به طور مستمر (repeatedly)، روزانه (daily) ، هفتگی (weekly) و حالت شروع رخداد (event – triggered) هستند. سپس بر اساس نوع تکرار انتخاب شده پارامترهایی در اختیار کاربر قرار می‌گیرد. در اینجا لازم است عکس العمل نرم افزار را در زمان عدم اجرای "task" زمان بندی شده مشخص نمائید. این گزینه‌ها نیزعبارتند از:

۱- توقف تا فرا رسیدن زمان بعدی اجرای "task" زمان بندی شده

۲- اجرای "task" در اولین فرصت ممکن

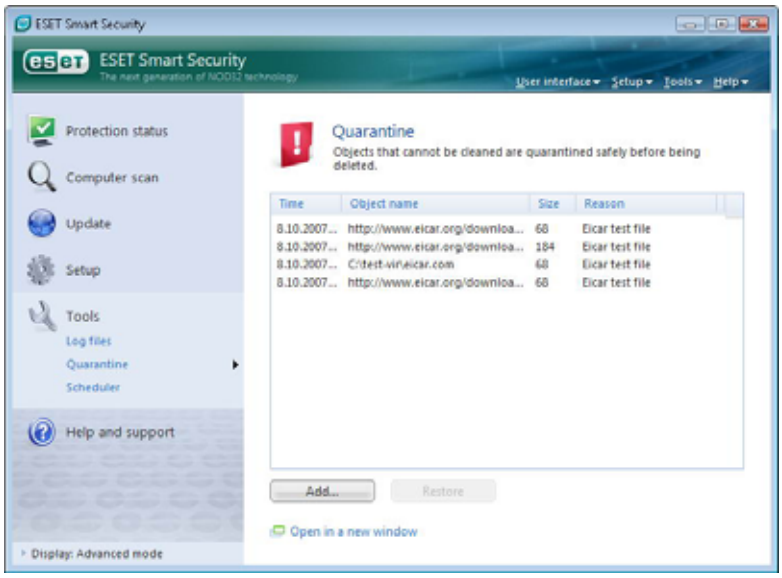
۳- اجرای سریع "task" اگر از آخرین زمان اجرای آن به اندازه مدت زمانی که از پیش تعریف شده است، گذشته باشد( این بازه زمانی را می توان در قسمت "task interval" مشخص نمود).

در گام بعدی نیز پنجره خلاصه وضعیت "task" مورد نظر به نمایش در می‌آید. توجه داشته باشید که می‌بایست گزینه "run task with specific parameters" فعال گردیده باشد. پس از این کار نیز بر روی دکمه "finish" کلیک کنید. اکنون پنجره‌ای گشوده می‌شود و کاربر به وسیله آن می‌تواند پروفایلهای مورد نظر جهت "task" زمان بندی شده را انتخاب کند. در اینجاست که می‌توانید یک پروفایل اصلی و یک پروفایل ثانویه را برگزینید.

از پروفایل ثانویه زمانی استفاده می‌شود که "task" به هر دلیلی نتواند از پروفایل اصلی استفاده نماید. مع الوصف پس از انتخاب پروفایلها بر روی گزینه "OK" موجود در پنجره "update profiles" کلیک کنید. پس از انجام مراحل ذکر شده "task" جدید به فهرست "task" های موجود افزوده می‌گردد.

### ۶-۴- پوشه قرنطینه

وظیفه اصلی پوشه قرنطینه نگهداری از فایلهای آلوده به روشی ایمن است. فایلهای آلوده را در شرائط خاص لازم است قرنطینه نمود. این شرائط به قرار زیر هستند:




- اگر نتوان این فایلها را پاکسازی نمود.
- اگر پاک کردن فایل آلوده ایمن و یا منطقی نباشد.
- اگر فایل آلوده به صورت اشتباه توسط "ESS" به عنوان آلودگی ویروسی شناسایی شده باشند.

کاربر می‌تواند هر فایلی را قرنطینه کند. همچنین بهتر است فایلهای مشکوک به آلودگی را نیز که توسط پویشگر ضدویروس شناسایی گردیده‌اند را نیز قرنطینه نمائید. علاوه بر این کاربران می‌توانند فایلهای موجود در پوشه قرنطینه را برای بررسی و تجزیه و تحلیل به لابراتوارهای ضدویروس شرکت "ESET" ارسال کنند.

نکته دیگر اینکه فایلهای قرنطینه شده را می‌توان در یک جدول به همراه جزئیات هر یک از آنها اعم از تاریخ و زمان قرنطینه شدن، مسیر اصلی فایل دارای آلودگی ویروسی، اندازه فایل برحسب بایت، دلیل قرنطینه کردن فایل (که توسط کاربر مشخص می‌شود) و همچنین تعداد تهدیدات موجود در پوشه قرنطینه (با توجه به اینکه ممکن است یک فایل آرشیو دارای آلودگی ویروسی باشد) مشاهده نمود.

#### ۱-۶-۴- قرنطینه نمودن فایلها

نرم افزار به صورت خودکار نسخه‌ای از هر فایل آلوده‌ای را که پاک می‌کند در پوشه قرنطینه ذخیره سازی می‌نماید مگر اینکه کاربر این ویژگی را در پنجره هشدارها غیر فعال نموده باشد. کاربر در صورت تمایل می‌تواند فایلهای مشکوک به آلودگی را با کلیک بر روی

دکمه "add..." قرنطینه کند. در این صورت فایل اصلی از محل اصلی خود پاک نمی‌گردد. برای افزودن فایلهای مشکوک به پوشه قرنطینه می‌توان از روش راست کلیک و انتخاب گزینه "add..." نیز استفاده نمود.

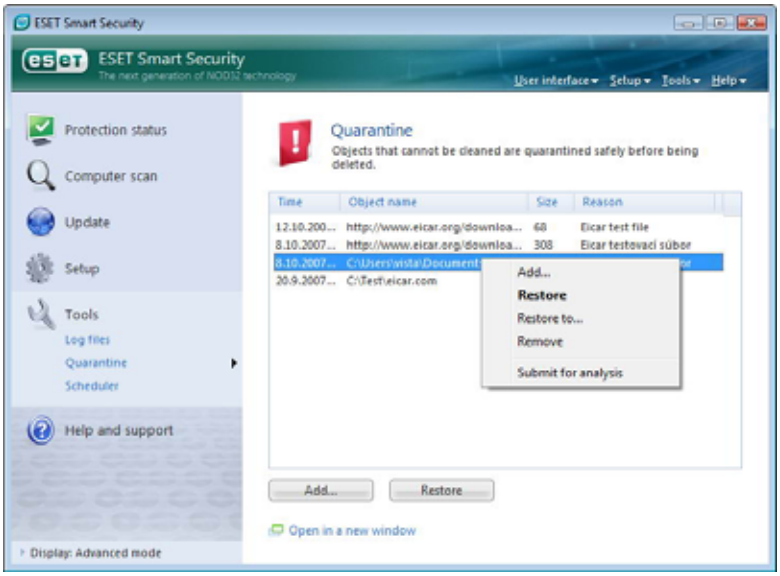
### ۴-۶-۲- برگرداندن (بازیابی) فایلها از پوشه قرنطینه

امکان بازگرداندن فایلهای قرنطینه به محل اصلی آنها فراهم می‌باشد. بدین منظور از ویژگی "restore" استفاده به عمل می‌آید. برای دسترسی به این ویژگی کافی است بر روی آیتم موجود در پنجره قرنطینه راست کلیک کرده و از منوی ظاهر شده گزینه "restore" را برگزینید. همچنین می‌توانید با انتخاب گزینه "restore to" از منوی ظاهر شده، فایل مورد نظر را در هر محل دلخواهی ذخیره سازی کنید.

*توجه:*

*اگر "ESS" یک فایل فاقد آلودگی را به اشتباه قرنطینه نمود، بهتر است آن فایل را از فهرست آیتم‌های پویش شونده حذف نموده و نسخه‌ای از آن را به خدمات فنی مشتریان (ESET customer care) ارسال کنید.*

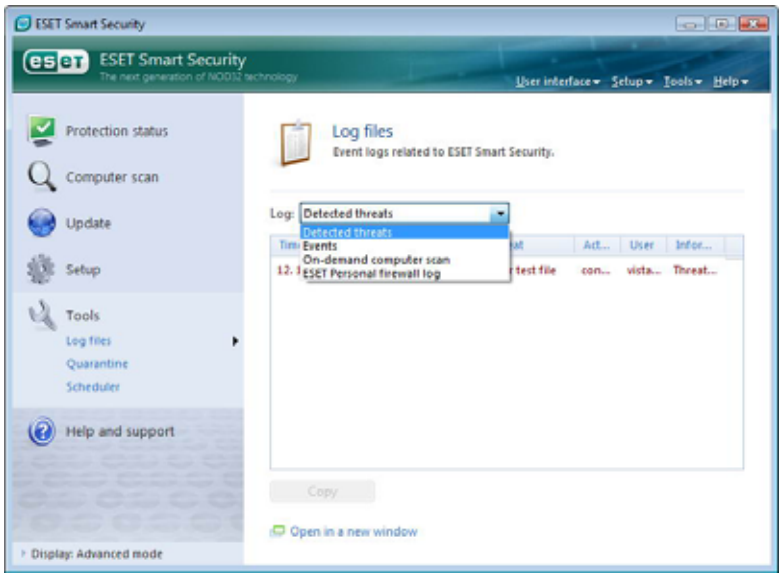
### ۴-۶-۳- ارسال فایلهای موجود در قرنطینه به شرکت "ESET"




اگر فایل مشکوک به آلودگی که توسط پویشگر نرم افزار شناسایی نشده است را قرنطینه نموده‌اید و یا فایلی به اشتباه به دلیل خطاهای مربوط به نرم افزار قرنطینه شده است، می‌توانید آن فایل را جهت تجزیه و تحلیل به لابراتورهای شرکت "ESET" ارسال کنید. بدین منظور کافی است بر روی آیتم مورد نظر موجود در پوشه قرنطینه راست کلیک کرده و از منوی ظاهر شده گزینه "submit for analysis" را برگزینید.

### ۴-۷- فایلهای ثبت رخدادها و وقایع

با استفاده از فایلهای ثبت رخدادها (log files) می‌توان تمامی رخدادهای مهم مربوط به نرم افزار "ESS" و همچنین اطلاعات مربوط به تهدیدات شناسایی شده را مرور نمود. در واقع ثبت رخدادها برای استفاده‌های بعدی روش بسیار موثری در تحلیل، شناسایی تهدیدات و رفع نقص (troubleshooting) نرم افزار است. ثبت رخدادها در پس زمینه کار رایانه انجام پذیرفته و خللی را در امور جاری کاربر ایجاد نمی‌نماید. همچنین اطلاعات مربوط به رخدادها بر اساس تنظیمات گوناگون مربوط به فایل ثبت رخدادهای جاری انجام می‌پذیرد. نکته دیگر اینکه می‌توان اطلاعات ثبت شده و همینطور آرشیو فایلهای ثبت رخدادها را مستقیما از طریق "ESS" مشاهده نمود.




بدین منظور کافی است بر روی گزینه "tools" منوی اصلی نرم افزار کلیک کرده و گزینه "log files" را برگزینید. پس از این کار می‌توانید نوع فایل ثبت رخدادهای مورد نظر را از منوی بازشونده "log:" انتخاب کنید. انواع فایلهای ثبت رخداد عبارتند از:

۱- فایل ثبت رخدادهای مربوط به تهدیدات شناسایی شده

برای مشاهده تهدیدات شناسایی شده از این گزینه استفاده می‌گردد.

۲- فایل ثبت وقایع

این گزینه برای مدیران سیستم و کاربران حرفه‌ای جهت حل مشکلات حادث شده طراحی گردیده است. ضمن اینکه تمامی عملکردهای مهم "ESS" در این نوع فایل ثبت می‌شود.

۳- فایل ثبت رخدادهای مربوط به پویش دستی رایانه

نتایج مربوط به تمامی پویش هایی که به صورت کامل انجام پذیرفته‌اند در این نوع فایل قابل مشاهده هستند. برای مشاهده جزئیات هر یک از این فایلها کافی است بر روی فایل مورد نظر کلیک چپ مضاعف نمائید.

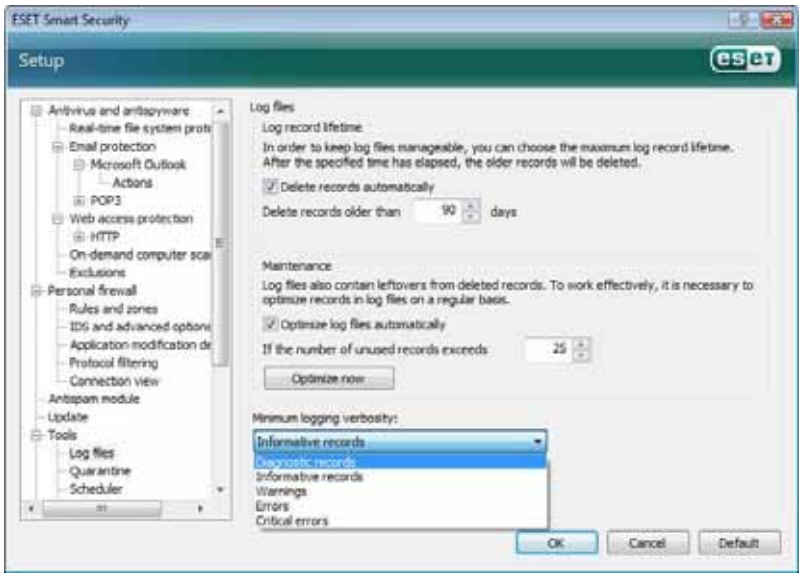
۴- فایل ثبت رخدادهای مربوط به دیواره آتش شخصی "ESET"

این فایل نیز شامل تمامی اطلاعات و تهدیدات شناسایی شده توسط دیواره آتش شخصی "ESET" است. بررسی این فایل می‌تواند در جهت شناسایی نقاط نفوذ سیستم رایانه‌ای و جلوگیری از دسترسی افراد غیرمجاز سودمند باشد.

