راهنمای سریع استفاده از

نسخه خانگی کوییک هیل

شرکت فناوری ارتباطات و اطلاعات فانوس

نماینده رسمی محصولات امنیتی کوییک هیل در ایران

۰۲۱۷۷۱۴۲۵۲۶ www.quickheal.co.ir info@qhi.ir

Quick Heal

Security Simplified

تیم فنی شرکت فناوری ارتباطات و اطلاعات فانوس به عنوان نخستین نماینده رسمی کوییک‌هیل در ایران چکیده بیش از ۷ سال تجربه کار با آنتی ویروس کوییک‌هیل را به صورت کاربردی و ساده، در این جزوه آموزشی گرد آورده است.

در صورت داشتن هر نوع سوال، پیشنهاد یا انتقادی می‌توانید با شرکت فناوری ارتباطات و اطلاعات فانوس از طریق ایمیل info@qhi.ir ، تلفن ۷۷۱۴۲۵۲۶-۰۲۱ ، پیامک ۳۰۰۰۴۶۲۵ ، وب سایت www.quickheal.co.ir و نیز وبلاگ اطلاع رسانی امنیتی این شرکت blogs.quickheal.co.ir ارتباط برقرار فرمایید.

سوالات فنی خود را با ایمیل support@quickheal.co.ir مطرح نمایید.

کاربران طرح جزیره امن می‌توانند برای ارتباط با شماره تلفن ۴۲۷۲۲-۰۱۱، پیامک ۱۰۰۰۴۲۷۲۲، ایمیل support@42722.ir تماس و یا به وب‌سایت طرح http://42722.ir مراجعه فرمایند.

فهرست مطالب

نیازمندی‌های سیستمی

حداقل مشخصات سیستمی به شرح زیر می‌باشد:

Operation Systems	Minimum Requirements
Windows XP	● 300 MHz Pentium Processor (or compatible) or higher ● 512 MB of RAM ● DVD or CD-ROM drive ● Service Pack 2 or later ● Service Pack 2 or later
Windows Vista	● 1 GHz Pentium Processor (or compatible) or higher ● 512 MB of RAM ● DVD or CD-ROM drive
Windows 7 / Windows 8 / Windows 8.1	● 1 GHz Pentium Processor (or compatible) or higher ● For 32-bit 1 GB or higher RAM; For 64-bit 2 GB or higher RAM ● DVD or CD-ROM drive

حداقل فضای کافی دیسک برای نصب آنتی‌ویروس:

Product	Free Disk Space
Quick Heal Total Security	2.25 GB
Quick Heal Internet Security	2.15 GB
Quick Heal AntiVirus Pro	2.15 GB

نیازمندی‌های Anti-Rootkit کوییک هیل

- Anti-Rootkit کوییک هیل در سیستم عامل های ۶۴ بیتی پشتیبانی نمی شود. (آسیب‌پذیری روتکیت، تنها در سیستم‌عامل‌های ۳۲ بیتی مایکروسافت وجود دارد)

PC2Mobile Scan کوییک هیل

- این ویژگی تنها در نسخه کوییک‌هیل توتال سکیوریتی به صورت رایگان ارائه می گردد.
- برای ابزارهای Windows Mobile :
  - برای سیستم عامل ویندوز XP و قبل از آن می‌بایست برنامه Microsoft Active Sync 4.0 یا بالاتر نصب باشد.
  - برای سیستم عامل ویندوز Vista و بالاتر می‌بایست برنامه Windows Mobile Device Center نصب باشد.
- برای دیدن لیست گوشی های موبایل که توسط کوییک هیل پشتیبانی می شود به آدرس زیر بروید:

http://www.quickheal.ir/pc2mobile.asp

PC Tuner کوییک هیل

- این ویژگی تنها در نسخه کوییک‌هیل توتال سکیوریتی به صورت رایگان ارائه می گردد.

سندباکس مرورگر کوییک هیل

- این ویژگی بر روی ویندوز XP نسخه ۶۴ بیتی ارائه نمی گردد.

بانکداری امن کوییک هیل

- این ویژگی بر روی ویندوز XP نسخه ۶۴ بیتی ارائه نمی گردد.

نصب آنتی‌ویروس کوییک‌هیل

ابتدا مطمئن شوید که آنتی‌ویروس دیگری بر روی سیستم شما نصب نباشد. (امکان نصب دو آنتی‌ویروس بر روی یک سیستم وجود ندارد.)

اگر سیستم شما به شدت آلوده باشد، می‌توانید از دیسک اورژانسی کوییک‌هیل سیستم را راه‌اندازی کرده و اقدام به ویروسیابی نمایید.

اگر نسخه‌ی قدیمی آنتی ویروس کوییک هیل بر روی سیستم شما نصب است، ابتدا آن‌را حذف و سیستم را ری‌استارت کرده و مجددا اقدام به نصب نمایید.

آخرین نسخه نرم‌افزار نصب را می‌توانید از سایت رسمی http://42722.ir/dw نیز دانلود نمایید.

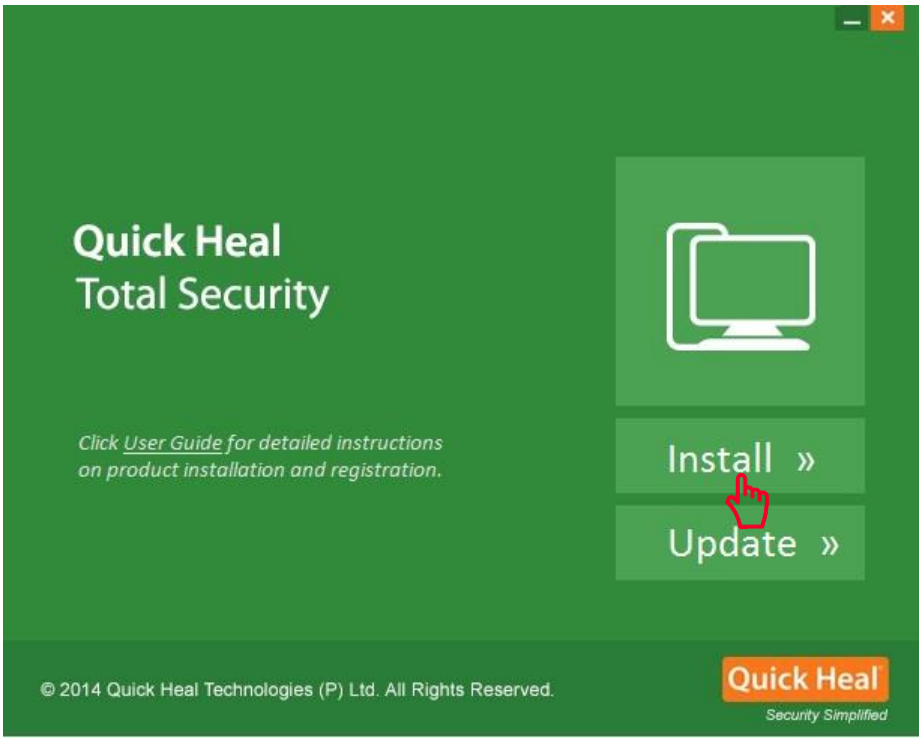
همچنین امکان تهیه CD/DVD نصب از مراکز مخابراتی مهیا می‌باشد.

امکان استفاده یک CD یا DVD نصب برنامه در چندین سیستم وجود دارد.

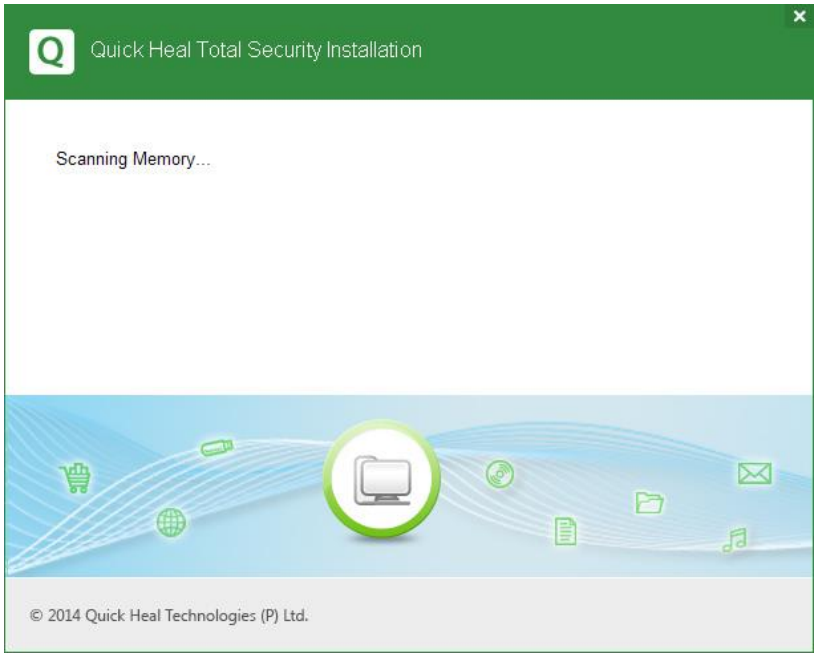
هر لایسنس (کلید محصول) تنها بر روی یک سیستم قابل استفاده می‌باشد.

الف) نصب (Install)

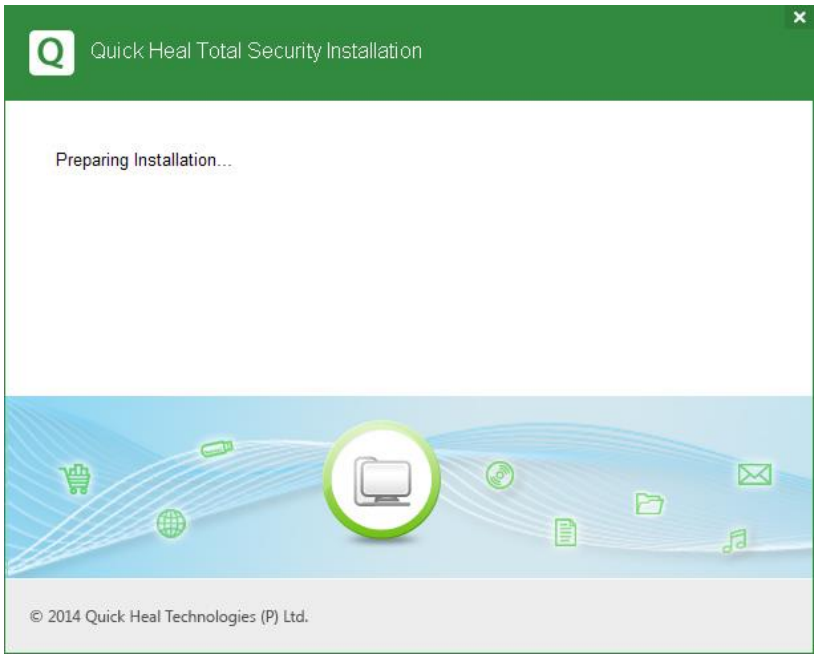
نصب آنتی ویروس کوییک هیل بسیار ساده می‌باشد. مراحل زیر را دنبال فرمایید:



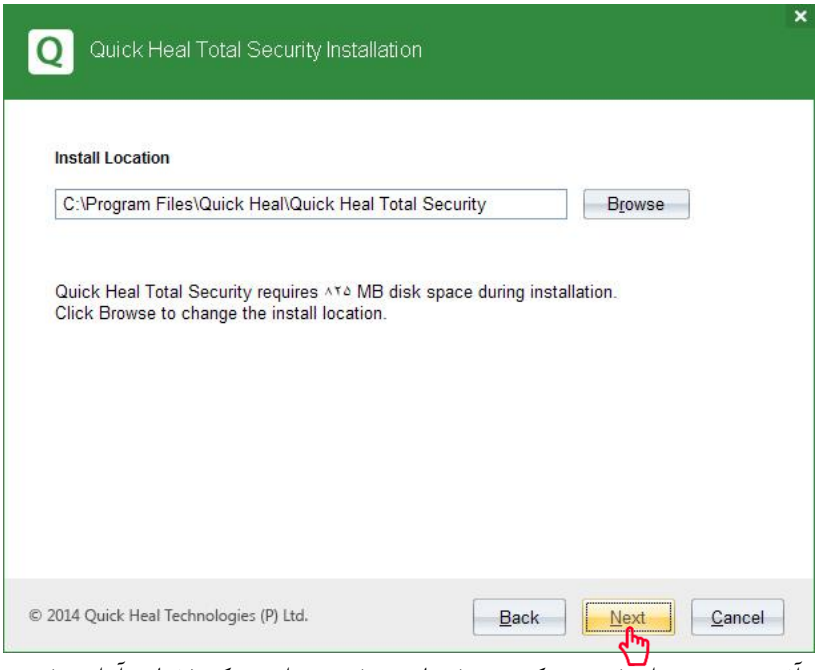
ابتدا CD محصول را وارد دستگاه کرده و منتظر بمانید تا صفحه ی زیر نمایش داده شود (در صورت عدم اجرای خودکار بر روی فایل Autorun.exe درون CD کلیک کنید). بر روی Install کلیک کنید.