صرف نظر از نوع هر یک از فایل‌های ثبت رخداد می‌توان اطلاعات مربوطه را با کلیک بر روی دکمه "copy" به حافظه موقت "clipboard" کپی نمود. ضمن اینکه برای انتخاب چند فایل نیز می‌توان از کلیدهای "shift" و یا "ctrl" صفحه کلید استفاده به عمل آورد.

### ۱-۷-۴- نگهداری از فایلهای ثبت رخداد

جهت پیکربندی ثبت رخدادها کافی است با فشردن کلید "F5" پنجره تنظیمات پیشرفته "ESS" را گشوده و پس از کلیک بر روی گزینه "tools" مبادرت به انتخاب گزینه "log file" نمائید.




گزینه‌های پیکربندی ثبت رخدادها عبارتند از:

۱- پاک کردن خودکار رکوردها

با استفاده از این گزینه می‌توانید زمان مورد نظری که لازم است سپری شود تا فایل‌های ثبت رخدادهای قدیمی به صورت خودکار حذف شوند را مشخص کنید.

۲- بهینه سازی خودکار فایل های ثبت رخداد

این گزینه جهت مرتب کردن (defragmentation) فایلهای ثبت رخداد در زمانی که درصد ذکر شده مربوط به عدم استفاده از رکوردها تحقق پذیرد، مورد استفاده قرار می‌گیرد.

۳- موارد ثبت شونده

جهت مشخص کردن سطح "logging verbosity" مورد استفاده قرار می‌گیرد. گزینه‌های موجود در اینجا عبارتند از:

الف) خطاهای بحرانی

صرفا خطاهای بحرانی مربوط به ماژول ضد ویروس، دیواره آتش شخصی و ... را ثبت می‌کند.

ب) خطاها

علاوه بر خطاهای بحرانی، خطاهای مربوط به دانلود فایلها را نیز ثبت می‌کند.

ج) هشدارها

علاوه بر خطاهای بحرانی، پیغام‌های هشدار نرم افزار را ثبت می‌کند.

د) رکوردهای اطلاع رسانی

تمامی رکوردها به علاوه پیام‌های اطلاع رسانی نرم افزار از قبیل پیام‌های مربوط به بروزرسانی نرم افزار را ثبت می‌کند.

هـ) رکوردهای تشخیصی (diagnostic records)

تمامی رکوردها به علاوه اطلاعات مورد نیاز جهت تنظیم بهینه نرم افزار را ثبت می‌نماید.

### ۸-۴- رابط گرافیکی کاربر

گزینه‌های مربوط به پیکربندی رابط گرافیکی کاربر را می‌توان با توجه به نیازهای کاربر تنظیم نمود. برای دسترسی به این گزینه‌ها کافی است کلید "F5" را فشرده و سپس گزینه "user interface" را در قسمت سمت چپ پنجره برگزینید تا اطلاعات مربوطه در پنجره به نمایش در آیند. در قسمت "user interface elements" می‌توان نمای نرم افزار را در حالت پیشرفته تنظیم نمود. در حالت یا مد پیشرفته گزینه‌های بیشتری در خصوص کنترل نرم افزار "ESS" در اختیار کاربر قرار می‌گیرد.

همچنین اگر المانهای گرافیکی باعث کاهش سرعت رایانه می‌گردند نیز می‌توان گزینه "graphical user interface" را غیر فعال نمود. توصیه می‌شود این گزینه در زمانی که کاربر به لحاظ بصری دچار مشکلاتی است و از نرم افزارهای ویژه‌ای جهت حل مشکل خود استفاده می‌کند نیز غیر فعال گردد.

برای غیرفعال کردن نمایش پنجره مربوط به "ESS" در زمان راه‌اندازی رایانه می‌توان گزینه

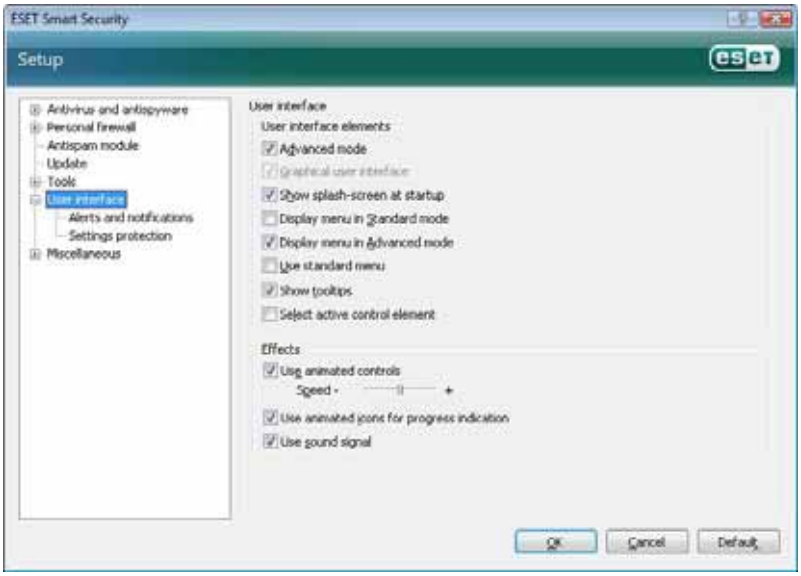
"show splash–screen at startup"

را غیر فعال کرد.

برای فعال یا غیر فعال کردن منوی استاندارد بالای پنجره "ESS" نیز می‌توان از گزینه "use standard menu" استفاده به عمل آورد. همچنین اگر گزینه "show tool tips" فعال باشد، در زمان قرار گرفتن ماوس بر روی هر یک از ابزار نرم افزار پنجره کوچکی نمایان شده و اطلاعاتی را در مورد ابزار مورد نظر در اختیار کاربر قرار می‌دهد.

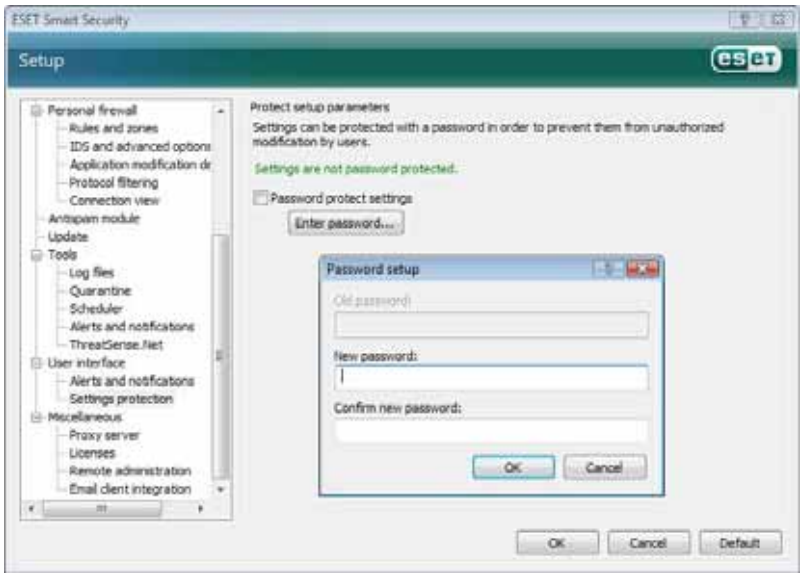
فعال نمودن گزینه "select active control element" نیز باعث می‌شود هر یک از المانهایی که در منطقه فعال نشانگر ماوس هستند، های لایت گردند. ضمن اینکه پس از کلیک ماوس، آیتم های لایت شده فعال می‌گردد. جهت افزایش و یا کاهش سرعت افکت‌های انیمیشنی نیز می‌توان از گزینه "animated controls" و همچنین اسلاید بار "speed" استفاده نمود.

جهت فعال ساختن آیکون‌های انیمیشنی نشان دهنده پیشرفت هر یک از عملکردهای نرم افزار نیز کافی است گزینه "use animated icons" را انتخاب نمائید. همچنین اگر می‌خواهید نرم افزار از طریق هشدار صوتی وقوع رخدادهای مهم را به اطلاع کاربر برساند نیز می‌توانید گزینه "use sound signal" را برگزینید.




علاوه بر مطالب ذکر شده در قسمت ویژگی‌های رابط گرافیکی کاربر نرم افزار (user interface) می‌توانید برای حفاظت از پارامترهای تنظیمات نرم افزار یک کلمه عبور تعریف نمائید. برای دسترسی به تنظیمات این گزینه لازم است به زیر منوی "settings protection" از منوی "user interface" مراجعه کنید. توجه داشته باشید که ضروری است جهت دستیابی به حداکثر حفاظت رایانه‌ای تمامی تنظیمات نرم افزار را به صورت صحیح انجام دهید. ضمن اینکه می‌بایست از دسترسی افراد غیرمجاز جهت انجام تغییرات بر روی تنظیمات"ESS" جدا جلوگیری به عمل آورید تا اطلاعات رایانه‌ای تحت الشعاع تخریب و یا

آلودگی قرار نگیرند. در گام بعدی جهت درج کلمه عبور برای حفاظت از تنظیمات نرم افزار بر روی دکمه "enter password" کلیک نمائید.




### ۱-۸-۴- پیام‌های هشدار و آگاهی رسانی نرم افزار

گزینه "alerts and notifications setup" موجود در قسمت "user interface" به کاربر امکان می‌دهد تا بتواند پیکربندی تنظیمات مربوط به پیام‌های هشدار و همچنین پیام‌های آگاهی رسانی "ESS" را پیکربندی نماید.

اولین آیتم در این قسمت گزینه "display alerts" است. غیر فعال کردن این گزینه باعث لغو شدن نمایش پنجره‌های هشدار نرم افزار گردیده و صرفا در موارد بسیار خاص به هیچ وجه توصیه نمی‌گردد. لذا جهت اکثر کاربران توصیه می‌شود تا این گزینه در حالت پیش فرض (فعال) خود قرار داشته باشد.

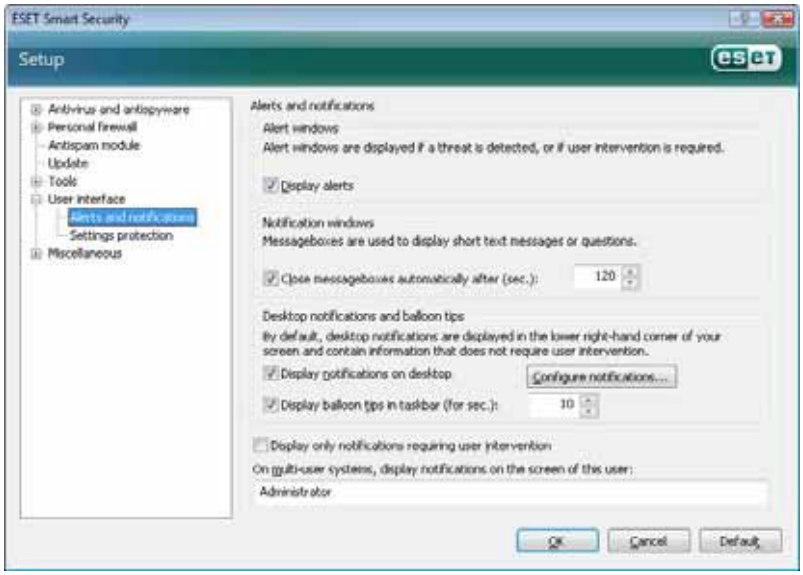
جهت بسته شدن خودکار پیامهای هشدار نرم افزار پس از گذشتن یک مدت زمان از قبل تعریف شده می‌توانید از گزینه "close message boxes automatically after (sec.)" استفاده به عمل آورید. پس از درج مدت زمان مورد نظر بر حسب ثانیه، اگر پنجره پیام یا هشدار نرم افزار قبل از سپری شدن این زمان به صورت دستی بسته نشود، با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

توجه داشته باشید که پیام‌های آگاهی رسانی و همچنین بالن‌های حاوی نکات مهم صرفا جنبه اطلاع رسانی داشته و لذا تداخلی با امور جاری کاربر ندارند و نیازی نیست که کاربر نسبت به بستن آن‌ها و ... کاری انجام دهد. این پنجره‌ها در قسمت گوشه سمت راست صفحه نمایش نشان داده می‌شوند. جهت فعال شدن قابلیت نمایش پنجره‌های آگاهی رسانی بر روی میز کار رایانه (desktop) کافی است گزینه

"display notifications on desktop"

را انتخاب نمائید. جهت انجام تنظیمات بیشتر مربوط به این پیام‌ها نیز کافی است بر روی گزینه "configure notifications" کلیک نمائید. همچنین می‌توانید جهت مشاهده پیش نمایش پیام‌های آگاهی رسانی بر روی دکمه

"preview" کلیک کنید. جهت پیکربندی دوره زمانی نمایش بالن‌های حاوی نکات مهم نیز کافی است از گزینه "display balloon tips in taskbar (sec.)" استفاده به عمل آورید.




در قسمت تحتانی پنجره تنظیمات "alerts and notifications" گزینه‌ای به عنوان

"display only notifications requiring user intervention"

قرار دارد.