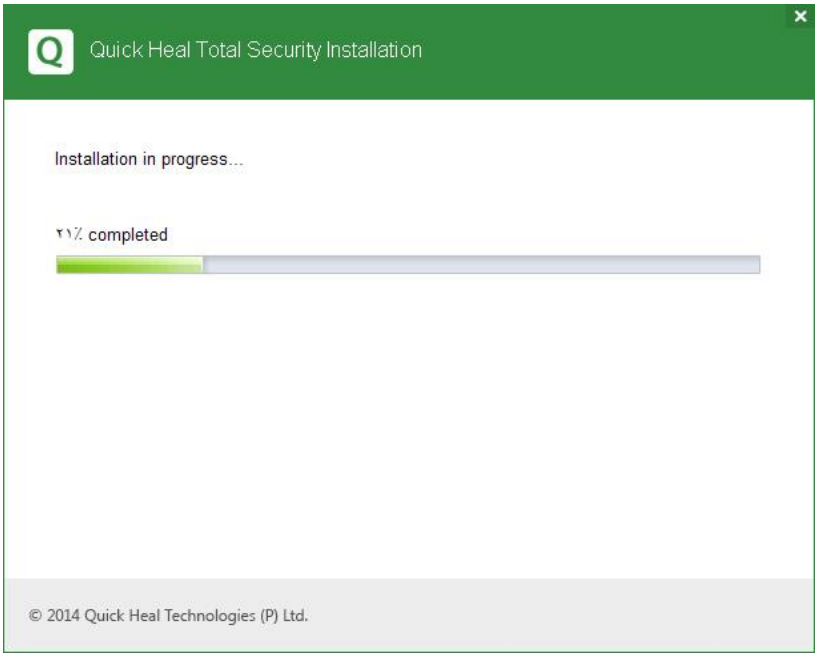
پیش از شروع به نصب، کوییک هیل حافظه اصلی RAM سیستم را ویروسیابی می‌کند. در صورتی که ویروس در RAM وجود داشت، از شما می‌خواهد تا سیستم را مجدداً راه اندازی نمایید تا پیش از بارگذاری ویندوز ویروس فوق از روی سیستم شما پاکسازی شده سپس نصب را ادامه دهید.



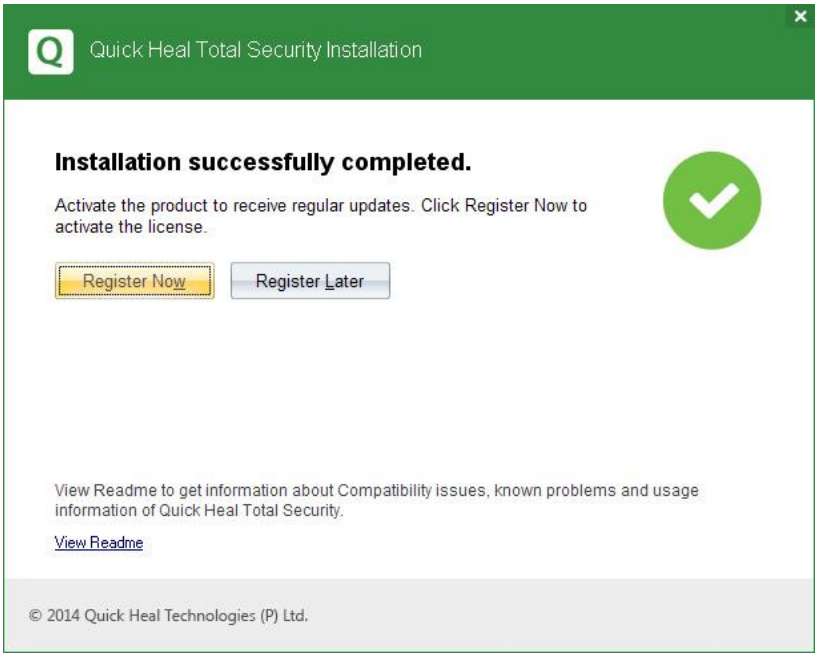
چند لحظه تأمل فرمایید تا فرایند استخراج فایل فشرده نصب تکمیل گردد.



مسیر نصب آنتی‌ویروس را مشخص کنید. پیشنهاد می‌شود درایوی که فضای آزاد بیشتری در اختیار دارد را انتخاب نمایید (3GB یا بیشتر پیشنهاد می‌شود).



در این مرحله نصب آنتی‌ویروس کوییک‌هیل آغاز می‌شود. کمی منتظر بمانید تا فرآیند نصب کامل گردد.

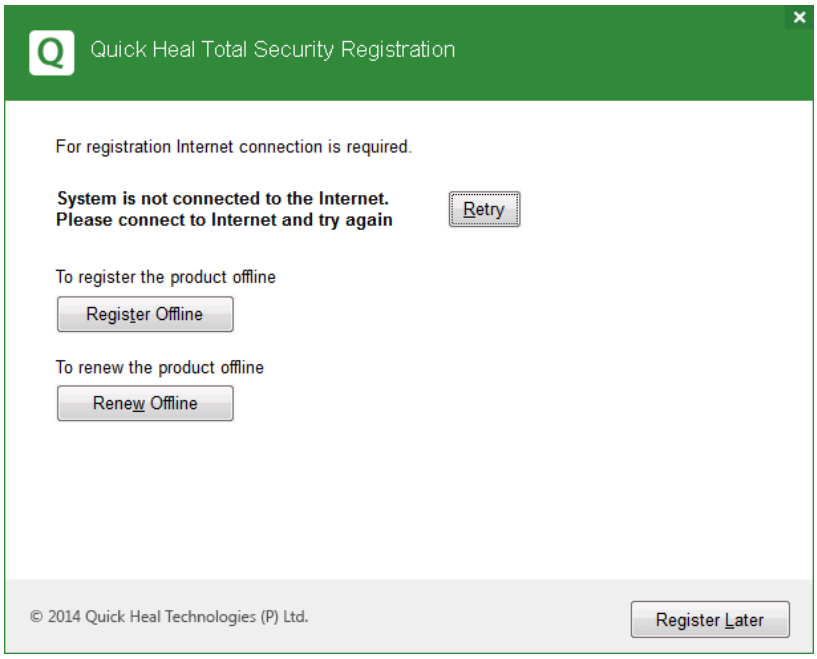


در انتها، پیغام نصب موفق آنتی‌ویروس نمایش داده می‌شود.

سیستم زمانی امن و بروز می‌شود که لایسنس محصول در نرم‌افزار ثبت (Register) شود. توصیه می‌شود بر روی دکمه *Register Now* کلیک کنید. در صورتی که می‌خواهید بعداً فرایند ثبت را انجام دهید دکمه *Register Later* را انتخاب نمایید.

برای فعالسازی، سیستم باید به اینترنت متصل باشد تا فرایند احراز اصالت با سرور کوییک‌هیل به صورت مستقیم صورت پذیرد (به علت اورجینال بودن).

ب) ثبت و فعالسازی (Register)



اگر سرور به اینترنت دسترسی نداشته باشد، پنجره فوق نمایش داده می‌شود. ابتدا سرور را به اینترنت متصل کرده و بر روی دکمه *Retry* کلیک کنید.

برای رجیستر کردن، سیستم باید به اینترنت متصل باشد. (برای مراکز حساس که امکان اتصال به اینترنت را ندارند، با نماینده کوییک‌هیل در ایران تماس بگیرید)

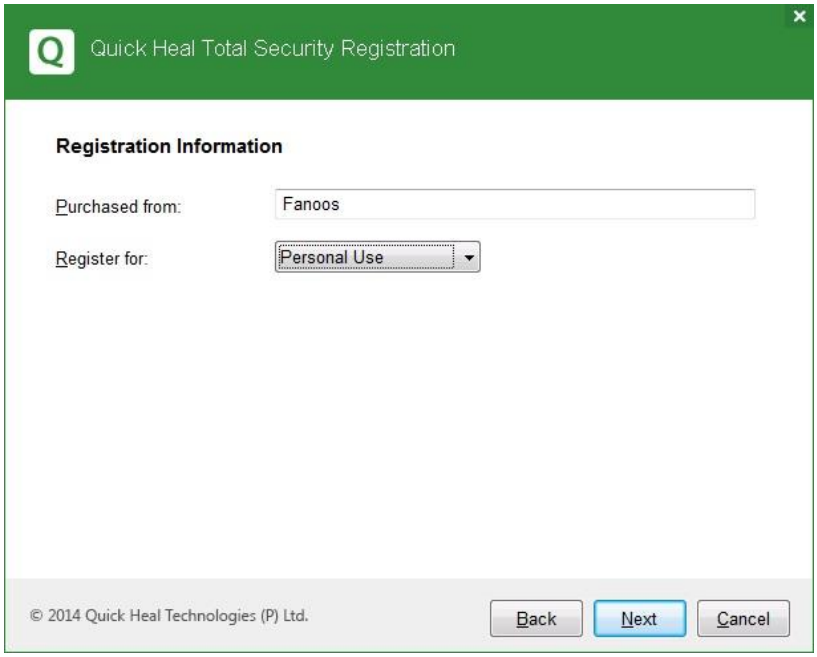
برای تست ارتباط صحیح اینترنتی، مرورگر اینترنت اکسپلورر (Internet Explorer) باید امکان مشاهده وب‌سایت quickheal.co.ir را داشته باشد. گزینه Work Offline مرورگر نباید تیک باشد.

لایسنس یا کلید محصول خود را وارد نمایید.

یادآوری ۱: اگر برای اولین بار اقدام به فعالسازی لایسنس آنتی‌ویروس کوییک‌هیل می‌نمایید، پس از وارد کردن لایسنس، در صفحات بعدی اطلاعات درخواستی را تکمیل نمایید.

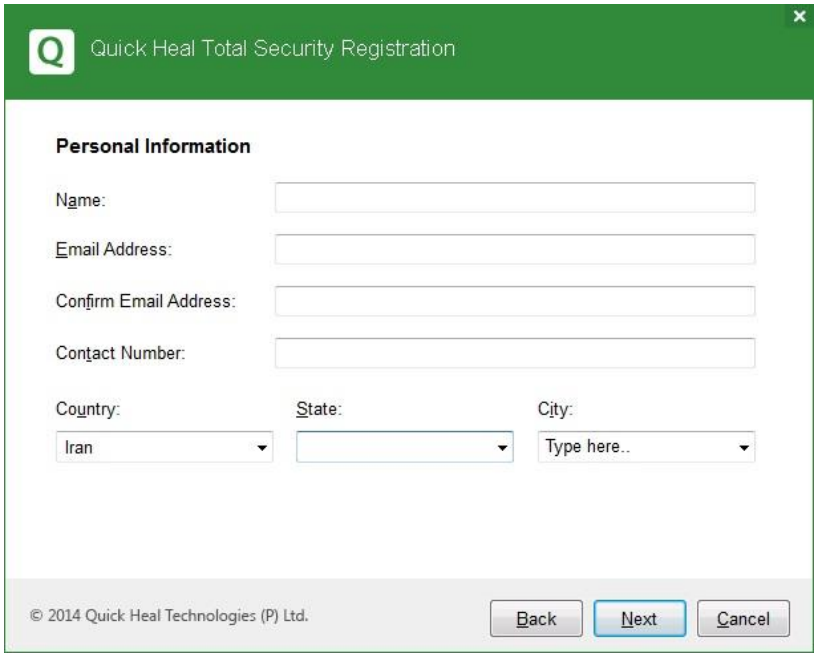
یادآوری ۲: هر لایسنس تنها بر روی یک سیستم قابل استفاده می‌باشد. در صورت استفاده بر روی چند سیستم لایسنس قفل خواهد شد.

یادآوری ۳: اگر به هر دلیلی ویندوز سیستم خود را تعویض کردید و می‌خواهید مجدداً کوییک‌هیل را بر روی آن نصب کنید، نیازی به خرید مجدد برای آن سیستم نمی باشد. پس از نصب مجدد کوییک‌هیل تنها کافی است همان لایسنس (کلید محصول) را وارد نمایید. سرور کوییک‌هیل به صورت خودکار تشخیص می‌دهد که اطلاعات سیستم مربوط به همان کاربر بوده و اطلاعات تماس ثبت شده کاربر را جهت تایید نشان می‌دهد. در صورتی که اطلاعات تماس صحیح می‌باشد، تایید نمایید. اگر لایسنس از قبل ثبت شده مربوط به شما نمی‌باشد ضمن Cancel کردن، با تیم پشتیبانی کوییک هیل (شرکت فناوری ارتباطات و اطلاعات فانوس) تماس بگیرید.



Purchased from: Fanoos
Register for: Personal Use

اطلاعات فوق را کامل نموده و بر روی *Next* کلیک کنید. در صفحه بعد اطلاعات مربوط به تماس خریدار تکمیل خواهد گردید.