این گزینه به کاربر امکان می‌دهد نمایش هشدارها و پیام‌هایی که به مداخله کاربر نیازی ندارند را فعال یا غیرفعال نماید. آخرین گزینه در این قسمت مشخص کردن آدرسهای پیام‌های هشدار در یک محیط چند کاربره می‌باشد.

فیلد "on multi–user systems , display notifications requiring user intervention" به مدیر سیستم یا شبکه امکان می‌دهد کاربر گیرنده پیام‌های هشدار نرم افزار را مشخص نماید. این گزینه در زمانی که از ترمینال سرورها استفاده به عمل می‌آید بسیار مفید می‌باشد. زیرا در این حالت تمامی پیام‌های آگاهی رسانی به مدیر سیستم یا شبکه ارسال می‌گردند.

### ۹-۴- فناوری ThreatSense.net

"ThreatSense.net" یک سیستم هشدار اولیه است که سبب می‌گردد شرکت "ESET" در اولین فرصت و به طور مستمر از وجود آخرین و جدیدترین تهدیدات رایانه‌ای آگاهی حاصل نماید. این سیستم هشدار اولیه دو طرفه (bidirectional) دارای یک هدف واحد است و این هدف چیزی جز افزایش حفاظت رایانه‌ای کاربران نیست. چرا که حصول اطمینان از کسب آگاهی نسبت به ایجاد و گسترش تهدیدات جدید در اولین فرصت ممکن و همچنین تولید پادزهرهای آنها جز با ارتباط مستمر با کاربران "ESS" محقق نمی‌گردد.

در ارتباط با "ThreatSense .net" دو گزینه وجود دارد:

الف) عدم فعال کردن سیستم هشدار اولیه

نرم افزار در حالت غیر فعال بودن این گزینه به هیچ وجه کارایی خود را از دست نمی‌دهد و کاربر کماکان از حداکثر حفاظت رایانه‌ای "ESET" برخورد خواهد بود.

ب) فعال کردن سیستم هشدار اولیه

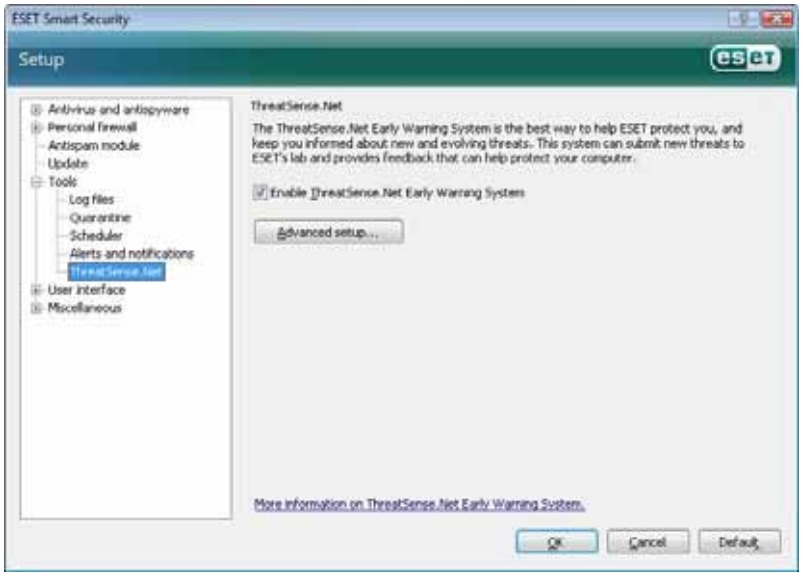
کاربران می‌توانند "ThreatSense.net " را جهت ارسال اطلاعات عمومی در خصوص تهدیدات رایانه‌ای جدید در کنار نمونه فایلهای حاوی کدهای مخرب جهت تجزیه و تحلیل به لابراتوارهای ضدویروس "ESET" ارسال نمایند.

مطالعه این تهدیدات توسط شرکت "ESET" باعث می‌شود تا این شرکت بتواند روشهای مقابله با آنها را در قالب فایلهای بروزرسانی نرم افزار در اختیار کاربران قرار دهد.

در واقع سیستم هشدار اولیه "ThreatSense.net" اطلاعات مرتبط با تهدید شناسایی شده جدید در رایانه کاربر را اعم از فایل دارای کد مخرب و یا نسخه‌ای از آن، مسیر فایل، نام فایل، اطلاعات مربوط به تاریخ و زمان فایل، پروسه مرتبط با فایل و نهایتا سیستم عامل رایانه را جمع‌آوری کرده و به شرکت "ESET" ارسال می‌کند. ضمن اینکه برخی از این اطلاعات می‌تواند شامل اطلاعات شخصی کاربر نیز باشد. به عنوان مثال می‌توان به شناسه کاربری کاربر اشاره کرد.

لذا با توجه به اینکه ممکن است در اطلاعات ارسالی به شرکت "ESET" اطلاعات شخصی کاربران نیز وجود داشته باشد، شرکت "ESET" به تمامی کاربران خود اطمینان داده است که از اطلاعات ارسالی صرفا جهت امور تحقیقاتی مربوط به مبارزه با تهدیدات رایانه‌ای جدید استفاده خواهد گردید.

به صورت پیش فرض، "ESET" به گونه‌ای پیکربندی شده است که قبل از ارسال اطلاعات مربوط به یک فایل مشکوک به آلودگی از کاربر اتخاذ تصمیم می‌کند. یادآوری این نکته ضروری است که فایلهای اسنادی از قبیل فایلهای ".doc" و ".xls" همواره از فهرست فایلهای مشکوک به آلودگی جهت ارسال به "ESET" به صورت خودکار حذف می‌گردند. لذا اگر کاربر دارای فایلهای خاص دیگری است که در صورت مشکوک بودن آنها به آلودگی ویروسی تمایلی به ارسال آنها به لابراتوارهای "ESET" ندارد، لازم است این نوع فایلها را در فهرست موجود در "ESS" درج نماید.



تنظیمات مربوط به "ThreatSense.net" در قسمت تنظیمات پیشرفته (کلید F5) قرار دارد. بدین منظور کافی است بر روی گزینه "tools" کلیک کرده و سپس گزینه "ThreatSense.net" را برگزینید. پس از آن می‌توانید گزینه

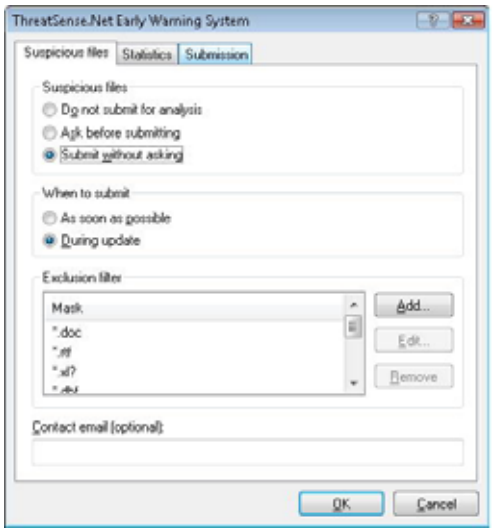
"enable ThreatSense.net early warning system"

را در سمت راست پنجره تنظیمات پیشرفته فعال نمائید. جهت انجام تنظیمات پیشرفته مربوط به سیستم هشدار اولیه نیز می‌توانید بر روی گزینه "advanced setup..." کلیک کنید تا پنجره مربوط به آن گشوده گردد.

### ۱-۹-۴- فایلهای مشکوک به آلودگی ویروسی

پنجره تنظیمات پیشرفته سیستم هشدار اولیه دارای سه برگ نشان است که یکی از آنها عبارت از برگ نشان "suspicious files"می‌باشد. با استفاده از گزینه‌های موجود در پنجره این برگ نشان می‌توانید چگونگی ارسال فایلهای مشکوک به آلودگی به شرکت "ESET" را پیکربندی نمائید.

همانطور که می‌دانید اگر در رایانه یک فایل مشکوک به آلودگی شناسایی شود، امکان ارسال آن به منظور تجزیه و تحلیل به لابراتوارهای "ESET" فراهم گردیده است. اگر پس از انجام بررسی‌های لازم بر روی فایل مشکوک، صحت آلودگی ویروسی فایل ارسالی تائید شود، روش مقابله با آن در قالب فایلهای بروزرسانی نرم افزار برای تمامی کاربران در دسترس قرار خواهد گرفت.




ویژگی ارسال فایلها به شرکت "ESET" را می‌توان بر روی حالت خودکار تنظیم نمود. اگر این حالت انتخاب شود، فایلهای مشکوک به آلودگی به صورت خودکار و در پس زمینه کار رایانه ارسال خواهند گردید. همچنین اگر کاربر تمایل داشته باشد که قبل از ارسال فایل مشکوک به آلودگی از نوع فایل و اطلاعات دیگر مربوطه آگاهی حاصل کند، می‌تواند گزینه "ask before submitting" را انتخاب نماید.

همچنین اگر در نظر دارید که هیچ فایل مشکوکی به لابراتوارهای "ESET" ارسال نگردد نیز می‌توانید گزینه "do not submit for analysis" را برگزینید. توجه داشته باشید که عدم ارسال فایلهای مشکوک به "ESET" به معنی عدم ارسال اطلاعات آماری نرم افزار به این شرکت نمی‌باشد. لازم است تنظیمات مربوط به اطلاع آماری را در برگ نشان "statistics" به انجام رسانید. این تنظیمات در بخش ۲-۹-۴ مورد بررسی قرار می‌گیرند.

دیگر قسمتهای موجود در برگ نشان "suspicious files" عبارتند از:

الف) زمان ارسال (when to submit)

در اینجا دو حالت وجود دارد. کاربر می‌تواند با انتخاب گزینه "as soon as possible" شرائطی را فراهم آورد تا فایلهای مشکوک در اولین فرصت ممکن ارسال گردند. این حالت برای زمانی که کاربران از یک ارتباط اینترنت دائمی بهره مند هستند توصیه می‌گردد.

حالت دیگر موجود عبارت از ارسال فایلها در زمان بروزرسانی نرم افزار (during update) است. اگر این گزینه انتخاب شود، فایلهای مشکوک به آلودگی پس از جمع‌آوری در زمان بروزرسانی نرم افزار ارسال خواهند گردید.

ب) فیلتر حذف (exclusion filter)

کاربران می‌توانند با استفاده از این ویژگی فایلهایی که تمایلی به ارسال آنها ندارند را مشخص نمایند. به صورت پیش فرض برخی از فایلهای اسنادی در فهرست حذف از ارسال ثبت گردیده‌اند و کاربر می‌تواند در صورت نیاز انواع دیگری از فایلها را به این فهرست اضافه کند.

ج) آدرس پست الکترونیک (contact email)

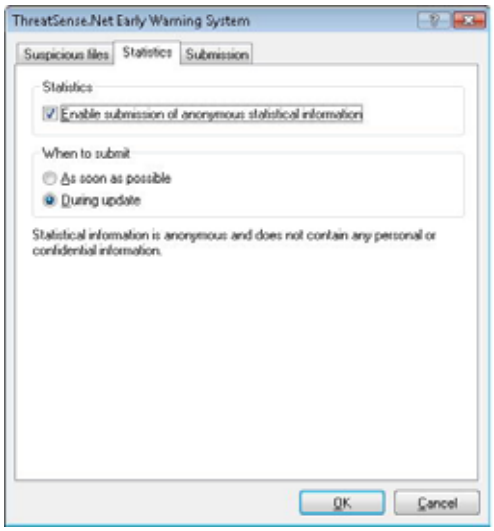
آدرس پست الکترونیکی ثبت شده در این قسمت در کنار فایلهای مشکوک به "ESET" ارسال می‌گردد تا اگر شرکت "ESET" نیاز به جزئیات بیشتری جهت تجزیه و تحلیل آیتم‌های دریافتی داشت، از طریق این آدرس بتواند با کاربر ارتباط برقرار نماید. توجه داشته باشید که صرفا این آدرس در زمان نیاز به اطلاعات بیشتر از طرف "ESET" مورد استفاده قرار می گیرد و لذا در شرائط معمول جوابی در پاسخ اطلاعات فرستاده شده برای کاربر ارسال نخواهد گردید.

### ۲-۹-۴- برگ نشان اطلاعات آماری (statistics)

سیستم هشدار اولیه مبادرت به جمع‌آوری اطلاعات مرتبط با فایل مشکوک به آلودگی شناسایی شده می‌نماید. این اطلاعات می‌تواند شامل نام تهدید شناسایی شده، نگارش سیستم عامل رایانه کاربر، نگارش "ESS" نصب شده بر روی رایانه کاربر و تنظیمات مربوط به محل نگهداری فایل مشکوک به آلودگی بر روی رایانه کاربر باشد.

این اطلاعات معمولا یک یا دو بار در روز به سرورهای "ESET" ارسال می‌گردند. نمونه‌ای از این اطلاعات ارسالی در ذیل آمده است:

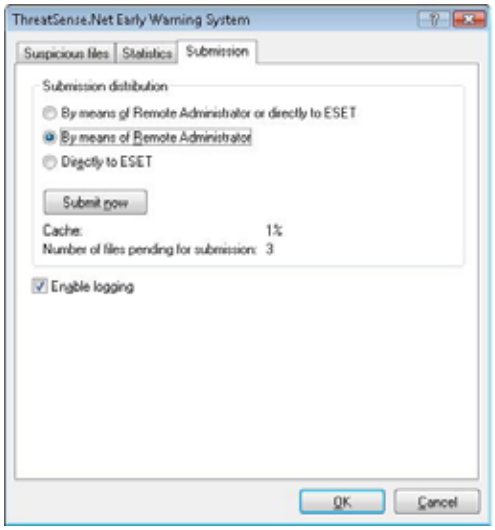
**# utc_time=2005-04-14 07:21:28**
**# country=“Slovakia“**
**# language=“ENGLISH“**
**# osver=5.1.2600 NT**
**# engine=5417**
**# components=2.50.2**
**# moduleid=0x4e4f4d41**
**# filesize=28368**
**# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1463[1].exe**




یکی دیگر از گزینه‌های موجود در برگ نشان "statistics" قسمت "when to submit" است. توضیحات مربوط به این قسمت همانند توضیحات مرتبط در برگ نشان "suspicious files" می‌باشد.

### ۴-۹-۳- برگ نشان ارسال (submission)

در این برگ نشان کاربر می‌تواند مشخص کند که فایلهای مشکوک به آلودگی و اطلاعات آماری مرتبط با آنها توسط مدیر از راه دور "ESET" (ESET remote administrator) ارسال گردند و یا مستقیما به "ESET" ارسال شوند. اگر صرفا ارسال این فایلها به همراه اطلاعات مربوطه مد نظر کاربر باشد می‌تواند گزینه"by means of remote administrator or directly to ESET" را برگزینید. اگر این گزینه انتخاب شود، فایلها به همراه اطلاعات آماری با هر وسیله ممکن ارسال خواهند شد. توجه داشته باشید که ارسال فایلها به وسیله مدیر از راه دور موجب ارسال فایلها و اطلاعات آماری مربوطه به سرور مدیریت از راه دور خواهد شد. لذا انتخاب این گزینه باعث حصول اطمینان از ارسال بعدی این فایلها به لابراتورهای "ESET" می‌گردد.




همچنین اگر گزینه "directly to ESET" انتخاب گردد، تمامی فایلهای مشکوک به همراه اطلاعات آماری مربوطه مستقیما از طریق نرم افزار به لابراتورهای "ESET" ارسال خواهند گردید.

علاوه بر مطالب ذکر شده اگر فایلهای مشکوکی وجود داشته باشند که در صف انتظار جهت ارسال قرار دارند، دکمه "submit now..." فعال می‌گردد و کاربر با کلیک بر روی این دکمه می‌تواند نسبت به ارسال فایلهای مشکوک به آلودگی به همراه اطلاعات آماری مربوطه اقدام نماید. ضمن اینکه تیک زدن گزینه "enable logging" موجب ثبت اطلاعات مربوط به فایلهای ارسالی و اطلاعات آماری آنها خواهد گردید. در واقع پس از ارسال، اطلاعات فایل مشکوک و بخشی از اطلاعات آماری آن در یک فایل ثبت می‌شود.

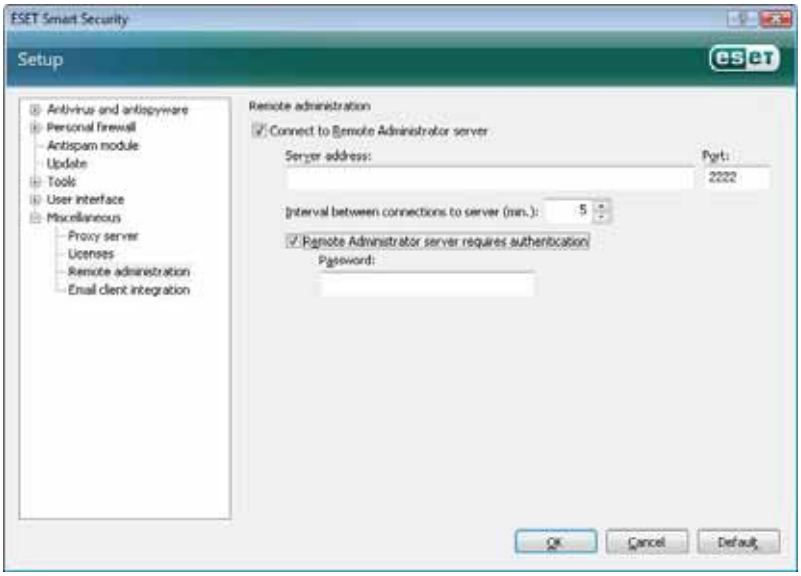
### ۴-۱۰- مدیریت از راه دور

ویژگی مدیریت از راه دور (remote administration) ابزار قدرتمندی برای حفظ سیاست امنیتی و همچنین کسب آگاهی کلی از مدیریت امنیتی در یک شبکه رایانه‌ای است. مزیت استفاده از این ویژگی در شبکه‌های رایانه‌ای بزرگ ملموس‌تر خواهد بود. این ویژگی

نه تنها سطح امنیتی را افزایش می‌دهد بلکه باعث راحتی مدیریت "ESS" نصب شده بر روی ایستگاه‌های کاری موجود در شبکه می‌گردد.

تنظیمات مربوط به مدیریت از راه دور در پنجره اصلی "ESS" قابل دسترسی است. بدین منظور کافی است بر روی گزینه "setup" کلیک کرده و سپس وارد پنجره تنظیمات پیشرفته نرم افزار ( دکمه F5) گردید. پس از آن می‌توانید بر روی گزینه "miscellaneous" کلیک نموده و زیر منوی "remote administration" را برگزینید.

در سمت راست پنجره امکان فعال یا غیر فعال نمودن این ویژگی فراهم آمده است. بدین منظور از گزینه "connect to remote administration server" استفاده می‌شود. پس از انتخاب این گزینه می‌توانید نسبت به انجام تنظیمات دیگر که در ذیل آمده‌اند اقدام نمایید:




الف) آدرس سرور (server address)

در این قسمت لازم است آدرس سروری که سرور مدیریت از راه دور بر روی آن نصب گردیده است را درج کنید.

ب) شماره پورت

این فیلد شامل شماره پورت از پیش تعریف گردیده جهت برقراری ارتباط است. توصیه می‌شود از پورت پیش فرض ۲۲۲۲ استفاده گردد.

ج) فاصله‌های زمانی جهت برقراری ارتباط با سرور (برحسب دقیقه)

فاصله زمانی مورد نظر جهت ارسال اطلاعات توسط "ESS" به سرور راه دور (ERA) در این قسمت درج می‌شود. به بیان دیگر اطلاعات ارسالی به سرور راه دور هر بار پس از سپری شدن زمان درج شده در این قسمت ارسال می‌شوند. اگر در این فیلد مقدار صفر درج شود، اطلاعات ارسالی در هر ۵ ثانیه ارسال می‌شوند.

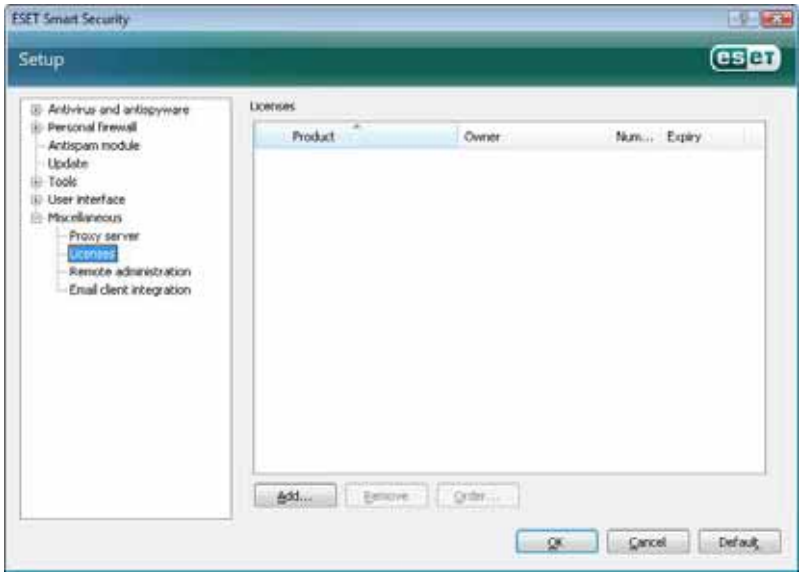
د) تائید اعتبار جهت ارتباط با سرور مدیریت از راه دور

در صورت نیاز می‌توان شناسه کاربری و کلمه عبور جهت برقراری ارتباط با سرور راه دور را در این قسمت درج نمود.

پس از انجام تنظیمات ذکر شده کافی است برای تائید آنها بر روی دکمه "OK" کلیک کنید تا "ESS" از این تنظیمات برای برقراری ارتباط با سرور مدیریت از راه دور استفاده کند.

### ۱۱-۴- مجوز استفاده از نرم افزار

در قسمت "license" می‌توان مجوزهای استفاده از نرم افزار مربوط به هر یک از محصولات شرکت "ESET" اعم از "ESS"، "ERA" نگارش ضدویروس "nod32" برای سرور "Microsoft Exchange" و ... را مدیریت نمود. همانطور که می‌دانید پس از خرید نرم افزار، مجوز استفاده از نرم افزار در قالب شناسه کاربری و کلمه عبور در اختیار کاربران قرار می‌گیرد.




لذا جهت اضافه نمودن و یا حذف یک فایل مجوز استفاده از نرم افزار می‌توانید از دکمه‌های مرتبط در پنجره مدیریت مجوزها استفاده کنید. این پنجره از طریق زیر منوی "licenses" موجود در قسمت "miscellaneous" قابل دسترسی می‌باشد.

فایل مجوز استفاده از نرم افزار یک فایل متنی است (text file) که شامل اطلاعاتی از جمله محصول خریداری شده، نام مالک نرم افزار، تعداد مجوزها و تاریخ انقضای مجوز می‌باشد. جهت افزودن یک فایل مجوز از دکمه "add..." و برای حذف از دکمه "remove" استفاده می‌شود.

همچنین اگر یک فایل مجوز استفاده از نرم افزار انقضاء یابد و کاربر تمایل به خرید مجدد داشته باشد می‌تواند با کلیک بر روی دکمه "order..." به صورت خودکار به فروشگاه اینترنتی دسترسی پیدا نماید.

### ۵- کاربران حرفه‌ای

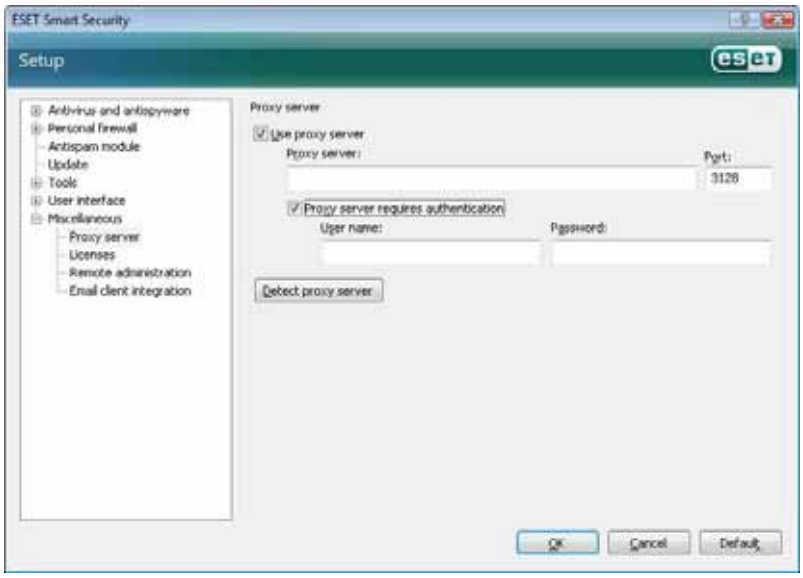
در این بخش به ویژگی‌هایی از "ESS" اشاره می‌شود که ممکن است برای کاربران حرفه‌ای بسیار مفید باشند. تنظیمات گزینه‌های مورد بحث صرفا در حالت پیشرفته (advanced mode) انجام می‌پذیرد. لذا جهت فعال کردن این مد کافی است بر روی گزینه "toggle advanced mode" در پائین سمت چپ پنجره نرم افزار کلیک کنید و یا از کلیدهای ترکیبی "ctrl+m" استفاده نمائید.

### ۱-۵- تنظیمات مربوط به سرور "proxy"

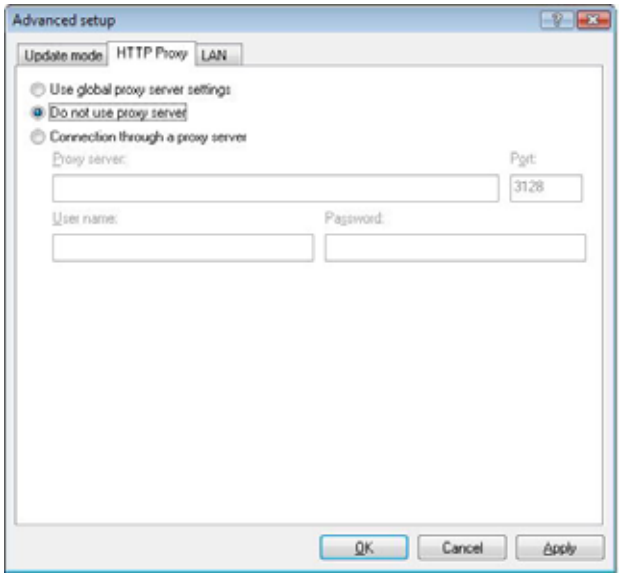
در "ESS" تنظیمات مربوط به سرور "proxy" در ۲ زیر قسمت ساختار درختی تنظیمات پیشرفته در دسترس کاربران حرفه‌ای قرار گرفته است.