در این صفحه اطلاعات تماس خریدار وارد می‌شود. لطفا اطلاعات صحیح را وارد نموده و بر روی *Next* کلیک کنید:

Name: نام و نام خانوادگی خود را وارد نمایید. (مثلاً Babak Karimi)

Email Address: آدرس ایمیل خود را وارد کنید. (مثلاً MyEmailID@yahoo.com)

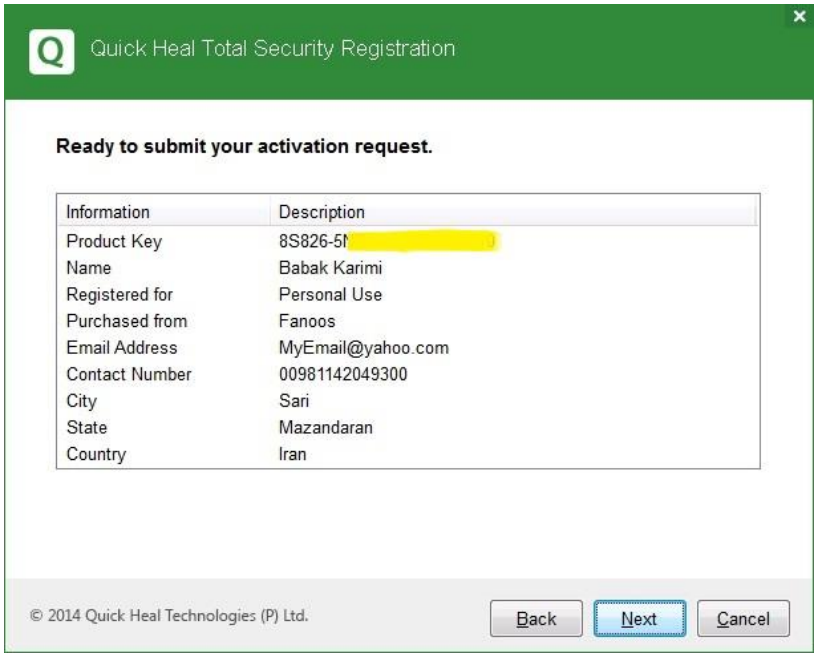
Confirm Email Address: آدرس ایمیل خود را مجدداً وارد نمایید.
(مثلاً MyEmailID@yahoo.com)

Contact Number: شماره موبایل یا تلفن خود را وارد نمایید. . (مثلا 00989111231234)

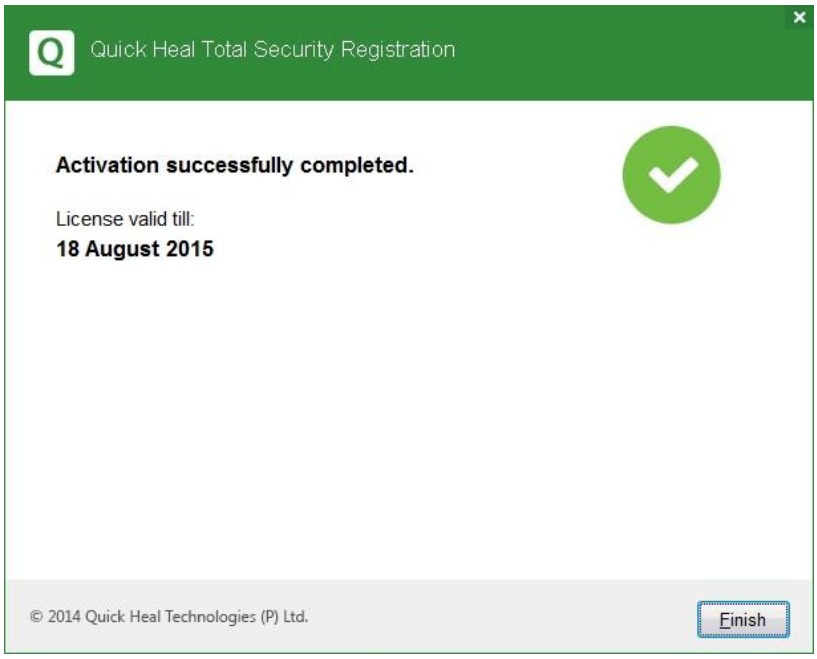
Country: کشور Iran را از لیست انتخاب کنید.

State: نام استان خود را وارد کنید. (مثلا Mazandaran)

City: نام شهر خود را وارد کنید. (مثلا Sari)



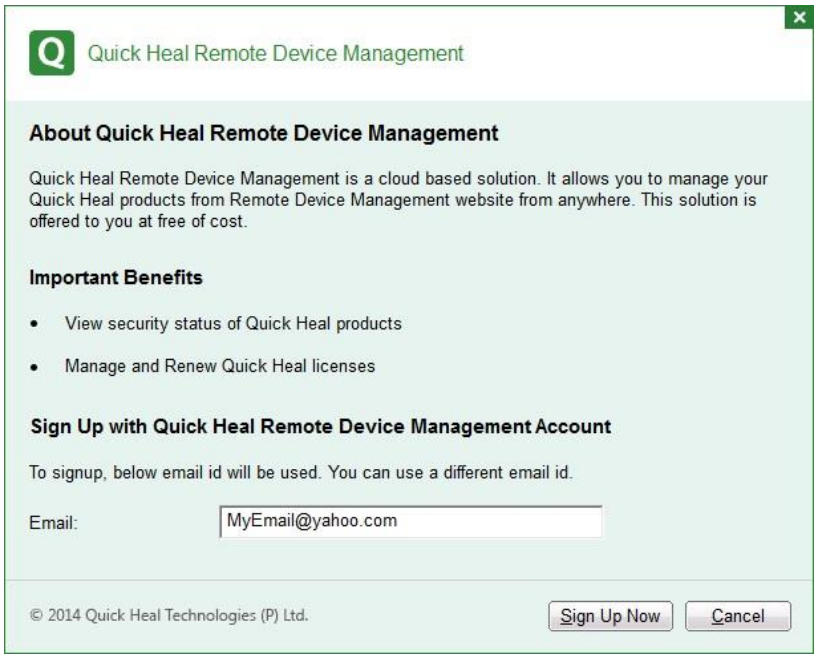
در این صفحه اطلاعات وارد شده توسط شما نشان داده می‌شود. در صورتی که اطلاعات نمایش داده شده صحیح است، بر روی *Next* و در غیر اینصورت برای ویرایش اطلاعات بر روی *Back* کلیک کنید.



در انتها پیام فعالسازی آنتی‌ویروس به صورت موفق نمایش داده خواهد شد.

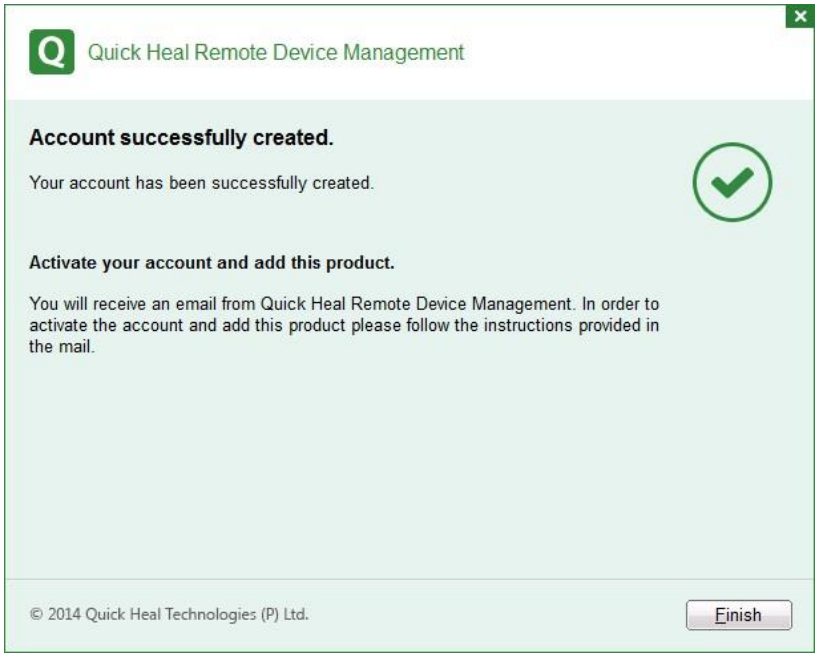
یادآوری: تاریخ انتهای لایسنس، بر اساس درخواست خرید شما در طرح جزیره امن خواهد بود. زمان انتهای لایسنس به صورت خودکار قابل افزایش و یا مسدود شدن (در صورت عدم پرداخت وجه می‌باشد) برای بررسی وضعیت لایسنس خود به بخش باشگاه مشتریان سایت 42722.ir مراجعه فرمایید.

ج) پورتال مدیریت ابزار راه دور (RDM)



پس از فعالسازی می‌توانید به صورت اختیاری از امکانات مدیریت راه دور ابزار کوییک‌هیل نیز به صورت رایگان استفاده نمایید. این صفحه به صورت خودکار پس از مدتی نشان داده خواهد شد. در صورت ثبت نام، بسته به نوع محصول خریداری شده، امکانات جالبی (مثل مشاهده وضعیت امنیتی سیستم، مدیریت از راه دور لایسنس، و یا در نسخه های موبایل و تبلت: امکان ردیابی گوشی، قفل کردن از راه دور در صورت سرقت و...) در پورتال راه دور فعال می‌گردد. برای ثبت نام کافی است ایمیل خود را وارد نموده و *Sign Up Now* را انتخاب نمایید.

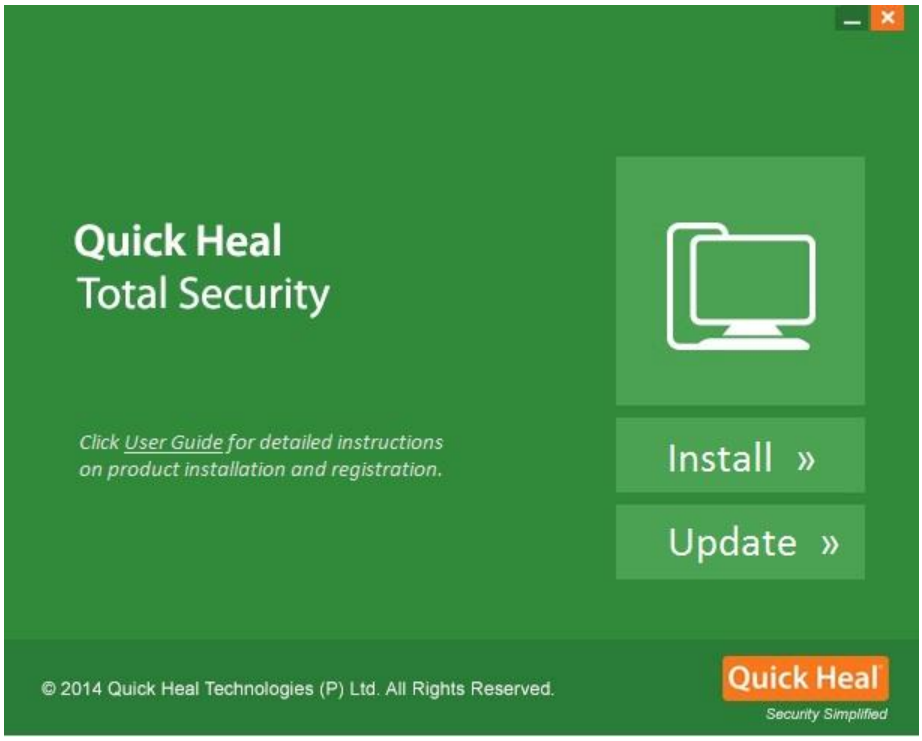
همچنین در صورت استفاده از چندین محصول کوییک‌هیل به صورت همزمان، می‌توانید با ورود به پورتال خود، لایسنس آنها را برای مدیریت متمرکز اضافه نمایید.



پس از ایجاد حساب کاربری، یک ایمیل فعالسازی به آدرس ایمیل شما ارسال می‌شود. لطفاً ایمیل خود را باز کرده و طبق راهنما بر روی لینک مربوطه کلیک نمایید.

د) بروزرسانی آفلاین (Update)

آنتی ویروس کوییک‌هیل پس از نصب و ثبت نام (Register) به صورت خودکار به اینترنت متصل شده و آپدیت می‌شود. با این حال امکان بروزرسانی به صورت آفلاین نیز پس از نصب و فعالسازی در نظر گرفته شده است. شما می‌توانید آخرین فایل‌های بروزرسانی را از سایت کوییک‌هیل به نشانی http://quickheal.co.ir/updates دانلود نمایید. در صفحه مربوطه بسته به نوع سیستم عامل (۳۲ یا ٦٤ بیتی) و همینطور مدت زمانی که سیستم شما بروز نشده (مثلا کمتر از یک هفته یا یک‌ماه، یا بیش از یک‌ماه و به صورت کلی) فایل آپدیت موردنظر خود را دانلود کنید.



همچنین درون DVD نصب نیز یک فایل آپدیت آفلاین قرارداده شده است. تاریخ این بروزرسانی بسته به زمان آماده‌سازی DVD متفاوت می‌باشد. شما می‌توانید پس از نصب و فعالسازی آپدیت اولیه را به صورت آفلاین از روی DVD انجام داده، سپس سیستم را به اینترنت متصل کرده و آخرین آپدیت‌ها را از اینترنت به صورت آنلاین دریافت نمایید. پس از اجرای آتوران DVD بر روی دکمه *Update* کلیک کنید.

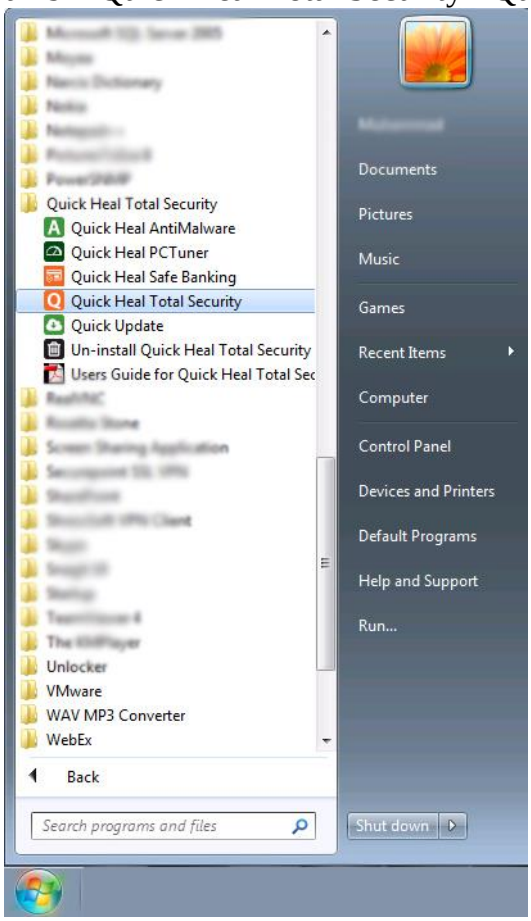
در صفحه بروزرسان کوییک‌هیل (Quick Heal Updater) دکمه Update Now را بفشارید.