اولین قسمت عبارت از زیر منوی "proxy server" موجود در بخش "miscellaneous" می باشد. درج و انجام تنظیمات سرور "proxy" در این سطح به معنای انجام تنظیمات کلی سرور "proxy" برای تمامی "ESS" است. به بیان دیگر در اینجا پارامترهای

تنظیم شده توسط تمامی ماژولهای "ESS" که نیاز به برقراری ارتباط اینترنتی دارند، مورد استفاده قرار می‌گیرند. لذا در اینجا صرفا کافی است گزینه "use proxy server" را تیک زده و آدرس سرور را به همراه شماره پورت ارتباطی در فیلدهای مرتبط درج کنید.

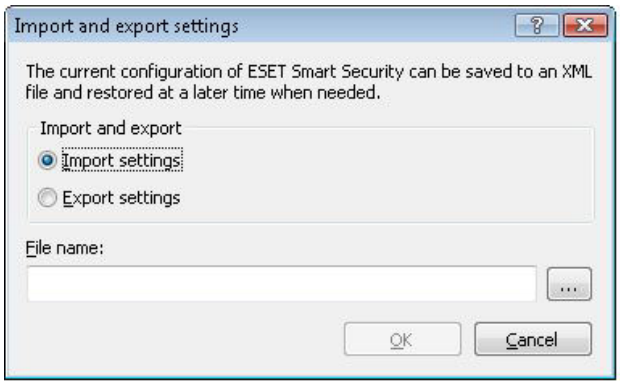



همچنین اگر برقراری بستر ارتباطی با سرور "proxy" مستلزم تائید اعتبار می‌باشد، لازم است گزینه "proxy server require authentication" را تیک زده و شناسه کاربری را به همراه کلمه عبور در فیلدهای مربوطه درج نمائید. ضمن اینکه می‌توان با کلیک بر روی گزینه "detect proxy server" نسبت به شناسایی و درج اطلاعات سرور "proxy" به صورت خودکار اقدام نمود. در این حالت تنظیمات سرور "proxy" نرم افزار "Internet Explorer" در فیلدهای مورد نظر کپی خواهند شد. توجه داشته باشید که در حالت اخیر اطلاعات و تنظیمات سرور "proxy" کپی می‌شوند و لازم است اطلاعات مربوط به تائید اعتبار توسط کاربر و به صورت دستی درج گردند.




روش دیگر درج اطلاعات مربوط به سرور "proxy" استفاده از تنظیمات پیشرفته بروزرسانی نرم افزار (گزینه update در ساختار درختی تنظیمات پیشرفته) است. این تنظیمات صرفا مرتبط با پروفایل مورد نظر بوده و برای رایانه‌های همراه توصیه می‌گردد. چرا که بروزرسانی بانک اطلاعاتی شناسه ویروسهای آنها ممکن است در مکانهای مختلف انجام پذیرد و لذا وجود پروفایلی برای هر یک از مکانها (با توجه به تنظیمات proxy مربوطه) امری است که کمک شایانی به کاربران می‌کند. جهت کسب اطلاعات بیشتر در این خصوص می‌توانید به بخش ۴-۴ مراجعه کنید.

### ۲-۵- "export/import" نمودن تنظیمات




ویژگی "export/import" نرم افزار "ESS" در مد پیشرفته به عنوان زیر مجموعه‌ای از گزینه "setup" در دسترس کاربران قرار گرفته است. در هر دو حالت "import" و "export" از فایلهای ".xml" استفاده می‌شود. این ویژگی‌ها جهت پشتیبان گیری از پیکربندی جاری "ESS" برای استفاده‌های آتی کاربرد دارند. ویژگی "export" برای کاربرانی که قصد دارند تنظیمات انجام شده بر روی "ESS" یک رایانه را بر روی رایانه‌های دیگر (به صورت مشابه) انجام دهند، بسیار مورد توجه می‌باشد. چرا که کافی است فایل ".xml" تولید شده (طی فرایند export) را در "ESS" کلاینت‌های دیگر "import" (وارد) نمایند.

### ۱-۲-۵- تنظیمات مربوط به "export" نمودن پیکربندی "ESS"

"export" (یا صادر نمودن) پیکربندی "ESS" بسیار ساده است. بدین منظور کافی است بر روی "setup" کلیک کرده و گزینه "import and export settings" را برگزینید. سپس گزینه "export settings" را انتخاب نموده و نهایتا نامی را برای فایل خروجی ".xml" درج نمائید. در انتها نیز می‌توانید مسیر ذخیره سازی فایل مورد نظر را مشخص کنید.

### ۲-۲-۵- تنظیمات مربوط به "import" نمودن پیکربندی "ESS"

مراحل این کار شبیه مراحل "export" نمودن است. در اینجا کافی است پس از انتخاب گزینه"import and export settings" گزینه "import settings" را برگزیده و سپس بر روی دکمه "..." کلیک نمائید و پس از فراخوانی فایل مورد نظر، آن را "import" کنید.

### ۳-۵- خط فرمان

این امکان فراهم آمده است تا کاربران بتوانند ماژول ضدویروس "ESS" را از طریق خط فرمان (command line) به دو صورت دستی (با دستور ecls) و یا به وسیله یک "batch file" اجرا نمایند.

در ادامه به بررسی پارامترها و سوئیچ‌هایی که می‌توان از آنها برای طراحی دستی پویشگر ضدویروس از طریق خط فرمان استفاده به عمل آورد پرداخته می‌شود:

الف: تنظیمات عمومی

| پارامتر | توضیحات |
|---|---|
| help | نمایش راهنما و پایان بخشیدن به کار |
| version | نمایش اطلاعات مربوط به نگارش و پایان بخشیدن به کار |
| base-dir= FOLDER | بارگذاری ماژولها از یک پوشه خاص |
| quar-dir= FOLDER | پوشه قرنطینه |
| aind | نمایش نشان گر فعالیت (عملکرد) |

ب) آیتم‌های مورد نظر جهت پویش

| پارامتر | توضیحات |
|---|---|
| files | پویش فایلها (حالت پیش فرض) |
| no-files | عدم پویش فایلها |
| boots | پویش سکتورهای راه‌اندازی (حالت پیش فرض) |
| no-boots | عدم پویش سکتورهای راه‌اندازی |
| arch | پویش آرشیوها (حالت پیش فرض) |
| no-arch | عدم پویش آرشیوها |
| max-archive-level= LEVEL | بالاترین سطح تو در تویی (nesting) آرشیو |
| scan-timeowt= LIMIT | درج زمان حداکثر زمان مورد نظر برای یک فایل آرشیو |
| max-arch-size= SIZE | پویش اولین فایل دارای اندازه ذکر شده در یک فایل آرشیو |
| mail | پویش نامه‌های الکترونیک |
| no-mail | عدم پویش نامه‌های الکترونیک |
| sfx | پویش آرشیوهای خود اجرا |
| no-sfx | عدم پویش آرشیوهای خود اجرا |
| rtp | پویش "runtime packer" ها |
| no-rtp | عدم پویش "runtime packer" ها |
| exclude= FOLDER | حذف یک پوشه از فرایند پویش |
| subdir | پویش زیر پوشه‌ها (حالت پیش فرض) |
| no-subdir | عدم پویش زیرپوشه ها |

| | |
|---|---|
| max–subdir-level =LEVEL | بالاترین سطح تو در تویی (nesting) زیر پوشه |
| symlink | ادامه و دنبال نمودن لینک‌های سیمبولیک (حالت پیش‌فرض) |
| no–symlink | عدم پویش لینک‌های سیمبولیک |
| ext-remove= EXTENSIONS | حذف پسوندهایی که با ویرگول از هم جدا شده اند از فرایند پویش |
| ext-exclude= EXTENSIONS | استثنا نمودن پسوندهایی که با ویرگول از هم جدا شده اند از فرایند پویش |

ج) روش‌ها

| پارامتر | توضیحات |
|---|---|
| adware | پویش "adware" ها، جاسوس افزارها و "riskware" ها |
| no–adware | عدم پویش "adware" ها، جاسوس‌افزارها و "riskware"ها |
| unsafe | پویش نرم افزارهای کاربردی‌ای که به صورت بالقوه ناامن هستند |
| no-unsafe | عدم پویش نرم‌افزارهای کاربردی‌ای که به صورت بالقوه ناامن هستند |
| unwanted | پویش نرم افزارهای کاربردی ای که به صورت بالقوه ناخواسته هستند |
| no–unwanted | عدم پویش نرم افزارهای کاربردی ای که به صورت بالقوه ناخواسته هستند |
| pattern | استفاده از بانک اطلاعاتی شناسه ویروسها |
| no-pattern | عدم استفاده از بانک اطلاعاتی شناسه ویروسها |
| heur | فعال شدن ابزار هوش مصنوعی |
| no–heur | غیر فعال شدن ابزار هوش مصنوعی |
| adv-heur | فعال شدن ابزار هوش مصنوعی پیشرفته |
| no-adv-heur | غیر فعال شدن ابزار هوش مصنوعی پیشرفته |

د) پاکسازی آیتم‌های آلوده

| پارامتر | توضیحات |
|---|---|
| action= ACTION | انجام عکس العمل در مقابل تهدیدات شناسایی شده. عکس العمل‌های موجود عبارتند از: پاکسازی، اتخاذ تصمیم توسط کاربر و رها نمودن تهدید شناسایی شده |
| quarantine | کپی فایلهای آلوده به پوشه قرنطینه |
| no-quarantine | عدم کپی فایلهای آلوده به پوشه قرنطینه |

هـ) فایلهای ثبت رخدادها

| پارامتر | توضیحات |
|---|---|
| log-file=FILE | ثبت خروجی در یک فایل |
| log-rewrite | نوشتن بر روی فایل خروجی قبلی – حالت پیش فرض افزودن اطلاعات جدید به فایل قبلی است |
| log-all | ثبت فایلهای پاکسازی شده در کنار دیگر فایلها |
| no-log-all | عدم ثبت فایلهای پاکسازی شده (حالت پیش فرض) |

در خاتمه نیز تعدادی از کدهای خروج از پویش معرفی می‌گردند:

| کد | توضیحات |
|---|---|
| ۰ | عدم شناسایی تهدید رایانه‌ای |
| ۱ | شناسایی تهدید رایانه‌ای که پاکسازی نشده است |
| ۱۰ | تعدادی از فایلهای آلوده باقی مانده‌اند |
| ۱۰۱ | خطای آرشیو |
| ۱۰۲ | خطای دسترسی |
| ۱۰۳ | خطای داخلی |

توجه: کدهای خروج بزرگتر از ۱۰۰ بیانگر عدم پویش فایلها بوده و به منزله امکان آلوده بودن آنها می‌باشند.

## ۶- واژه نامه تخصصی

### ۱-۶- انواع تهدیدات رایانه‌ای

تهدیدات رایانه‌ای عبارت از کدهای مخربی هستند که با استفاده از آنها می‌توان به صورت غیرمجاز وارد رایانه کاربر شده و یا خساراتی را به رایانه کاربر وارد آورد.

#### ۱-۱-۶- ویروسها

ویروسها کدهای مخربی هستند که فایلهای موجود در رایانه کاربر را تخریب می‌کنند. وجه مشترک ویروسهای رایانه‌ای و ویروسهای بیولوژیکی استفاده از تکنیک‌های مشابه جهت گسترش و تکثیر است.

عمدتا ویروسهای رایانه‌ای به فایل‌های اجرایی و همچنین فایلهای اسنادی حمله می‌کنند. ضمن اینکه به منظور تکثیر نیز بدنه خود را به فایل هدف متصل می‌نمایند. به طور خلاصه چگونگی عمل یک ویروس رایانه‌ای به قرار زیر است:

پس از اجرای فایل اجرایی آلوده، ویروس خود را (قبل از فایل اجرایی اصلی) فعال کرده و وظیفه از پیش تعیین شده خود را به انجام می‌رساند. توجه داشته باشید که ویروس تا زمانی که کاربر فایل اجرایی آلوده را به صورت عمدی و یا به طور تصادفی اجرا ننموده است، قادر به اثرگذاری بر روی رایانه نخواهد بود.

ویروسهای رایانه‌ای را معمولا از دو منظر نوع فعالیت و شدت عمل طبقه بندی می‌کنند. برخی از ویروسها با توجه به توانایی آنها در پاک نمودن فایلهای موجود بر دیسک سخت کاربران بسیار خطرناک هستند.

به بیان دیگر برخی از ویروسها نیز وجود دارند که اطلاعات را تخریب (و یا حذف) نمی‌کنند و هدف از آنها صرفا خسته کردن کاربران و نمایش قدرت مهارتهای فنی نویسندگان آنها است.

نکته مهم دیگری که لازم است بدان توجه شود این است که ویروسها (در مقایسه با جاسوس افزارها و اسبهای تروا) با توجه به اینکه سود اقتصادی خاصی برای نویسندگانشان ندارند، از نرخ رشد کاهنده‌ای برخوردارند. نکته دیگر اینکه متاسفانه به اشتباه لغت "ویروس" به تمامی انواع تهدیدات رایانه‌ای اطلاق می‌شود که امروز به جای استفاده از لغت "ویروس" برای تمامی انواع تهدیدات رایانه‌ای از کلمه "malware" به معنای "برنامه‌های مخرب" استفاده می‌شود.

در زمان آلوده شدن یک فایل می‌بایست با استفاده از برنامه‌های ضدویروس فایل آلوده را به طرق مختلف (اعم از پاکسازی و ...) به حالت اولیه برگرداند. برخی از ویروسهای معروف عبارتند از: "yankee doodle" ، "tenga" و "onehalf"

### ۲-۱-۶- کرم‌های رایانه‌ای

کرم‌ها برنامه‌هایی هستند که حاوی کدهای مخرب بوده و به رایانه‌های یک شبکه حمله نموده و در سطح شبکه گسترش پیدا می‌کنند. تفاوت اصلی کرم‌ها با ویروسها این است که کرم‌ها (بر خلاف ویروسها) می‌توانند خود را تکثیر کرده و از رایانه‌ای به رایانه دیگر انتقال یابند و لذا مستقل از فایلهای رایانه‌ای و یا سکتورهای راه‌اندازی عمل می‌کنند.

ابزار گسترش کرم‌ها عبارت از نامه‌های الکترونیک و بسته‌های اطلاعات تبادلی در شبکه‌های رایانه‌ای است. بر این اساس کرم‌ها به دو روش طبقه بندی می‌شوند:

۱- کرم‌هایی که از طریق نامه‌های الکترونیک گسترش می‌یابند: این نوع کرم‌ها خود را به آدرس‌های پستی موجود در فهرست آدرس‌های پستی کاربر الحاق کرده و موجبات گسترش خود را فراهم می‌آورند.

۲- کرم‌هایی که در سطح شبکه گسترش می‌یابند: این کرم‌ها از حفره‌های امنیتی نرم افزارهای کاربردی استفاده کرده و خود را در سطح شبکه گسترش می‌دهند. بنابراین کرم‌ها نسبت به ویروسها کارآمدی بیشتری دارند. چرا که با وجود بستر اینترنت براحتی می‌توانند در ساعتهای اولیه شووع (و گاهی اوقات در چند دقیقه اول شیوع) به طرز چشمگیری گسترش یابند.

در نتیجه قابلیت تکثیر آنها بدون نیاز به داشتن میزبان و به صورت مستقل و سرعت زیاد این تکثیر باعث شده است که کرم‌ها در مقایسه با دیگر تهدیدات رایانه‌ای بتوانند خسارات بیشتری را به کاربران وارد نمایند.

نکته دیگر این که یک کرم فعال شده در سیستم می‌تواند به طرق مختلف از جمله پاک کردن فایلهای کاربران، کاهش کارایی سیستم و حتی غیر فعال ساختن برخی از برنامه‌های کاربردی موجبات ناراحتی کاربران را فراهم آورد. ضمن اینکه کرم‌ها به صورت ذاتی می‌توانند راه ورود دیگر تهدیدات رایانه‌ای را به سیستم باز نمایند.

بنابراین اگر رایانه کاربر توسط یک کرم آلوده شده باشد، توصیه می‌شود فایل دارای آلودگی پاک شود. زیرا ممکن است آن فایل حاوی کدهای مخرب باشد.

چند مورد از کرم‌های معروف عبارتند از: "lovsan/blaster , stration/warezov, bagle , netsky"

### ۳-۱-۶- اسبهای تروا

اسبهای تروای رایانه‌ای را به عنوان نوعی از تهدیدات رایانه‌ای که خود را به عنوان برنامه‌های سودمند قلمداد می‌کنند، تعریف می‌نمایند. در نتیجه کاربران با مشاهده ظاهر این برنامه‌ها، آنها را اجرا می‌کنند. این نکته مهم است که توجه داشته باشید اسب‌های تروا در گذشته از چنین روشی استفاده می‌کردند و امروزه دیگر نیازی به تغییر شکل و مخفی نمودن خود ندارند. هدف واحد آنها نفوذ راحت و سریع به سیستم‌های رایانه‌ای و انجام اهداف مخرب است. امروزه واژه اسب تروا به اصطلاحی تبدیل شده است که از آن برای تعریف هر نوع نفوذی به سیستم‌های رایانه‌ای استفاده می‌شود.

لذا چون این نوع تهدیدات دامنه وسیعی را به خود اختصاص داده است، اغلب طبقه‌بندی ای را برای آنها لحاظ می‌کنند که اهم آنها عبارتند از:

الف) دانلود کننده‌ها (downloader): کد مخربی است که توانایی دانلود دیگر کدهای مخرب را از اینترنت به رایانه کاربر دارا می‌باشد.

ب) دراپر (dropper) : نوعی اسب تروا است که باعث ورود دیگر تهدیدات رایانه‌ای به رایانه‌های در معرض آلودگی می‌گردد.

ج) بک دور (backdoor): نرم افزاری است که با هکرهای (attacker) راه دور ارتباط برقرار می‌کند و آنها را قادر می‌سازند تا بتوانند به سیستم کاربر دسترسی یافته و کنترل آن را بدست گیرند.

د) کی لاگر (keylogger) و یا (keystroke logger) : برنامه‌ای است که کلیدهای فشرده شده صفحه کلید توسط کاربر را ضبط کرده و این اطلاعات را برای هکرهای (attacker) راه دور ارسال می‌نماید.

هـ) تماس گیرنده یا دایالر (dialer) : برنامه‌ای است که هدف از طراحی آن برقراری ارتباطات ناخواسته از طریق مودم کاربر است به گونه‌ای که معمولا برقراری این ارتباطات توسط کاربر مورد آگاهی واقع نمی‌شود. با توجه به اینکه این نوع تهدید منوط به وجود مودم بر روی رایانه کاربر است، امروزه کمتر مورد استفاده هکرها قرار می‌گیرد.

معمولا اسبهای تروا دارای پسوند ".exe" هستند. لذا اگر چنین تهدیداتی را در رایانه شناسایی کردید، بهتر است آنها را پاک کنید. زیرا ممکن است حاوی کدهای مخرب باشند.

چند مورد از اسبهای تروای معروف عبارتند از: "netbus , trojandownloader, small.zl, slapper"

### ۴-۱-۶- "rootkit" ها

"rootkit" ها برنامه‌های مخربی هستند که برای هکرهای اینترنتی امکان دسترسی کامل به رایانه کاربر را فراهم می آورند. ضمن اینکه این نوع تهدیدات از دید کاربران نیز مخفی هستند. به بیان دیگر این نوع تهدیدات پس از دسترسی به سیستم، از برخی از ویژگی‌های سیستم عامل استفاده می‌کنند تا بتوانند خود را از شناسایی توسط نرم‌افزارهای ضدویروس در امان دارند. ضمن اینکه فرایندها، فایلها و اطلاعات رجیستری ویندوز را مخفی می‌کنند. بدین جهت اغلب شناسایی آنها با استفاده از تکنیک‌های معمولی غیر ممکن است. در زمان مقابله با این نوع تهدیدات دو سطح شناسایی را در نظر داشته باشید:

۱- زمانی که این نوع تهدیدات سعی در دسترسی به سیستم دارند: در این حالت غیر فعال هستند و اکثر نرم‌افزارهای ضدویروس قادرند (با فرض شناسایی آنها) آنها را از بین ببرند.

۲- زمانی که این نوع تهدیدات از دید روش‌های عادی شناسایی مخفی هستند: در اینجا است که فناوری "anti–stealth" شرکت "ESET" به کمک کاربر می آید که علاوه بر"rootkit" های غیر فعال قادر است "rootkit" های فعال را نیز شناسایی نماید.

### ۵-۱-۶- برنامه‌های تبلیغاتی یا افزودنی (adware)

منظور از "adware" ها نرم افزارهایی هستند که دارای نوعی سیستم تبلیغاتی هستند و همواره موارد تبلیغاتی خاصی را به کاربر نمایش می‌دهند. معمولا این نرم‌افزارها یک پنجره "pop-up" جدید گشوده که حاوی اطلاعات تبلیغاتی در رابطه با یک موضوع می‌باشد.

برخی از این نوع تهدیدات نیز آدرس صفحه خانگی کاربر در نرم‌افزار مرورگر وب را تغییر می‌دهند. معمولا "adware"ها در کنار نرم‌افزارهای رایگان (در واقع در دل آنها) ارائه می‌گردند و نویسندگان خود را قادر می‌سازند تا هزینه‌های توسعه برنامه‌های کاربردی (و مفید) خود را پوشش دهند.

"adware" ها به تنهایی خطرناک نیستند و صرفا کاربران را به جهت نمایش دادن پیام‌های تبلیغاتی متعدد خسته می‌کنند. نکته خطرناک در رابطه آنها این است که ممکن است هکرها از آنها به جهت مقاصد جاسوسی استفاده به عمل آورند.

بنابراین اگر تمایل به استفاده از یک نرم‌افزار رایگان (freeware) دارید، لازم است توجه خاصی به روند نصب برنامه مورد نظر داشته باشید زیرا فایل نصب کننده این برنامه‌ها طی پیام‌هایی نسبت به نصب برنامه‌های افزودنی در ضمن نصب خود به کاربر آگاهی می دهد و کاربر نیز می‌تواند با اتخاذ تصمیم در مورد عدم نصب برنامه افزودنی مانع نصب آن گردد. برخی از برنامه‌های کاربردی رایگان دیگر نیز به گونه‌ای طراحی شده‌اند که لازم است کاربر در ضمن نصب آنها، نرم افزار افزودنی پیشنهادی آن برنامه را نیز نصب کند و در صورت عدم نصب نرم افزار افزودنی در کنار نرم افزار رایگان، ممکن است کارایی نرم افزار رایگان محدود گردد. این بدان معنی است که کاربر شخصا مسیر دسترسی به سیستم خود توسط نرم افزار افزودنی را – با قبول نصب آنها در کنار نرم افزار کاربردی رایگان – فراهم می‌آورد. در نتیجه عواقب خوشایندی در انتظار کاربر نخواهد بود. پس بهتر است از نصب چنین نرم افزارهایی اجتناب به عمل آید.

### ۶-۱-۶- جاسوس افزار

این واژه تمامی نرم‌افزارهایی که اطلاعات شخصی کاربران را بدون آگاهی و اتخاذ تصمیم آنها به اشخاص غیرمجاز ارسال می‌کنند پوشش می‌دهد. این برنامه‌ها اغلب از ویژگی‌های خاصی برخوردارند که آنها را قادر می‌سازد اطلاعاتی چون نام سایتهایی که توسط کاربر بازدید گردیده‌اند، آدرس‌های پست الکترونیکی موجود در دفترچه آدرس الکترونیکی کاربر، فهرستی از دکمه‌های صفحه کلید که توسط کاربر مورد استفاده قرار گرفته‌اند و ... را در دسترس اشخاص غیرمجاز قرار دهند. تولیدکنندگان این نوع نرم افزارها (جاسوس افزارها) ادعا می‌کنند که استفاده از چنین تکنیکهایی می‌تواند باعث شناسایی نیازها و علائق کاربران شده و مسائل تبلیغاتی جهت کاربران را با اهداف دقیق‌تری پیاده نمود. اما مشکل اینجاست که هیچ تفاوت آشکاری بین جاسوس افزارها و نرم‌افزارهای مفید در زمینه مسائل تبلیغاتی و حواشی آن وجود ندارد و هیچ کس نمی‌تواند مطمئن باشد که از اطلاعاتی که بدین شکل بدست می‌آید، سوء استفاده نخواهد شد.

اطلاعات بدست آمده توسط جاسوس افزارها می‌توانند شامل کدهای امنیتی، شماره‌های شناسایی شخصی (pin) ، شماره حساب‌های بانکی و غیره باشند.

در اغلب مواقع جاسوس افزارها در کنار نگارش‌های رایگان یک نرم افزار – و توسط نویسنده نرم‌افزار – ارائه می‌گردند تا نویسنده نرم افزار بتواند از این طریق درآمدی بدست آورد و یا امکان ارائه پیشنهاد جهت فروش نرم‌افزار را برای خود فراهم آورد. بنابر این در اکثر اوقات و در زمان نصب نگارشهای رایگان یک نرم افزار کاربران از وجود جاسوس افزار در طی نصب برنامه رایگان آگاهی پیدا می‌کنند و نرم افزار رایگان پیشنهاد خرید نگارش اصلی نرم افزار بدون وجود جاسوس افزار را به کاربر ارائه می‌نماید.

مثال‌های معروف در زمینه جاسوس افزارها عبارت از نرم افزارهای شبکه‌ای نقطه به نقطه (P2P) هستند که می‌توان در این زمینه به نرم‌افزارهای "spyfalcon" و یا "spysheriff" اشاره کرد. این نرم افزارها در ظاهر ضد جاسوس افزار هستند ولی در حقیقت خود آنها در طیف نرم‌افزارهای جاسوس افزار قرار دارند.

لذا اگر فایلی در رایانه به عنوان جاسوس افزار شناسایی شد، بهتر است آن فایل را پاک کنید. چرا که ممکن است فایل مورد نظر حاوی کدهای مخرب باشد.

### ۷-۱-۶- نرم‌افزارهای به صورت بالقوه ناامن

امروزه نرم‌افزارهای سودمند متعددی وجود دارند که با استفاده از آنها می‌توان مدیریت شبکه‌های رایانه‌ای را تسهیل بخشید. با این حال کاربران غیرمجاز می‌توانند از این نرم‌افزارها برای مقاصد سودجویانه استفاده به عمل آورند. لذا شرکت "ESET" سیستم ضدویروس خود را به گونه‌ای طراحی نموده است تا بتواند در صورت تمایل کاربر چنین تهدیداتی را شناسایی کند.

در واقع تمامی نرم‌افزارهای مدیرتی شبکه از راه دور، نرم افزارهای شکستن کلمات عبور و نرم‌افزارهای ضبط دکمه‌های صفحه کلید در مجموعه "نرم‌افزارهای به صورت بالقوه ناامن" قرار می‌گیرند.