بسته به سرعت سیستم چند دقیقه (حدود ۱۵ دقیقه) منتظر بمانید تا فرایند استخراج فایل‌های فشرده و اعمال بر پایگاه داده آنتی ویروس انجام پذیرد.

آغاز به کار آنتی ویروس کوییک‌هیل

۱. اجرای آنتی‌ویرس کوییک‌هیل:

Start > All Programs > Quick Heal Total Security> Quick Heal Total Security



نسخه اینترنت سکیوریتی کوییک هیل:

Start > All Programs > Quick Heal Internet Security> Quick Heal Internet Security

نسخه آنتی‌ویروس پرو کوییک هیل:

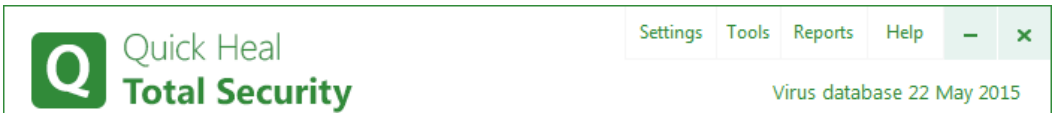
Start > All Programs > Quick Heal Antivirus Pro> Quick Heal Antivirus Pro

همچنین می‌توانید با دوبار کلیک بر روی آیکن کوییک‌هیل در نوار Tray (پایین سمت چپ کنار ساعت ویندوز) برنامه آنتی‌ویروس کوییک‌هیل را اجرا نمایید.

رنگ آیکن کوییک‌هیل بر اساس وضعیت امنیتی سیستم تغییر می‌کند. سبز نشانه امنیت کامل و نارنجی در حالت خطر و قرمز نیاز به اقدامات امنیتی می‌باشد. (مثلا در صورتی که آنتی‌ویروس برای مدتی آپدیت نشود، ابتدا نارنجی و پس از چند روز قرمز خواهد شد.)

داشبورد مدیریتی

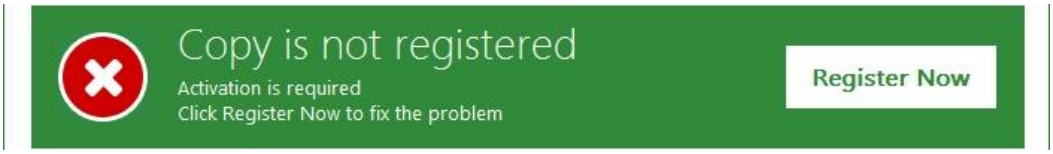
صفحه نخست (داشبورد پویا) اطلاعات کاملی از وضعیت امنیت سیستمی ارائه می‌دهد. همچنین امکان پیکربندی قابلیت‌های امنیتی آنتی‌ویروس وجود دارد. امکان اسکن و بهینه‌سازی نیز در بخش پایینی صفحه آورده شده است.



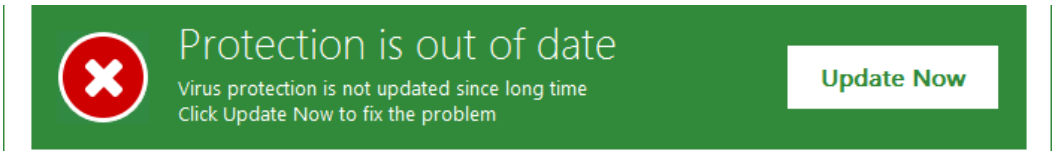
منوهای نرم افزار در نوار بالایی نرم‌افزار قابل دسترس است. تاریخ بروزرسانی آنتی‌ویروس در پایین منو (Virus database) نمایش داده می‌شود.

در نوار اطلاع‌رسانی، وضعیت امنیت سیستم نمایش داده می‌شود. در صورتی که نیاز به انجام کاری برای افزایش امنیت باشد، راهنمایی لازم در این بخش انجام می‌پذیرد.

نمونه‌هایی از اخطارها عبارتند از:



- رجیستر (ثبت نام) نکردن آنتی‌ویروس، پس از نصب می‌بایست آنتی‌ویروس را ثبت و فعال نمایید.

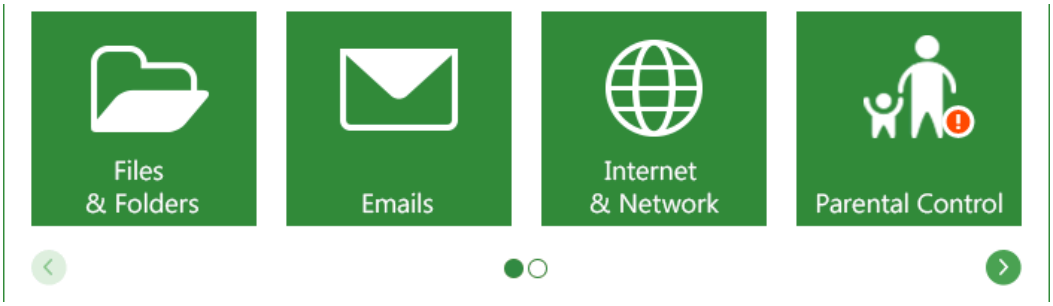


- به روز نبودن آنتی‌ویروس (معمولا به علت عدم اتصال به اینترنت)

- غیرفعال بودن محافظت ویروس (Virus Protection): با کلیک بر روی Resolve می‌توانید آنتی‌ویروس را فعال کنید.

- غیرفعال بودن بروزرسانی اتوماتیک: با کلیک بر روی Resolve گزینه Automatic Update که در Settings قرار دارد روشن می‌گردد.

- شناسایی ویروس در حافظه اصلی (RAM): با کلیک بر روی Resolve، سیستم راه اندازی مجدد شده و پیش از بارگذاری ویندوز، ویروس از بین می‌رود.



در بخش مرکزی، گزینه‌های مختلف امنیتی و محافظتی قابل پیکربندی می‌باشد. بسته به نیاز خود می‌توانید این گزینه‌ها را پیکربندی نمایید.

در باکس پایینی، گزینه های مختلف اسکن و ویروسیابی وجود دارد. همچنین امکان بهینه سازی سیستم با استفاده از برنامه PC Tuner وجود دارد.

آخرین اخبار امنیتی در این بخش نمایش داده خواهد شد. همچنین امکان لایک کردن کوییک هیل در فیسبوک، ارتباط با تیم پشتیبانی کوییک هیل و دسترسی به حساب کاربری در فضای ابری کوییک‌هیل وجود دارد.

با کلیک بر روی My Account به پورتال مدیریت از راه دور ابزار RDM خود دسترسی یافته و می‌توانید از آخرین اطلاعات وضعیت امنیتی همه آنتی‌ویروس‌های نصب شده بر روی رایانه، موبایل و تبلت خود مطلع شده و نسبت به پیکربندی متمرکز از راه دور آنها اقدام نمایید.

Quick Heal Protection Center (مرکز حفاظت کوییک هیل)

هنگام کار با رایانه، شما به اینترنت متصل می‌شوید، درایوهای خارجی را به سیستم متصل می‌کنید، ایمیل ارسال و دریافت می‌کنید. این ارتباطات موجب می‌شود تا سیستم شما در معرض ویروس‌هایی قرار گیرد که قصد دارند به رایانه شما نفوذ کنند. با ویژگی‌هایی که در مرکز حفاظت کوییک‌هیل قرار دارد، می‌توانید تنظیمات را به گونه ای پیکربندی نمایید تا سیستم‌ها، پوشه‌ها، فایل‌ها و داده‌های شما در برابر هرگونه تهدید بدافزارها، ویروس‌ها، کرم‌ها و سرقت اطلاعات امن بماند.

همچنین این ویژگی شرایط فعلی امنیتی کوییک‌هیل را نشان می‌دهد، اگر سیستم شما در معرض خطر باشد، یا یک تهدیدی شناسایی شود، رنگ‌بندی آیکن‌ها بیانگر این تغییرات می‌باشد.

رنگ آیکن کوییک‌هیل بدین معناست:

قرمز: نشان می‌دهد که کوییک‌هیل توتال سکیوریتی با بهترین تنظیمات پیکربندی نشده و نیاز فوری به توجه شما دارد. پیام متناسب با اقدام نمایش داده شده و برای حفظ امنیت سیستم باید فوری اقدام شود.

سبز: نشان می‌دهد که کوییک‌هیل توتال سکیوریتی با بهترین تنظیمات پیکربندی شده و سیستم شما درحال محافظت می‌باشد.

نارنجی: نشان می‌دهد که یک ویژگی کوییک‌هیل توتال سکیوریتی نیاز به توجه شما در زمان مناسب (نه به صورت فوری) دارد.

مرکز حفاظت کوییک‌هیل شامل ویژگی‌های جدید می‌باشد:

Files & Folders (فایل‌ها و پوشه‌ها)

شامل تنظیمات اسکن، محافظت ویروس، DNA Scan پیشرفته، مسدود کردن فایل‌های بسته‌بندی (Packed) شده مشکوک، اسکن آنتی‌ویروس‌های جعلی، زمانبندی اسکن، استثنا کردن فایل‌ها و پوشه‌ها، و قرنطینه و پشتیبان می‌باشد.

Emails (ایمیل‌ها)

شامل محافظت ایمیل، محافظت کلاینت‌های ایمیل مطمئن، و محافظت هرزنامه می‌باشد.

Internet & Network (اینترنت و شبکه)

شامل محافظت فایروال، محافظت مرور، محافظت بدافزار، محافظت فیشینگ (سایت‌های کلاهبردارانه)، سندباکس مرورگر، بانکداری امن، اخبار، و شناسایی و پیشگیری از نفوذ غیرمجاز (IDS/IPS) می‌باشد.

Parental Control (کنترل خانواده)

شامل تنظیماتی است که دسترسی به سایت‌ها را کنترل کرده و زمان دسترسی به اینترنت را برنامه‌ریزی می‌کند.

External Drives and Devices (دستگاه‌ها و درایوهای خارجی)

شامل محافظت اجرای خودکار (آتوران)، اسکن درایوهای خارجی، محافظت از سرقت اطلاعات، و اسکن موبایل در ویندوز می‌باشد.

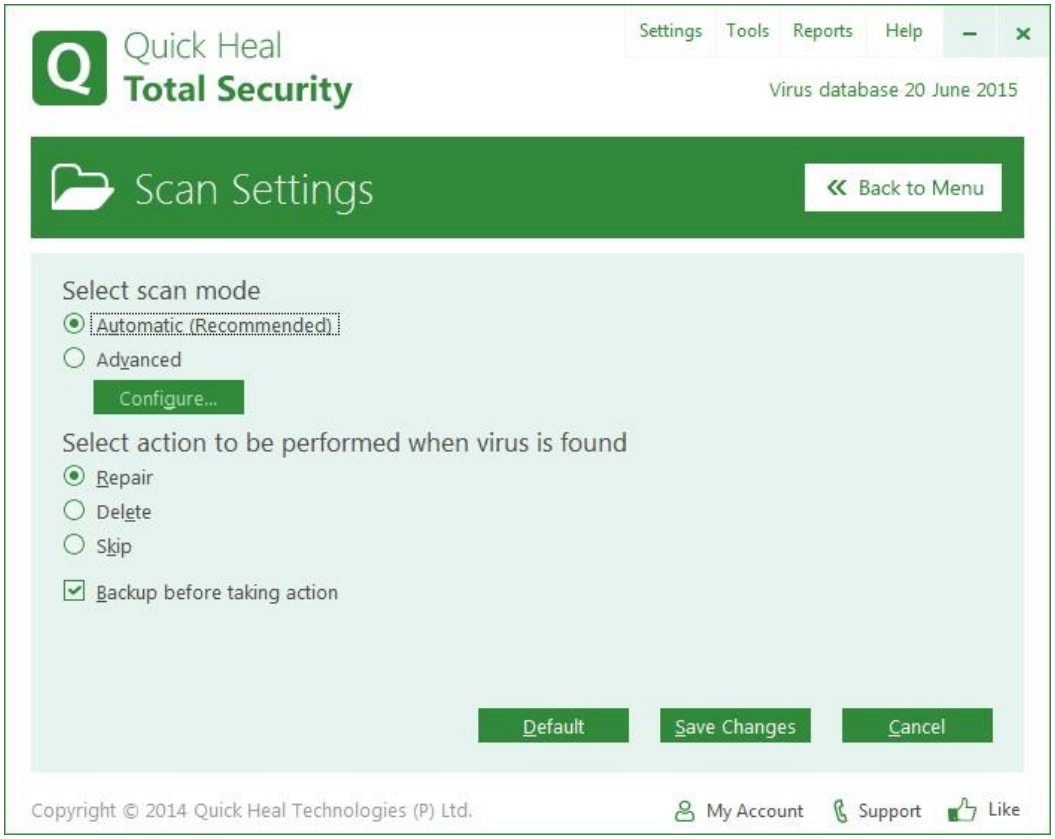
Files & Folders (فایل‌ها و پوشه‌ها)

با کلیک بر روی اولین هسته امنیتی، شما می‌توانید تنظیمات حفاظتی فایل‌ها و پوشه‌های رایانه خود را پیکربندی نمایید.

در ادامه به شرح ویژگی‌های مختلف این بخش می‌پردازیم.