لذا اگر چنین برنامه‌هایی را بر روی رایانه شناسایی نمودید، بهتر است با مدیر شبکه مشورت نموده و یا اقدام به حذف آنها نمائید.

### ۸-۱-۶- نرم افزارهای به صورت بالقوه ناخواسته

برنامه‌های به صورت بالقوه ناخواسته لزوما جزء کدهای مخرب محسوب نمی‌شوند، اما می‌توانند اثرات نامطلوبی را بر روی کارایی سیستم رایانه‌ای داشته باشند. چنین نرم‌افزارهایی برای نصب نیاز به اتخاذ تصمیم از ناحیه کاربر دارند. در صورتی که چنین نرم‌افزارهایی بر روی رایانه کاربر نصب باشد، رایانه رفتار متفاوتی نسبت به زمان قبل از نصب آنها از خود نشان می‌دهد. چنین رفتارهایی عبارتند از:

الف) پنجره‌هایی که کاربر قبلا با آنها روبرو نبوده است گشوده می‌شوند.

ب) پروسه‌های مخفی فعال شده و اجرا می‌گردند.

ج) میزان استفاده از منابع رایانه‌ای افزایش می‌یابد.

د) نتایج حاصله از کاوش فایلها دستخوش تحویل می‌گردد.

هـ) نرم افزار مورد نظر با سرورهای راه دور ارتباط برقرار می‌کند.

### ۲-۶- انواع حملات از راه دور

انواع متعددی از تکنیک‌های ویژه وجود دارند که هکرها (افراد غیرمجاز) جهت دسترسی و به خطر انداختن رایانه‌های راه دور از آنها استفاده به عمل می‌آورند. در ادامه طبقه بندی این نوع از تهدیدات رایانه‌ای مورد بررسی قرار می‌گیرد.

### ۱-۲-۶- حملات "DoS"

"DoS" مخفف عبارت "denial of service" بوده و به حملاتی اطلاق می‌شود که هدف از آنها غیر قابل دسترس نمودن یک رایانه و یا یک شبکه از دسترس کاربران است. لذا لازم است رایانه‌هایی که مورد چنین حملاتی قرار می‌گیرند را راه‌اندازی مجدد نمائید تا بتوانند مجددا ارتباط شبکه‌ای را برقرار نمایند.

در اغلب اوقات هدف اصلی این نوع حملات سرورهای "web" و به بیان دیگر غیر قابل دسترس نبودن آنها توسط کاربران در یک بازه زمانی است.

### ۲-۲-۶- تاثیر گذاری منفی بر روی "DNS"

هکرها با استفاده از روش مسموم نمودن "DNS" اطلاعات غیر واقعی در اختیار سرور "DNS" قرار می‌دهند تا سرور از این اطلاعات دروغین استفاده به عمل آورد. این اطلاعات دروغین برای یک بازه زمانی نگهداری (cache) شده و هکرها می‌توانند در این بازه زمانی اطلاعات "DNS" مربوط به آدرس‌های "IP" را بازنویسی (rewrite) نمایند. در نتیجه کاربران سایتهای اینترنتی به جای دانلود اطلاعات اصلی مورد نظر، ویروسها و یا کرم‌های رایانه‌ای را دانلود خواهند نمود.

### ۳-۲-۶- حملات کرم‌های رایانه‌ای

کرم رایانه‌ای عبارت از کد مخربی است که رایانه میزبان را آلوده نموده و از طریق بستر شبکه گسترش پیدا می‌کند. کرم‌های شبکه از حفره‌های امنیتی نرم افزارهای مختلف جهت گسترش و ایجاد آلودگی استفاده به عمل می‌آورند. کرم‌ها با توجه به حفره‌های امنیتی و

نقاط آسیب‌پذیری از طریق بستر اینترنت می‌توانند در مدت زمان بسیار کوتاهی (چند ساعت و حتی در پاره‌ای موارد چند دقیقه) در اقصی نقاط جهان تکثیر شوند.

حملات بسیاری از کرم‌ها از قبیل "sasser" و یا "sqlslammer" را می‌توان با استفاده از تنظیمات پیش فرض دیواره آتش و یا بستن پورتهایی که مورد استفاده قرار نمی‌گیرند، دفع نمود. همچنین لازم است همواره سیستم عامل را بروز نمائید تا سطح امنیتی رایانه افزایش یابد.

### ۴-۶- پویش پورتها

هکرها با پویش پورتها می‌توانند پورتهای باز رایانه موجود در شبکه رایانه‌ای را جهت مقاصد سوء شناسایی نمایند. در اینجا وسیله مورد استفاده آنها نرم‌افزارهای پویشگر پورت (port scanner) است.

یک پورت رایانه‌ای گذرگاه یا نقطه‌ای مجازی است که داده‌های ورودی و خروجی را کنترل می‌کند و لذا از لحاظ امنیتی دارای اهمیت ویژه‌ای است. در یک شبکه بزرگ، اطلاعات بدست آمده از پویشگرهای پورت می‌تواند منجر به شناسایی نقاط آسیب‌پذیری شبکه گردد. لذا مدیران شبکه با استفاده از پویشگرهای پورت می‌توانند نسبت به شناسایی و رفع نقاط آسیب‌پذیری شبکه اقدام کنند. با این حال هکرها نیز از چنین نرم‌افزارهایی استفاده می‌کنند تا بتوانند امنیت رایانه‌ها را با مخاطره روبرو نمایند. اولین قدم آنها ارسال بسته‌های اطلاعات به هر یک از پورت‌ها است. در گام دوم بر اساس پاسخ دریافت شده از سوی پورت، می‌توانند تخمین بزنند که از کدام یک از پورتها استفاده به عمل می‌آید. پویش پورت‌ها به تنهایی خطرناک نیست. اما توجه داشته باشید که این کار نقاط آسیب‌پذیری بالقوه سیستم را آشکار نموده و هکرها می‌توانند بر این اساس کنترل رایانه‌های راه دور را بدست گیرند.

لذا توصیه می‌شود که مدیران شبکه پورتهایی که مورد استفاده قرار نمی‌گیرند را بسته و حفاظت از پورت‌هایی که مورد استفاده هستند را به عمل آورند.

### ۵-۲-۶- غیرهمزمان سازی "TCP"

غیرهمزمان سازی "TCP" تکنیکی است که در حملات "TCP HIJACKING" مورد استفاده قرار می‌گیرد. استفاده از این تکنیک در زمانی که رشته اعداد در پکت‌های دریافتی با رشته اعداد مورد انتظار متفاوت هستند شناسایی می‌گردد. پکت‌های دارای رشته اعدادی که انتظار دریافت آن نمی‌رفته است حذف گردیده و در صورت حضور در پنجره ارتباطی جاری و یا در یک محل نگهداری بافر ذخیره می‌شوند.

در حالت غیر همزمانی، هر دو نقاط انتهایی بستر ارتباطی پکت‌های دریافتی را حذف می‌کنند. در این زمان است که هکرهای راه دور می‌توانند به سیستم نفوذ کرده و پکت‌های دارای رشته اعداد صحیح را بدست آورند. هکرها حتی می‌توانند با دستورات رایانه‌ای خود بستر ارتباطی را کنترل نموده و یا تغییراتی را در آن ایجاد نمایند.

هدف از حملات "TCP HIJACKING" اختلال در ارتباطات سرور – کلاینت و یا شبکه‌های نقطه به نقطه است. بسیاری از حملات را می‌توان با استفاده از سیستم تائید اعتبار برای هر یک از بخشهای "TCP" دفع نمود. همچنین توصیه می‌شود از پیکربندی‌های توصیه شده سخت افزارهای شبکه‌ای استفاده به عمل آید.

### "SMB" رله -۶-۲-۶

"SMBRELAY" و "SMBRELAY2" برنامه‌های ویژه‌ای هستند که قادرند حملاتی را علیه رایانه‌های راه دور به انجام رسانند. این برنامه‌ها از مزیت پروتکل به اشتراک گذاری فایل "server message block" که در "netbios" لایه بندی شده است استفاده به عمل می‌آورند. اگر کاربر یک پوشه و یا دایرکتوری را درسطح شبکه محلی به اشتراک گذارد، به احتمال بسیار زیاد از پروتکل مورد نظر استفاده نموده است. کلمات عبور در ارتباطات شبکه‌های محلی رد و بدل می‌شوند.

در واقع نرم افزار "SMBRELAY" یک ارتباط را در پورتهای ۱۳۹ و ۴۴۵ (پروتکل) "UDP" دریافت کرده، پکت‌ها تبادلی بین سرور و کلاینت‌ها را رله نموده و آنها را تغییر می‌دهد. ارتباط کلاینت پس از اتصال و تائید اعتبار قطع می‌گردد و نرم افزار "SMBRELAY" یک آدرس "IP" مجازی ایجاد می‌نماید. می‌توان به این آدرس "IP" با دستور "net use \\192.168.1.1" دسترسی یافت. از این آدرس توسط تمامی ویژگی‌های شبکه‌ای ویندوز استفاده به عمل می‌آید. نرم افزار "SMBRELAY" تمامی ترافیک پروتکل "SMB" را بجز ترافیک مربوط به مذاکرات (negotiation) و مراحل تائید اعتبار رله می‌کند و هکرهای راه دور از این آدرس "IP" در زمان اتصال رایانه کلاینت (به شبکه) استفاده‌های سوء می نمایند.

پایه و اساس کار نرم افزار "SMBRELAY2" نیز شبیه نرم افزار "SMBRELAY" است و تنها تفاوت آن استفاده از نام‌های "netbios" رایانه‌ها به جای آدرس "IP" آنها است. هر دوی این نرم‌افزارها قادر به انجام حملات "man–in–the–middle" هستند. این نوع حملات امکان خواندن پیام‌ها، وارد کردن پیام‌ها و تغییر پیام‌های تبادلی بین دو نقطه ارتباطی را به صورت مخفیانه برای هکرها فراهم می‌آورند. اغلب رایانه‌هایی که دچار چنین حملاتی شده باشند، هنگ کرده و یا به صورت غیر قابل انتظاری راه‌اندازی مجدد می‌گردند.

لذا توصیه می‌شود به منظور ممانعت از چنین حملاتی از کلیدها و یا کلمات شناسایی تائید اعتبار در تبادل اطلاعات استفاده به عمل آید.

### "ICMP" حملات -۶-۲-۷

"ICMP" یکی از پروتکل‌های معروف و پرکاربرد در اینترنت بوده و به معنای پروتکل کنترل پیام‌های اینترنتی است. اساسا رایانه‌های شبکه‌های رایانه‌ای از این پروتکل جهت ارسال طیف گسترده‌ای از پیام‌های خطا استفاده می‌کنند.

هکرهای راه دور همواره سعی نموده‌اند تا از نقاط ضعف و آسیب پذیری این پروتکل سودجویی نمایند. در واقع پروتکل "ICMP" به صورت ارتباط یک طرفه و بدون تائید اعتبار طراحی شده است و این موضوع امکان حملات "DoS" را برای هکرهای راه دور فراهم می‌آورد.

مثالهای نوعی حملات "ICMP" عبارت از "ping flood"، "ICMP_ECHO flood" و حمله "smurf" هستند. رایانه‌هایی که مورد حملات "ICMP" قرار می‌گیرند با افت سرعت و اختلال در برقراری ارتباط با اینترنت روبرو می‌گردند.

### ۳-۶- پست الکترونیک

"email" یا پست الکترونیک یک روش مدرن ارتباطی با مزایای بسیار زیاد است. از مزایای آن می‌توان به قابلیت انعطاف، سرعت و مستقیم بودن آن اشاره کرد. ضمن اینکه نقش عمده‌ای را در گسترش اینترنت در دهه "1990" بر عهده داشته است.

متاسفانه، پست الکترونیک و اینترنت با وجود تمام مزایای خود نتوانسته‌اند مانع فعالیتهای غیرقانونی مرتبط از جمله انتشار هرزنامه‌ها شوند.

هرزنامه‌ها شامل پیام‌های تبلیغاتی ناخواسته و پیام‌های "hoax" و ... بوده و از این طریق بستر مناسبی را برای گسترش کدهای مخرب نیز فراهم آورده‌اند.

افزایش ناراحتی و رشد تهدید علیه کاربران در این زمینه بر این اساس استوار است که ارسال هرزنامه‌ها به کاربران تقریبا هیچ گونه بار مالی را متوجه فرستنده هرزنامه نمی‌نماید و نویسندگان هرزنامه‌ها از ابزار و منابع متعددی جهت دسترسی به آدرسهای پست الکترونیکی کاربران بهره می‌برند. به علاوه، حجم و تنوع هرزنامه‌ها باعث شده است که کنترل آنها (مبارزه با آنها) بسیار دشوار گردد. ضمن اینکه هر چقدر کاربر از آدرس پست الکترونیکی خود بیشتر استفاده نماید، احتمال اینکه آدرس پستی وی به یکی از بانک‌های اطلاعاتی موتورهای ارسال هرزنامه افزوده شود نیز افزایش می‌یابد. چند مورد از نکات مهم که با رعایت آنها می‌توان تا حدود زیادی از دریافت هرزنامه‌ها در امان بود به قرار زیر هستند:

الف) در صورت امکان آدرس پست الکترونیک خود را در اینترنت انتشار ندهید.

ب) صرفا آدرس پست الکترونیک خود را در اختیار افراد حقیقی و حقوقی قابل اعتماد قرار دهید.

ج) در صورت امکان از نام‌های رایج در آدرس پست الکترونیک استفاده نکنید. زیرا رهگیری آنها ساده‌تر است.

د) به هرزنامه‌های دریافتی در صندوق پستی خود جواب ندهید.