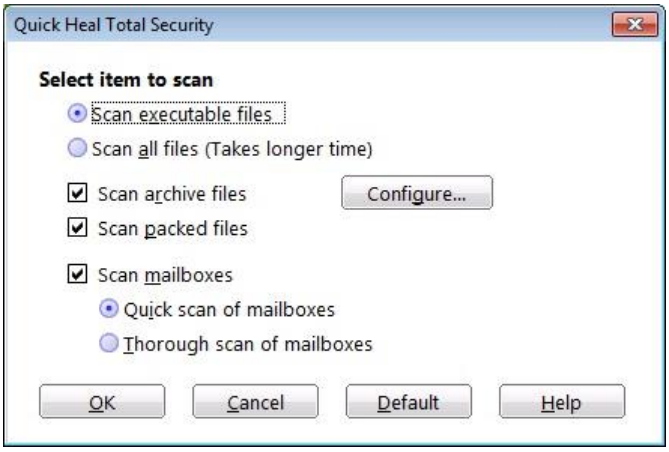
الف) Scan Settings (تنظیمات اسکن)

با کلیک بر روی *Scan Settings* می‌توانید نحوه اسکن سیستم و اقدامی که پس از شناسایی ویروس صورت می‌پذیرد را مشخص کنید. با این حال، تنظیمات پیش فرض بهینه شده و حداکثر محافظت سیستم درنظر گرفته شده است. بنابراین کاربران نیازی به تغییر تنظیمات ندارند.



Select scan mode: در بخش انتخاب حالت اسکن، دو گزینه *Automatic (Recommended)* (خودکار (توصیه شده)) و *Advanced* (پیشرفته) برای انتخاب سطوح پیشرفته‌تر اسکن می‌باشد.

توصیه می‌شود گزینه پیش‌فرض یعنی *Automatic (Recommended)* را انتخاب شده بگذارید تا بهترین امنیت در پیکربندی اسکن درنظر گرفته شود.



اما اگر گزینه *Advanced* را انتخاب کنید، با کلیک بر روی دکمه *Configure* صفحه زیر اجرا می‌شود و کاربر می‌تواند تنظیمات پیشرفته‌تری را انجام دهد.

Select action to be performed when virus is found: در این قسمت اقدامی که در زمان پیدا شدن یک ویروس، کوییک‌هیل باید انجام دهد را تعیین می‌کنید. اقدامات بر روی ویروس اسکن و پیدا شده شامل:

Repair: اگر در هنگام اسکن، یک فایل ویروسی پیدا شد، آن را تعمیر می‌کند. اگر قابل تعمیر نباشد، آن را به صورت خودکار قرنطینه می‌کند. اگر فایل آلوده حاوی یک درب پشتی (Backdoor)، کرم (Worm)، تروجان (Trojan)، یا بدافزار (Malware) باشد، کوییک‌هیل توتال سکیوریتی به صورت خودکار آن فایل را حذف می‌کند.

Delete: اگر این گزینه انتخاب شود، فایل آلوده شناسایی شده، بدون اعلان اخطار به کاربر حذف می‌شود. فایل ها پس از حذف امکان بازیابی ندارند.

Skip: اگر می‌خواهید هیچ اقدامی بر روی فایل آلوده شناسایی شده انجام نگیرد، این گزینه را انتخاب کنید.

Backup before taking action: اگر این گزینه فعال باشد، اسکنر کوییک‌هیل پیش از رفع آلودگی فایل‌های آلوده، از آنها پشتیبان می‌گیرد. فایل‌های پشتیبان گرفته شده، از بخش قرنطینه (Quarantine) قابل بازیابی می‌باشند.

ب) Virus Protection (محافظت ویروس)

ویروس‌ها از منابع گوناگون مانند پیوست‌های ایمیل، دانلودهای اینترنتی، نقل و انتقال فایل، و اجرای فایل، تلاش می‌کنند تا سیستم شما را آلوده سازند. این ویژگی کمک می‌کند تا سیستم به صورت مداوم و مستمر برای نفوذ ویروس‌ها تحت نظر و مانیتورینگ باشد. نکته مهم این ویژگی کوییک‌هیل این است که فایل‌هایی که پس از اسکن قبلی، تغییر نیافته‌اند را اسکن مجدد نمی‌کند (اسکن مارک دار). این قابلیت منابع مصرفی سیستم را کاهش داده و موجب افزایش سرعت کار با سیستم می‌گردد.

توصیه می‌شود که Virus Protection را همواره روشن (ON) بگذارید تا سیستم شما در برابر انواع تهدیدات بالقوه پاک و امن باقی بماند. اگرچه به صورت پیش‌فرض این گزینه روشن می‌باشد.

Display alert messages: اگر می‌خواهید پیام‌ها و اعلان‌های مختلف مربوط به وقایع مختلف مانند زمانی که بدافزار شناسایی شد را دریافت کنید، این گزینه را انتخاب کنید. به صورت پیش‌فرض فعال است.

Select action to be performed when virus is detected: اقدامی که پس از یافتن یک ویروس در هنگام اسکن روی خواهد داد را در این بخش تعیین می‌کنید:

Repair: اگر در هنگام اسکن، یک فایل ویروسی پیدا شد، آن را تعمیر می‌کند. اگر قابل تعمیر نباشد، آن را به صورت خودکار قرنطینه می‌کند.

Delete: اگر این گزینه انتخاب شود، فایل آلوده شناسایی شده، بدون اعلان اخطار به کاربر حذف می‌شود. پس از حذف فایل ها، امکان بازیابی وجود ندارد.

Deny access: در این حالت دسترسی به فایل آلوده به ویروس توسط کوییک هیل امکان پذیر نمی‌باشد.

Backup before taking action: اگر این گزینه فعال باشد، کوییک‌هیل پیش از انجام هر اقدامی بر روی فایل‌های آلوده از آنها پشتیبان می‌گیرد. فایل‌های پشتیبان گرفته شده از بخش قرنطینه (Quarantine) قابل بازیابی می‌باشند.

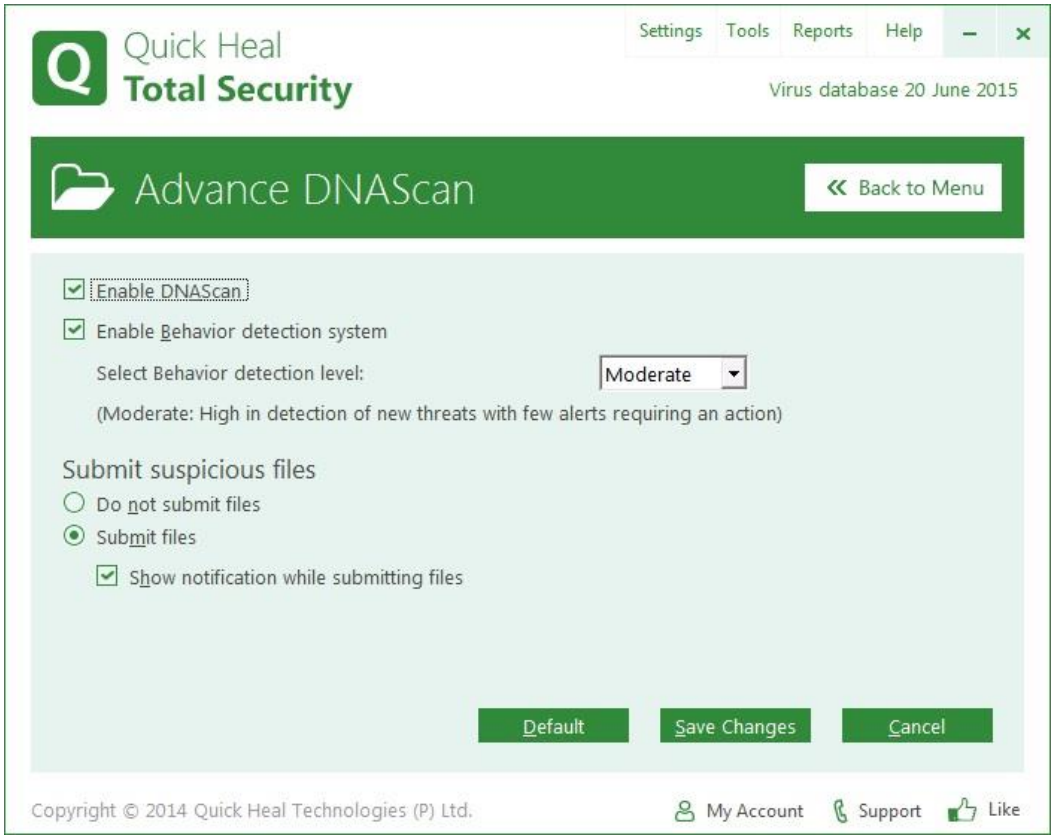
Enable sound when threat is detected: اگر می‌خواهید در زمان شناسایی ویروس، اعلان صوتی پخش شود، این گزینه را تیک کنید.

ج) Advance DNAScan (دی.ان.ای اسکن پیشرفته)

ویژگی DNAScan یک فناوری منحصربفرد و ابداعی کوییک‌هیل می‌باشد که تهدیدات مخرب ناشناخته و جدید را شناسایی و نابود می‌کند. تکنولوژی DNAScan پیشرفته با موفقیت و با کمترین اخطارهای اشتباه، فایل‌های مشکوک را به تله می‌اندازد. علاوه بر این فایل مشکوک را قرنطینه کرده و در نتیجه بدافزار نمی‌تواند به سیستم شما آسیب رساند. این فناوری یک لابراتوار مجازی در هر سیستم تشکیل می‌دهد که ویروس‌های جدید و ناشناخته را شناسایی می‌کند.

می‌توان فایل‌های مشکوک قرنطینه شده را برای آنالیز بیشتر به آزمایشگاه ویروس‌شناسی کوییک‌هیل ارسال کرد تا تهدیدات جدید ردیابی شده و به موقع آنها را تحت کنترل درآورد.

پس از آنالیز تهدید، امضاهای تهدیدات شناخته شده به پایگاه داده افزوده شده ودر بروزرسانی‌های آتی به همه کاربران ارسال خواهد شد.



گزینه های پیکربندی به شرح زیر می‌باشند:

Enable DNAScan: انتخاب این گزینه سبب فعال شدن ویژگی DNAScan می‌گردد.

Enable Behavior detection system: اگر می‌خواهید سامانه رفتارشناسی (Behavior detection system) را فعال کنید، این گزینه را انتخاب کنید. رفتار برنامه‌های درحال اجرا تحت مانیتور و

رصد قرار می‌گیرد. همچنین می‌توانید از لیست سطوح رفتارشناسی یک سطح اعلان امنیتی شامل بالا (High)، متوسط (Moderate)، یا پایین (Low) را انتخاب نمایید.

High: اگر این گزینه انتخاب شده باشد، کوییک‌هیل توتال سکیوریتی به صورت دقیق رفتار برنامه های درحال اجرا را مانیتور کرده و در صورت هرگونه رفتار *غیرمعمول* برنامه، اعلان مناسب را نشان می‌دهد. در این حال ممکن است کاربر اخطارهای زیادی حتی در برخی مواقع که فایل‌های معتبر باشند، دریافت کند.

Moderate: اگر این گزینه انتخاب شده باشد، کوییک‌هیل توتال سکیوریتی زمانی اخطار می‌دهد که رفتار مشکوک از برنامه های درحال اجرا مشاهده کند.

Low: اگر این گزینه انتخاب شده باشد، کوییک‌هیل توتال سکیوریتی تنها زمانی اخطار می‌دهد که رفتار مخرب از برنامه های درحال اجرا مشاهده کند.

توجه: اگر سطح امنیتی Moderate یا Low را انتخاب کنید، سامانه رفتارشناسی همچنین بسیاری از تهدیدات ناشناخته را در پس‌زمینه بدون نشان دادن پیام یا درخواست اقدام از سوی کاربر برای رفتار مشکوک برنامه یافت شده، مسدود می‌کند.

Do not submit files: اگر می‌خواهید فایل‌های مشکوک به آزمایشگاه تحقیقاتی کوییک‌هیل ارسال نشود، این گزینه را تیک نمایید.

Submit files: اگر این گزینه تیک باشد، فایل‌های مشکوک برای آنالیز بیشتر به لابراتوار کوییک‌هیل ارسال می‌گردد.

Show notification while submitting files : اگر می‌خواهید پیش از ارسال فایل، به شما پیغام نشان داده و منتظر تایید شما بماند، این گزینه را تیک نمایید. اگر این گزینه فعال نباشد، فایل‌های مشکوک بدون اعلان به کوییک‌هیل ارسال خواهد شد.

DNAScan پیشرفته با مطالعه ویژگی‌های کاراکتری و رفتار فایل‌ها، آنها را شناسایی می‌کند.

شناسایی از طریق کاراکتر

روزانه هزاران تهدید چندشکلی (با تغییر اطلاعات کد/فایل) متولد می‌شوند. شناسایی همه آنها از طریق امضا نیاز به زمان دارد. فناوری DNAScan پیشرفته چنین تهدیداتی را به صورت بلادرنگ و بدون وقفه شناسایی می‌کند.

زمانی که DNAScan یک تهدید مخرب جدید را در سیستم‌تان شناسایی می‌کند، آن فایل را قرنطینه کرده و یک پیغام به همراه نام فایل نمایش می‌دهد. با این حال اگر فایل شناسایی شده، معتبر و جنیون می‌باشد، می‌توانید آن فایل را با گزینه فراهم شده در پنجره پیغام، از قرنطینه بازیابی نمایید.

شناسایی از طریق رفتار

اگر سامانه رفتارشناسی (Behavior detection system) فعال باشد، DNAScan به طور مداوم و مستمر فعالیت‌های اجرا شده توسط برنامه‌ها در سیستم شما را مانیتور می‌کند. اگر رفتار یک برنامه از حالت نرمال خود منحرف گردد، یا فعالیت مشکوکی انجام دهد، سامانه رفتارشناسی اجرای برنامه را متوقف کرده و از آسیب رساندن احتمالی به سیستم شما جلوگیری می‌کند.

به محض شناسایی یک برنامه مشکوک، یک پیغام مناسب نشان داده و گزینه‌های اقدام زیر توسط کاربر قابل انتخاب است:

Allow: اگر از اصل و معتبر بودن آن برنامه مطمئن هستید، با انتخاب این گزینه اجازه اجرای آن برنامه را می‌دهید.

Block: زمانی که می‌خواهید اجرای یک برنامه را مسدود کنید، این گزینه را انتخاب نمایید.

د) Block Suspicious Packed Files (مسدود کردن فایل‌های بسته‌ای مشکوک)

فایل‌های بسته‌بندی شده مشکوک، برنامه‌های مخربی هستند که فشرده یا بسته‌بندی شده و با استفاده روش‌های گوناگون رمزنگاری شده‌اند. زمانی که این فایل‌ها از حالت بسته بندی خارج می‌شوند، می‌توانند موجب بروز آسیب‌ها و زیان‌های جدی به سیستم های رایانه‌ای گردند. این ویژگی به شما کمک می‌کند تا چنین فایل‌های بسته‌ای مشکوک را شناسایی و مسدود نمایید.

توصیه می‌شود برای جلوگیری از دسترسی فایل‌های مشکوک بسته‌ای و انتشار آلودگی، این گزینه را همچنان ON بگذارید.

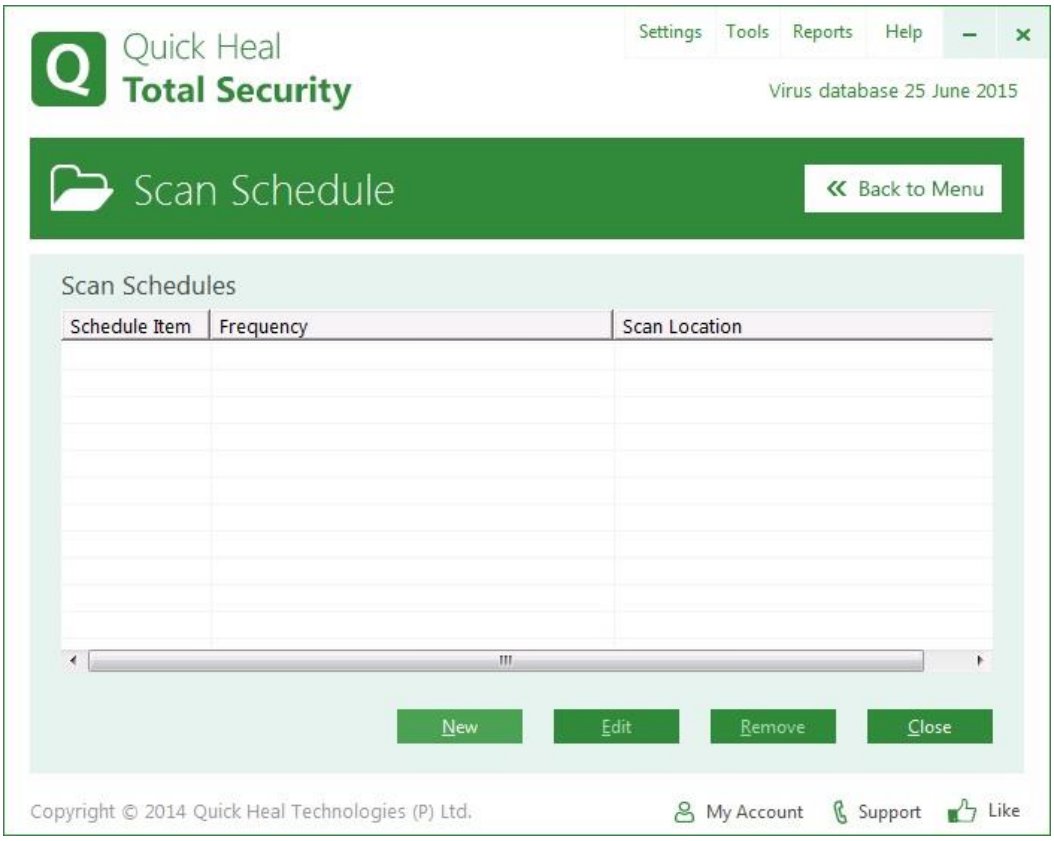
هـ) Automatic Rogueware Scan (اسکن خودکار آنتی‌ویروس جعلی)

این ویژگی به صورت خودکار rogueware‌ها و نرم‌افزارهای آنتی‌ویروس جعلی را اسکن و حذف می‌کند. اگر این ویژگی فعال باشد، همه فایل‌ها برای وجود یک فایل rogueware اسکن می‌شود.

به صورت پیش فرض این گزینه فعال است.

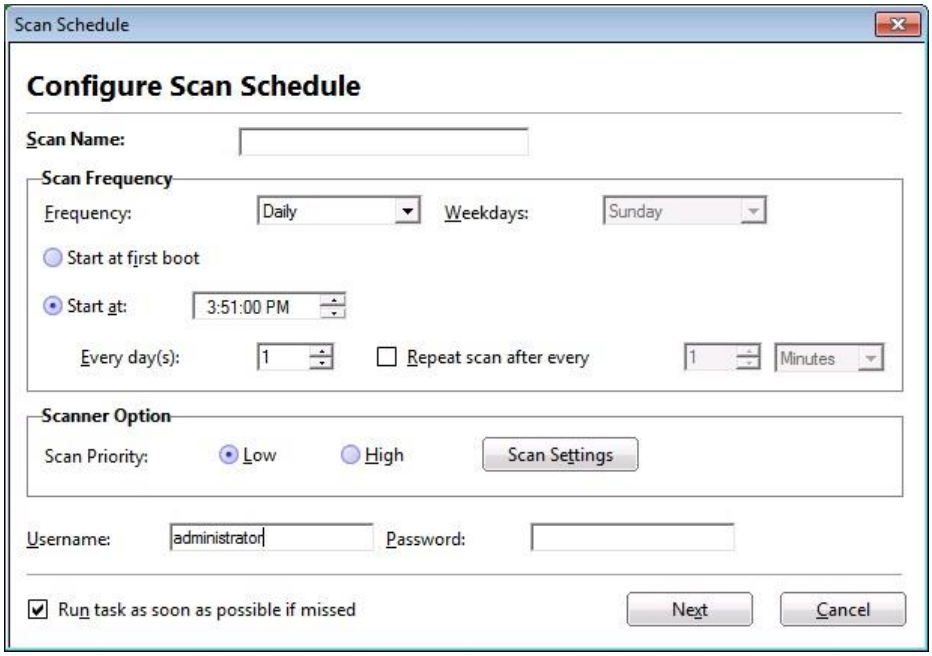
و) Scan Schedule (زمانبندی اسکن)

با استفاده از این ویژگی می‌توانید یک زمانبندی اسکن خودکار تعریف نمایید. امکان تعریف چندین برنامه زمانبندی اسکن به صورت دلخواه وجود دارد. اسکن منظم سیستم موجب می‌شود تا رایانه شما از ویروس‌ها و دیگر انواع آلودگی آزاد شود.



در این صفحه می‌توانید زمانبندی‌های اسکن موجود را ویرایش (*Edit*) و یا حذف (*Remove*) نماید.

برای افزودن یک برنامه زمانبندی جدید بر روی *New* کلیک کنید.



گزینه های پیکربندی زمانبندی اسکن عبارتند از:

Scan Name: یک نام برای زمانبندی اسکن تعیین نمایید. (مثلاً DailyScan)

Scan Frequency: در این بخش می‌توانید دوره و تکرار اسکن را مشخص کنید.

Daily: اگر می‌خواهید سیستم شما به صورت روزانه اسکن شود، این گزینه را انتخاب کنید. به صورت پیش‌فرض این گزینه انتخاب شده است.

Weekly: اگر می‌خواهید در روز خاصی از هفته (مثلا پنج‌شنبه‌ها) سیستم شما اسکن شود، این گزینه را انتخاب کنید. با انتخاب هفتگی (Weekly)، لیست بازشونده‌ی روز هفته (Weekdays:) فعال می‌شود که از این لیست می‌توانید روز موردنظر خود را انتخاب کنید.

Start at first boot: با انتخاب این گزینه، کوییک‌هیل در اولین راه‌اندازی سیستم اسکن خواهد شد. اگر این گزینه را فعال کنید، نیازی به تعیین زمان اسکن روز ندارید. فرایند اسکن و ویروسیابی در اولین راه‌اندازی سیستم صرف‌نظر از زمان روشن کردن سیستم، اجرا خواهد شد.

Start at: برای اجرای اسکن سیستم در زمان خاص، این گزینه را انتخاب کنید. با انتخاب این گزینه، می‌توانید زمان دقیق شروع اسکن را در فیلد مقابل تعیین نمایید. این گزینه به صورت پیش فرض فعال است.

شما می‌توانید تکرار اسکن را در هر چند روز / هفته یکبار با گزینه *Everyday* یا *Every Weekday* تعیین کرده و تکرار اسکن پس از چند دقیقه یا ساعت را نیز با *Repeat scan after* مشخص کنید.

Scan priority: اولویت اسکن در این بخش تعیین می‌گردد.

High: می‌توانید اولویت اسکن را بالا تعیین کنید.

Low: می‌توانید اولویت اسکن را پایین تعیین کنید. این گزینه به صورت پیش فرض انتخاب است.

در بخش تنظیمات اسکن (Scan Settings)، می‌توانید حالت اسکن را تعیین، گزینه‌های پیشرفته اسکن را تعریف، اقدامی که در زمان یافتن ویروس باید انجام گیرد، و آیا پیش از انجام هر اقدامی از فایل‌ها پشتیبانی گرفته شود یا خیر را مشخص کنید. اگرچه تنظیمات پیش‌فرض برای حفظ پاکسازی و امنیت سیستم شما کافی است.

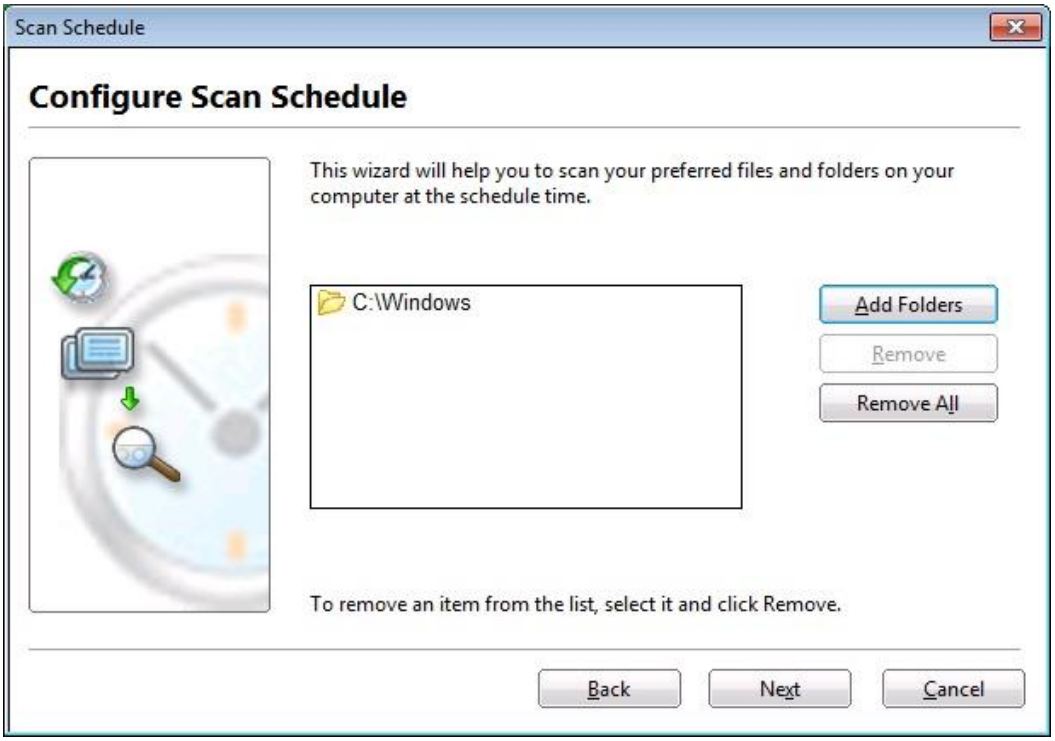
Username: نام کاربری ویندوز خود را در این بخش وارد نمایید.

Password: رمزعبور ویندوز خود را در این بخش وارد نمایید.

Run task as soon as possible if missed: اگر این گزینه را انتخاب کنید، زمانی که زمانبندی اسکن از دست رفته باشد، در اسرع وقت اجرا خواهد شد. هنگامی که سیستم شما خاموش باشد، و زمان اجرای زمانبندی اسکن بگذرد، بعداً هر وقت که سیستم را روشن کردید، اسکن زمانبندی به صورت خودکار در اسرع وقت اجرا خواهد شد.