هـ) در زمان پر کردن فرم‌های اینترنتی توجه ویژه‌ای عنایت نمائید. باید دقت ویژه مضاعفی را در مورد گزینه‌های خاصی که به معنی اتخاذ تصمیم کاربر در مورد ارسال اطلاعات بیشتر به آدرس پست الکترونیک وی است، معطوف نمود.

و) برای هر کار از یک آدرس پستی استفاده کنید. به عنوان مثال بهتر است صندوق پست الکترونیک مورد استفاده جهت امور مربوط به کار با صندوق مورد استفاده جهت ارتباط با دوستان متفاوت باشد.

ز) هر ازگاهی بهتر است آدرس پست الکترونیک خود را تغییر دهید.

ح) از نرم‌افزارهای ضد هرزنامه استفاده به عمل آورید.

#### ۱-۳-۶- پیام‌های تبلیغاتی

یکی از روش‌های جدید و رو به رشد تبلیغات استفاده از بستر اینترنت است. در ارسال پیام‌های تبلیغاتی اینترنتی از آدرس های پست الکترونیکی کاربران استفاده به عمل می‌آید. مهمترین نکته در این نوع بازاریابی عبارت از هزینه های نزدیک به صفر، سطح بالای مستقیم بودن ارتباط و تاثیر پذیری پیام‌ها و سرعت بسیار بالای ارسال این پیام‌ها است. بسیاری از شرکت‌ها از پیام‌های بازاریابی

اینترنتی جهت برقراری ارتباط موثر با مشتریان خود استفاده می‌کنند. این نوع تبلیغات قانونی است، چرا که ممکن است کاربر تمایل به دریافت اطلاعات در رابطه با محصولات خاصی داشته باشد.

اما نکته اصلی اینجاست که بسیاری دیگر از شرکت‌ها با استفاده از ابزار پست الکترونیک مبادرت به ارسال پیام‌های تجاری ناخواسته به کاربران می‌نمایند. در اینجاست که از واژه هرزنامه برای نام بردن چنین پیام‌هایی استفاده می‌گردد.

امروزه رشد و حجم هرزنامه‌های دریافتی توسط کاربران به یک معضل عمده تبدیل شده است. نویسندگان هرزنامه‌ها همواره سعی نموده‌اند وجهه قانونی به هرزنامه‌های خود دهند. به بیان دیگر تبلیغات اینترنتی قانونی در مقیاس بزرگ ممکن است نتیجه معکوس داشته باشد.

### ۲-۳-۶- پیام‌های "Hoax"

"Hoax" پیامی است که در سطح اینترنت پخش می‌گردد. این نوع پیام‌ها معمولا توسط پست الکترونیک و در برخی از مواقع توسط نرم افزارهای ارتباطی اینترنتی نظیر "ICQ" و "Skype" ارسال می‌گردند. محتوای این نامه‌ها معمولا یک جک و یا محتوای یک رخداد در سطح جامعه است.

هکرها از ویروس‌های "hoax" جهت ایجاد وحشت، تردید و سلب اطمینان کاربران استفاده می‌کنند. به عنوان مثال باعث می‌شوند کاربران باور کنند که یک ویروس غیر قابل حذف در رایانه آنها وجود داشته و علاوه بر پاک کردن فایلهای آنها، اطلاعات مربوط به کلمات عبور را نیز جمع‌آوری کرده و برای افراد غیرمجاز ارسال می‌نماید و یا اینکه ویروسی در رایانه آنها وجود دارد که در حال انجام فعالیت‌های مخرب بر روی رایانه است.

از برخی از پیام‌های "hoax" نیز جهت آبرو ریزی افراد استفاده به عمل می‌آید. معمولا این پیام‌ها از دریافت کننده خود می‌خواهند تا پیام دریافتی را جهت اطلاع دیگران ارسال نمایند و لذا این امر باعث افزایش زمان ماندگاری پیام "hoax"خواهد شد.

علاوه بر پیام‌های "hoax"مورد نظر، پیام‌های "hoax"دیگری نیز وجود دارند که از طریق بستر مخابراتی تلفن‌های همراه تکثیر می‌شوند و معمولا کشف نیت اصلی ارسال کننده این پیام‌ها غیر ممکن است.

به طور کلی ، اگر کاربر پیامی را دریافت کند که فرستنده پیام از کاربر بخواهد تا پیام دریافتی را به دیگران ارسال کند، قطعا کاربر یک پیام "hoax" را دریافت نموده است. توجه داشته باشید که در اینترنت سایتهای متعددی وجود دارند که می‌توانند به کاربر در شناسایی اینکه پیام دریافتی وی یک پیام قانونی و یا یک "hoax"است، کمک کند. بنابراین قبل از ارسال پیام دریافتی به دیگران با استفاده از ابزار کاوش اینترنتی از "hoax" نبودن پیام اطمینان حاصل کنید.

### ۳-۳-۶- "phishing"

واژه "phishing" مبین نوعی فعالیت خطرناک است که از تکنیک‌های مهندسی اجتماعی بهره می‌جوید. در واقع هکرها با استفاده از این نوع تهدید مبادرت به اخذ اطلاعات محرمانه کاربران می‌نمایند و به بیان دیگر هدف اصلی این تهدیدات دسترسی به شماره حسابهای بانکی، شماره‌های شناسایی شخصی کاربران و ... است.

معمولا دسترسی افراد غیرمجاز به سیستم رایانه‌ای کاربر از طریق ارسال یک نامه الکترونیکی است که به ظاهر از طرف یک شخص حقیقی و یا حقوقی قابل اعتماد ارسال گردیده است. این نامه الکترونیکی می‌تواند ظاهری بسیار موجه داشته و شامل تصاویر گرافیکی و محتویات دیگری باشد که نشان می‌دهد مرجع ارسال کننده نامه کاملا معتبر است. نامه مورد نظر در گام بعدی از کاربر می‌خواهد تا برخی از اطلاعات محرمانه خود از جمله شماره حسابهای بانکی، شناسه‌های کاربری و کلمات عبور و ... را درج و ارسال کند. در صورت درج این اطلاعات و ارسال آنها، هکرها به راحتی می‌توانند از آنها سوء استفاده به عمل آورند.

بنابراین توجه به این نکته امنیتی بسیار ضروری است که هیچ یک از بانک‌ها، موسسات مالی و اعتباری در یک نامه الکترونیکی ناخواسته از کاربران تقاضای درج و ارسال کلمات عبور و شناسه‌های کاربری خود را برای آن موسسات نخواهند داشت.

### ۴-۳-۶- شناسایی نشانه‌های هرزنامه‌ها

به طور کلی، چند نشانه محدود وجود دارد که بر اساس آنها کاربر می‌تواند یک هرزنامه را در صندوق پست الکترونیکی خود شناسایی نماید. به بیان دیگر اگر پیام دریافتی در برگیرنده هر یک از موارد ذیل باشد، به احتمال بسیار زیاد یک هرزنامه است.

الف) آدرس پست الکترونیکی ارسال کننده نامه در فهرست آدرس‌های کاربر نباشد.

ب) در نامه پیشنهاد دریافت مبلغ زیادی در ازای پرداخت مبلغ ناچیزی به کاربر ارائه شده باشد.

ج) در نامه دریافتی از کاربر درخواست شده باشد که اطلاعات شخصی خود را درج و ارسال نماید.

د) نامه دریافتی به زبان خارجی (زبانی متفاوت از زبان مادری کاربر) باشد.

هـ) در متن نامه دریافتی از کاربر خواسته شده باشد تا یک کالای ناخواسته را خریداری نماید. در این شرایط لازم است در صورت تمایل به خرید، از صحت نامه دریافتی آگاهی کامل کسب شود.

و) برخی از واژگان خاص جهت عبور نامه دریافتی از فیلتر ضدهرزنامه کاربر به صورت اشتباه و یا به صورت ناقص درج گردیده باشند.

### ۱-۴-۳-۶- قوانین

نرم افزارهای ضدویروس از قوانین جهت حفاظت کاربران از هرزنامه‌ها استفاده به عمل می‌آورند. این قوانین دارای دو بخش اصلی هستند:

الف) شرط (به عنوان مثال دریافت نامه از یک آدرس الکترونیکی خاص)

ب) عکس العمل (به عنوان مثال پاک کردن نامه، انتقال آن به یک پوشه خاص و ...)

تعداد و ترکیب قوانین در نرم‌افزارهای ضد هرزنامه متفاوت است. ضمن اینکه قوانین یک نرم افزار ضد هرزنامه نقش کلیدی در حفاظت کاربر دارند. در ادامه سه مثال از قوانین ارائه گردیده‌اند:

الف)

۱- شرط: نامه دریافتی حاوی واژگانی است که عموما در هرزنامه‌ها دیده می‌شوند.

۲- عکس العمل: حذف نامه دریافتی

ب)

۱- شرط: نامه دریافتی حاوی پیوستی است که دارای پسوند ".exe" می‌باشد.

۲- عکس العمل: حذف پیوست نامه و انتقال نامه به صندوق پستی کاربر

ج)

۱- شرط : یک نامه از کارفرمای کاربر دریافت می‌شود.

۲- عکس العمل: انتقال نامه دریافتی به پوشه "work"کاربر

توصیه می‌شود کاربران از ترکیب قوانین در نرم‌افزارهای ضد هرزنامه استفاده به عمل آورند تا مدیریت برنامه آسان گردیده و هرزنامه‌ها به شکل موثرتری فیلتر شوند.

### ۲-۴-۳-۶- فیلتر بایسیان

فیلتر بایسیان یکی از روشهای موثر فیلتر نمودن هرزنامه‌ها است که در اکثر نرم‌افزارهای ضد هرزنامه مورد استفاده قرار می‌گیرد. این فیلتر قادر است نامه‌های ناخواسته را با دقت بسیار بالایی شناسایی کند. فیلتر بایسیان بر اساس شرائط مورد نظر هر یک از کاربران یک رایانه عمل نماید.

چگونگی عمل این فیلتر بر اساس موارد ذیل انجام می‌پذیرد:

الف) فرایند یادگیری در فاز اول انجام می‌شود. به بیان دیگر کاربر وضعیت تعدادی از نامه‌ها را به صورت دستی مشخص می‌کند که آیا نامه مورد نظر هرزنامه است و یا خیر.

ب) فیلتر بایسیان هردو گروه نامه‌های عادی و هرزنامه‌ها (که توسط کاربر مشخص گردیده‌اند) را تحلیل نموده و متوجه می‌شود (یاد می‌گیرد) که چه نامه‌هایی از دیدگاه کاربر هرزنامه هستند.

بنابراین فیلتر بایسیان با ایجاد یک ایندکس از مشخصات هرزنامه‌ها مبادرت به کنترل نامه‌های دریافتی می‌نماید. مزیت اصلی این فیلتر قابلیت انعطاف آن است.

### ۳-۴-۳-۶- فهرست سفید

به طور کلی فهرست سفید به فهرستی از آیتم‌ها و یا اشخاص قابل اعتماد و یا افرادی که دسترسی آنها مجاز می‌باشد، اطلاق می‌گردد. واژه "email whitelist"اشاره به فهرست کاربرانی دارد که کاربر تمایل به دریافت نامه‌های الکترونیکی از آنها را دارد.

### ۴-۴-۳-۶- فهرست سیاه

نقطه مقابل فهرست سفید است.

### ۵-۴-۳-۶- قسمت کنترلی سمت سرور

قسمت کنترلی سمت سرور تکنیکی برای شناسایی حجم هرزنامه‌های دریافتی بر اساس تعداد نامه‌های دریافتی و عکس العمل کاربران در رابطه با آنها است. هرزنامه بر اساس محتویات آن یک ردپای دیجیتالی منحصر به فرد را بر روی سرور از خود به جای می‌گذارد. در

واقع، این ردپا یک شماره شناسایی منحصر به فرد است که حاوی هیچ اطلاعاتی در مورد محتوی نامه الکترونیکی نمی‌باشد. بنابراین دو نامه مشابه دارای یک ردپا و دو نامه متفاوت دارای ردپاهای دیجیتالی متفاوتی هستند.

اگر یک نامه به عنوان هرزنامه شناسایی شود، ردپای دیجیتالی آن به سرور فرستاده می‌گردد. لذا اگر سرور ردپاهای دیجیتالی یکسانی را (با توجه به ردپای یک هرزنامه خاص) دریافت کند، آن ردپا را در بانک اطلاعاتی ردپاهای هرزنامه‌ها ثبت و نگهداری خواهد نمود. بنابراین در زمان پویش پیام‌های دریافتی، نرم افزار ضد هرزنامه ردپاهای دیجیتالی مربوط به نامه‌ها را به سرور ارسال میکند و سرور اطلاعات مورد نظر نرم افزار ضد هرزنامه را در اختیار نرم افزار قرار می‌دهد تا با بررسی این اطلاعات مشخص شود که نامه دریافتی هرزنامه است یا خیر.

ORIGINAL DOC DATA:
- TITLE OF HANDBOOK: ESET SMART SECURITY USER GUIDE REV.20071129-003
- NAME OF FILE: ESET_ESS_User_Guide_EN.Pdf
- SIZE AND SIZE ON DISK: 3.72 MB (3,906,272 bytes) 3.72 MB (3,907,584 bytes)
TRANSLATION DATA FILE:
- LAST VERSION NUMBER: 100
- DATE:22-2-2008
-TRANSLATOR: MAJID GHASEMY
- EMAIL:majid_ghaemy@yahoo.com
- NOMBER OF WORDS: 28154
- SUPPORT TIME : NOT SUPPORTED