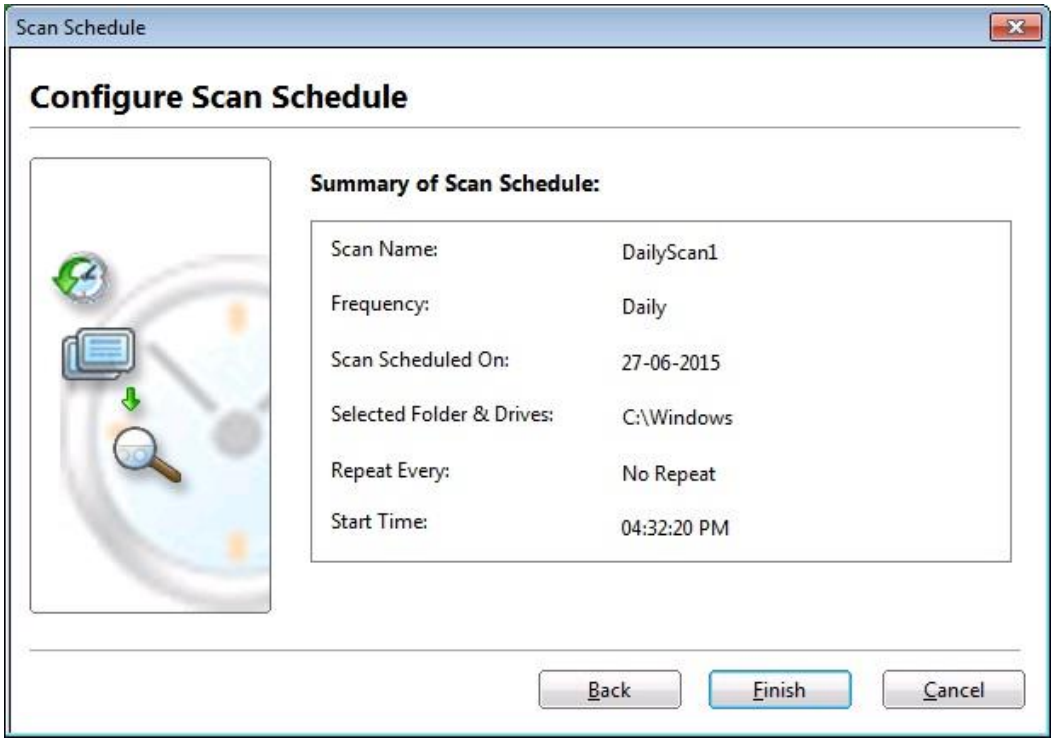
این گزینه از ویندوز ویستا به بعد قابل اجرا است.

با کلیک بر روی *Next* می‌توانید پوشه‌های مورد نظر خود برای اسکن را بیفزایید.



در صفحه جدید دکمه *Add Folders* را کلیک کنید. در پنجره Browse for Folder درایوها و پوشه‌هایی که می‌خواهید در دوره های زمانی تعیین شده اسکن شوند را انتخاب کنید.

شما می‌توانید چندین درایو یا پوشه را به صورت دلخواه انتخاب کنید. اگر می‌خواهید زیرشاخه‌ها اسکن نشوند و فقط محتویات پوشه اصلی اسکن شود گزینه *Exclude Subfolder* را انتخاب کنید.



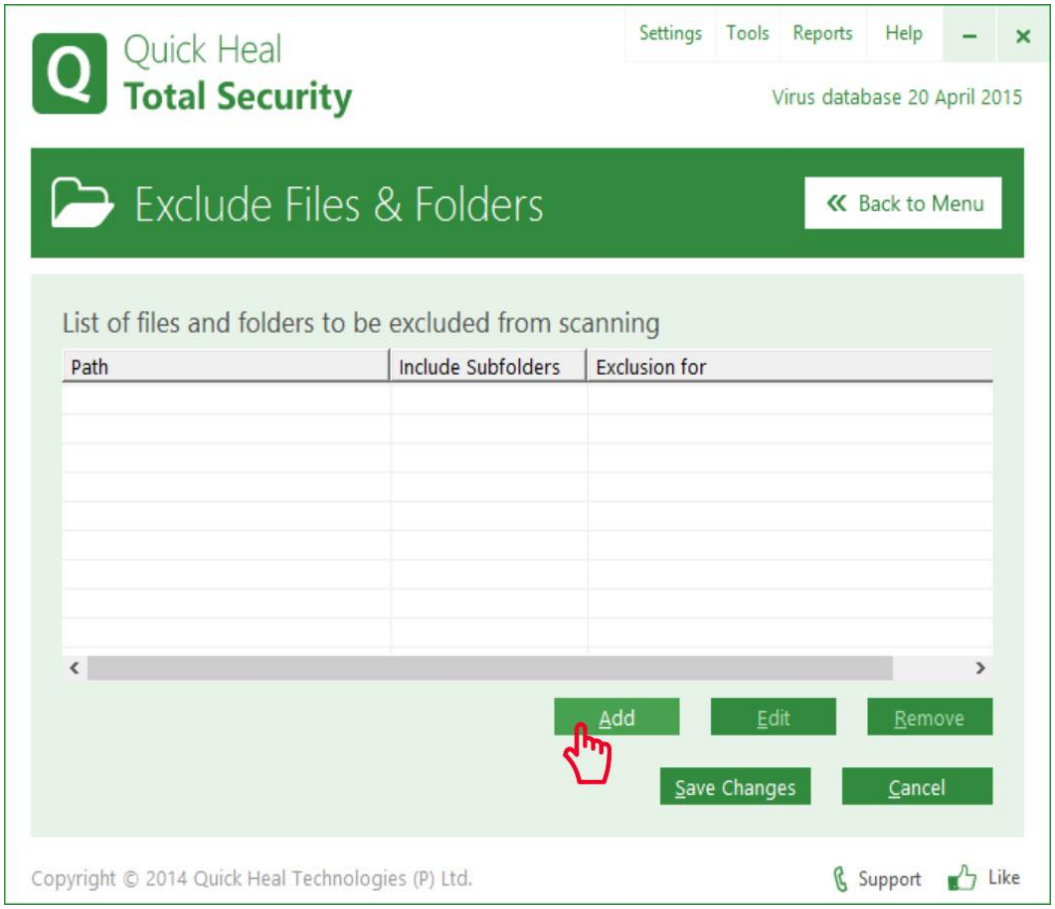
در انتها خلاصه ای از تنظیمات پیکربندی را می‌توانید مشاهده کنید. در صورتی که پیکربندی صحیح می‌باشد، برای ذخیره بر روی *Finish* کلیک کنید. برای ویرایش بر روی *Edit* و یا برای لغو تنظیمات بر روی *Cancel* کلیک کنید.

ز) Exclude Files & Folders (استثنا کردن فایل‌ها و پوشه‌ها)

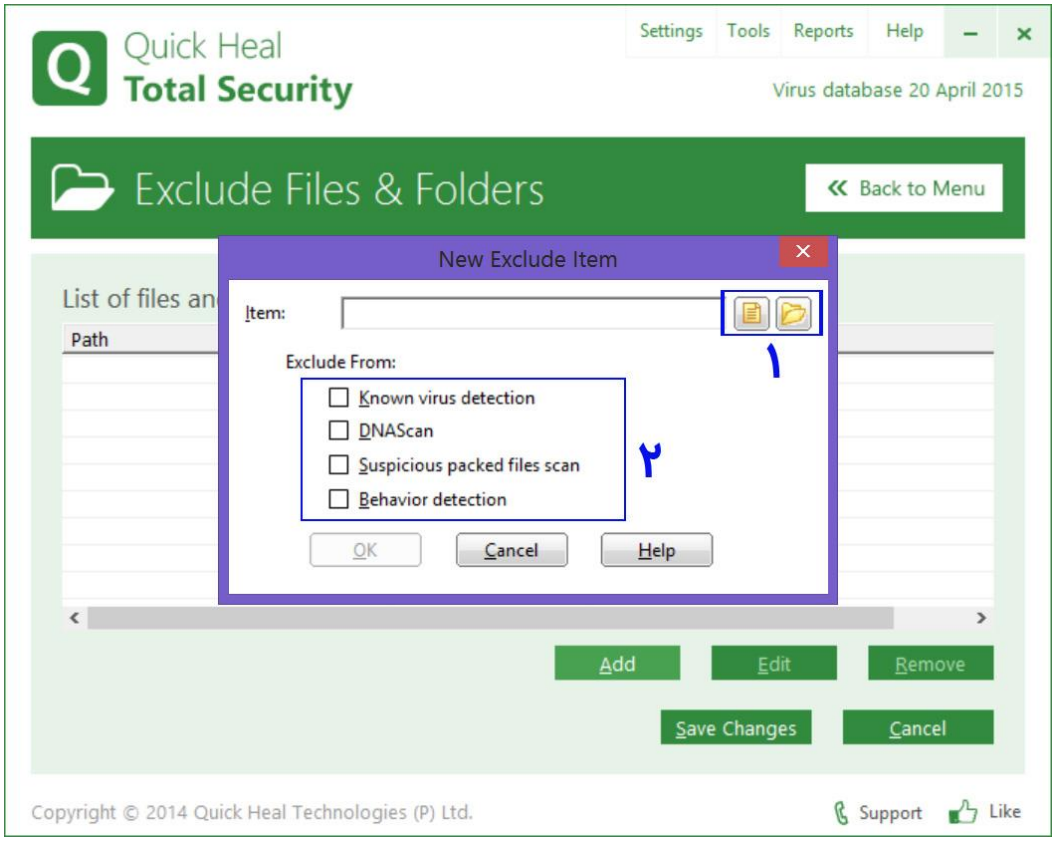
با استفاده از این ویژگی می‌توانید تصمیم بگیرید که کدام فایل‌ها یا پوشه‌ها در زمان اسکن نباید برای ویروس‌های شناخته شده، DNAScan، فایل‌های بسته‌ای مشکوک، و رفتار شناسی ویروسیابی شوند.

در برخی موارد کاربران مایلند تا درایو، پوشه یا فایل خاصی که ویروسی نیز می‌باشد (مانند Keygen، Crack، درایور قفل‌های سخت‌افزاری غیرمجاز، برخی پچ‌های نرم‌افزاری ایرانی و...) را در کامپیوتر خود نگه دارند. کوییک‌هیل برای این دسته از کاربران ویژگی خاصی به نام Exclude را تعریف کرده است تا فایل یا پوشه مورد نظر را از ویروسیابی مستثنی کرده و در عین حال از انتشار آن جلوگیری می‌کند. پیشنهاد می‌شود همه‌ی فایل‌های آلوده (کرک، کی‌جن و...) را در یک پوشه (مثلا D:\install*.*) قرار داده و آن پوشه را استثناء کنید.

همچنین ممکن است شما فایل‌ها یا پوشه‌هایی داشته باشید که قبلا اسکن شده یا از آلوده نبودن آن مطمئن هستید، برای جلوگیری از اسکن غیرضروری فایل‌ها می‌توانید آنها را استثناء کنید. فایل‌های استثناء شده در این بخش در ماژول‌های زیر اثر می‌گذارد: اسکنر (Scanner)، محافظت بلادرنگ ویروس (Virus Protection)، اسکن حافظه (Memory Scanner) و DNAScan.



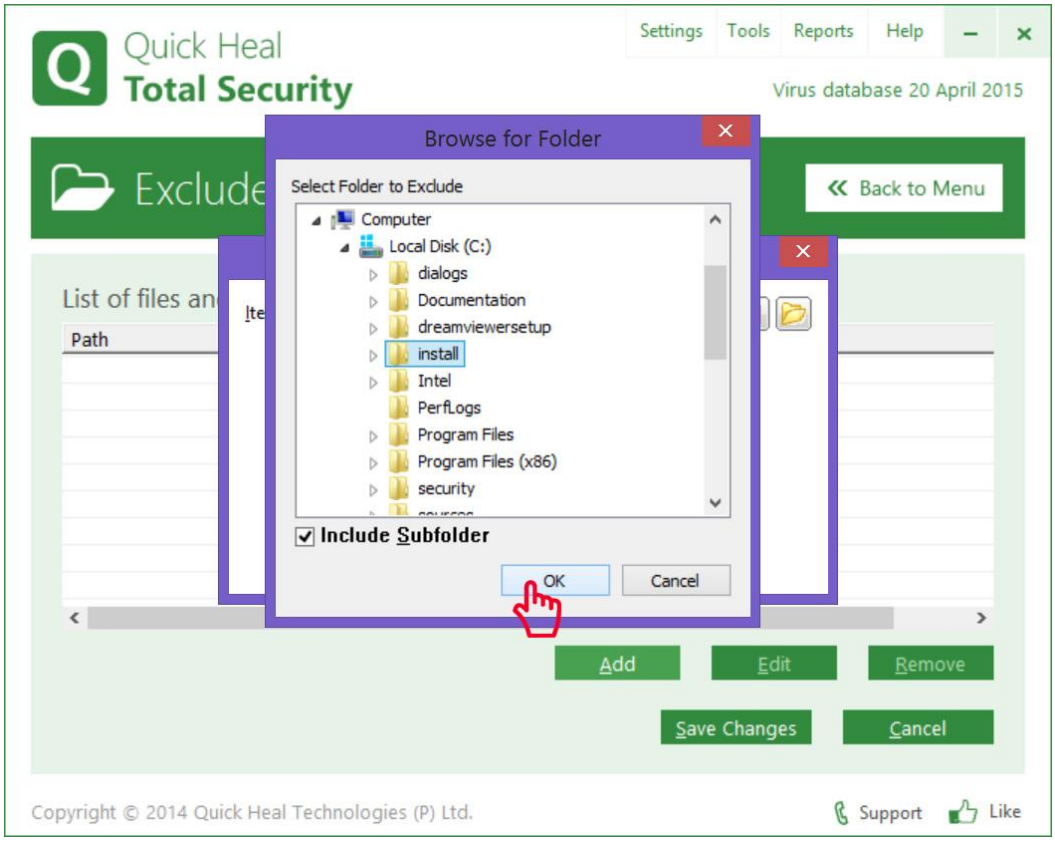
در پنجره Exclude Files & Folders دکمه Add را کلیک می‌کنیم:



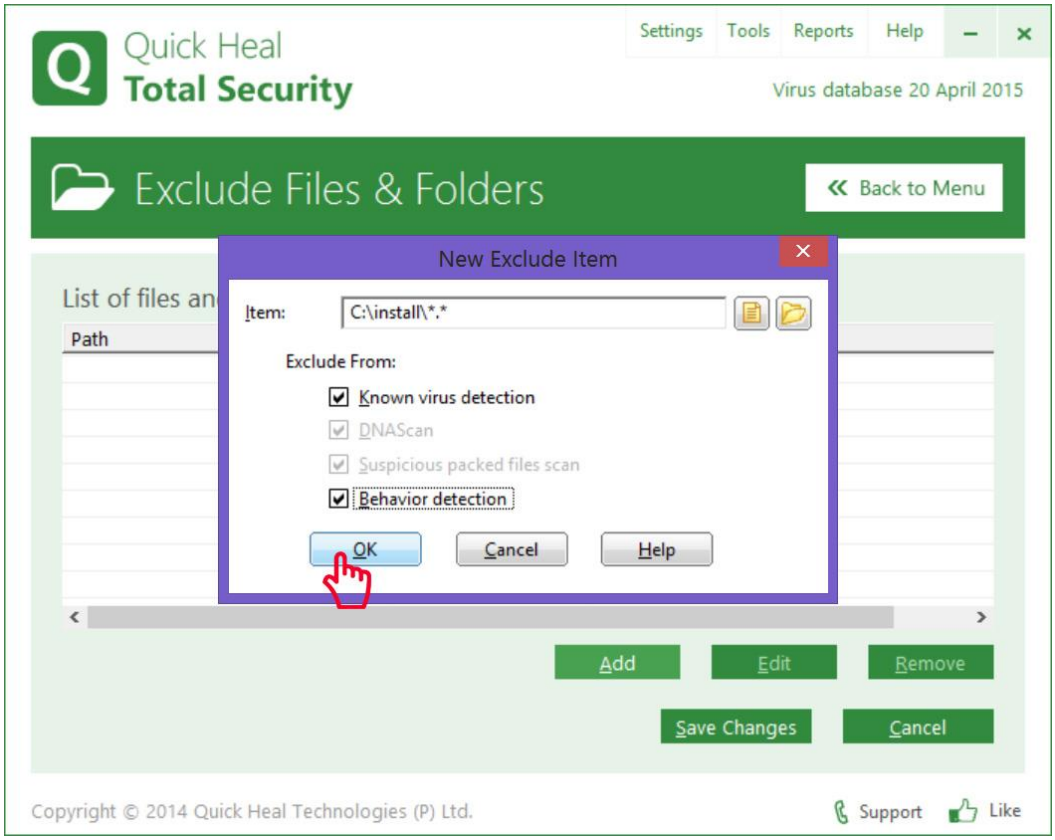
پنجره New Exclude Item باز می‌شود که به شرح زیر قابل تنظیم می‌باشد:

در قسمت (۱) دو دکمه فایل و فولدر وجود دارد. با توجه به نوع آیتمی که می‌خواهید استثناء کنید (فایل یا پوشه)، بر روی دکمه مورد نظر کلیک نمایید.

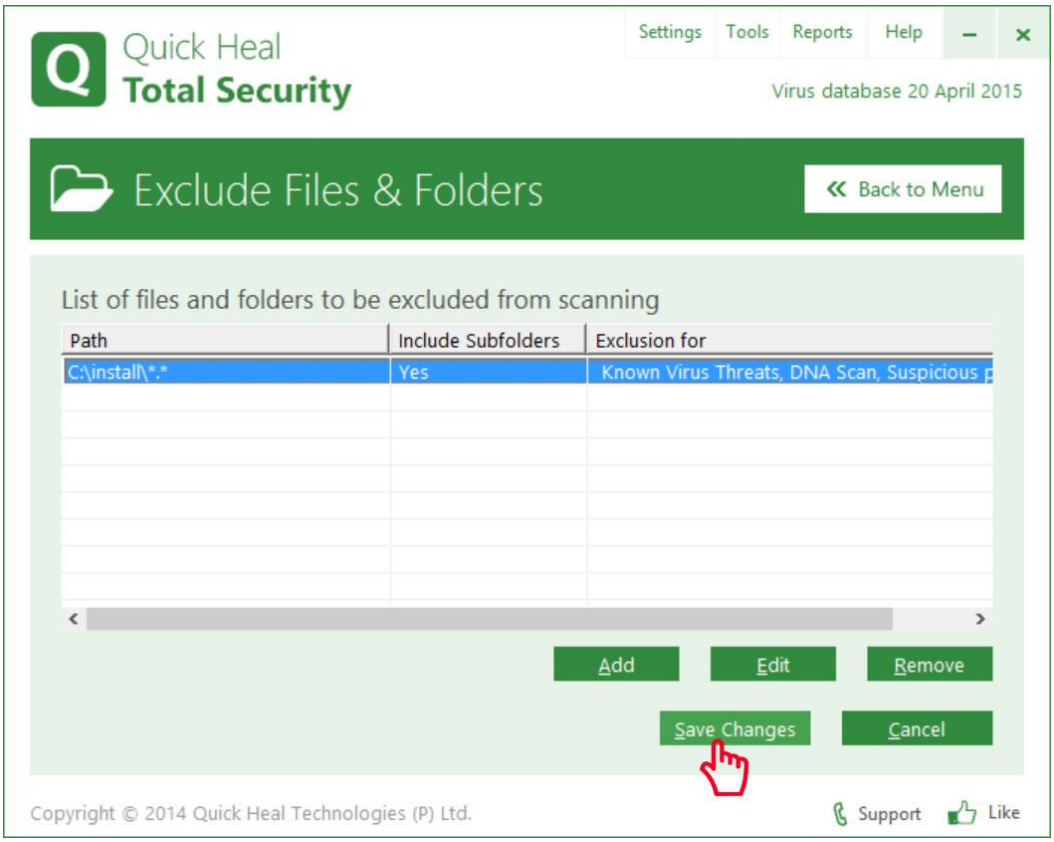
در قسمت (۲) چهار گزینه دارد: گزینه نخست برای عدم شناسایی همه ویروس‌ها، گزینه دوم استثناء کردن از اسکن DNA و گزینه سوم استثناء کردن از فایل‌های بسته‌ای مشکوک و گزینه چهارم استثناء کردن از سامانه رفتارشناسی می‌باشد. پیشنهاد می‌شود گزینه اول و آخر را تیک نمایید.



پس از کلیک بر روی دکمه Folder، پنجره Brows باز می‌شود که می‌توانید فولدر موردنظر را انتخاب نمایید. در صورتی که مایلید همه زیرپوشه‌ها و فولدرهای داخلی آن نیز از اسکن استثناء شوند، گزینه *Include Sebfolder* را نیز تیک نمایید.



بر روی *OK* کلیک نمایید.



در انتها بر روی دکمه *Save Changes* کلیک می‌کنیم.

ح) Quarantine & Backup(قرنطینه و پشتیبان)

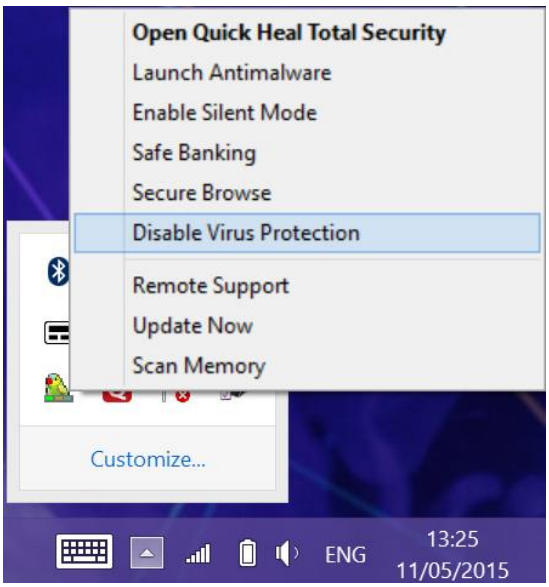
آنتی‌ویروس کوییک‌هیل برخلاف برخی از آنتی‌ویروس‌ها، اقدام به حذف کامل فایل آلوده یا مشکوک بصورت پیش‌فرض نمی‌کند، بلکه فایل‌ها را به صورت مطمئن قرنطینه می‌کند. می‌توان فایل‌های قرنطینه شده را بازیابی، حذف یا برای آنالیز بیشتر به شرکت تکنولوژی‌های کوییک‌هیل ارسال نمود.

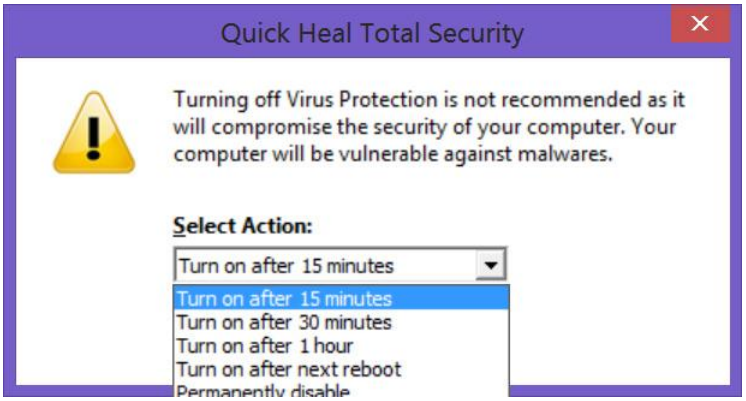
این ویژگی کمک می‌کند تا فایل‌های آلوده یا مشکوک به طور امن ایزوله گردند. فایل‌های مشکوک برای جلوگیری از اجرا به فرمت رمزشده‌ای قرنطینه می‌شوند. این کار موجب جلوگیری از آلودگی می‌گردد.

اگر می‌خواهید پیش از انجام تعمیر فایل‌های آلوده، یک پشتیبان گرفته شود، در بخش *Scan Settings* گزینه *Backup before taking action* را تیک بزنید.

همچنین می‌توانید در صورت نیاز فایل‌های قرنطینه شده را حذف و یا در صورت نیاز یک پشتیبان از آنها تهیه کنید.

برای بازیابی فایل ویروسی، در صورتی که مایلید از آن فایل به صورت دائمی نگهداری و استفاده کنید، می‌توانید آن فایل یا پوشه مربوطه را با استفاده از گزینه *Exclude File & Folder* –که شرح کامل آن در بخش قبل آمده است– را از ویروسیابی مستثنی نمایید. اما اگر به صورت موقت نیاز به فایل آلوده دارید، می‌توانید با غیرفعال کردن محافظت ویروس برای مدتی مشخص این کار را عملی سازید.



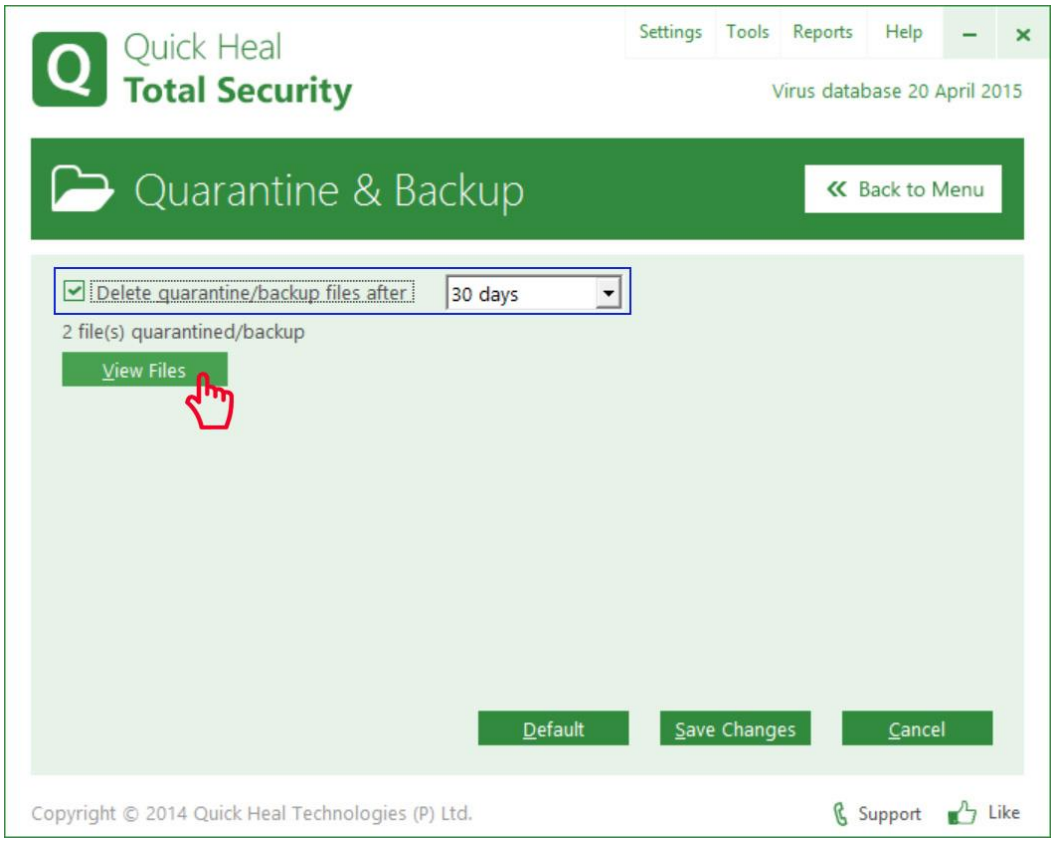


پس از استثناء کردن پوشه‌ی خاص از ویروسیابی یا غیرفعال کردن Virus Protection می‌توانید فایل موجود در قرنطینه را بازیابی نمایید:

نحوه بازیابی فایل مشکوک یا آلوده از قرنطینه به صورت تصویری شرح داده شده است:

در پنجره Quarantine & Backup بر روی دکمه View Files کلیک می‌کنیم:

لازم به توضیح است گزینه Delete quarantine/backup files after برای حذف فایل‌های قرنطینه شده و پشتیبان پس از مدتی مشخص می‌باشد.



برای بازیابی فایل مورد نظر پس از انتخاب فایل، از دکمه Restore برای بازیابی آن در پوشه مربوطه استفاده می‌کنیم.

پنجره Quarantine دارای امکانات زیر می‌باشد:

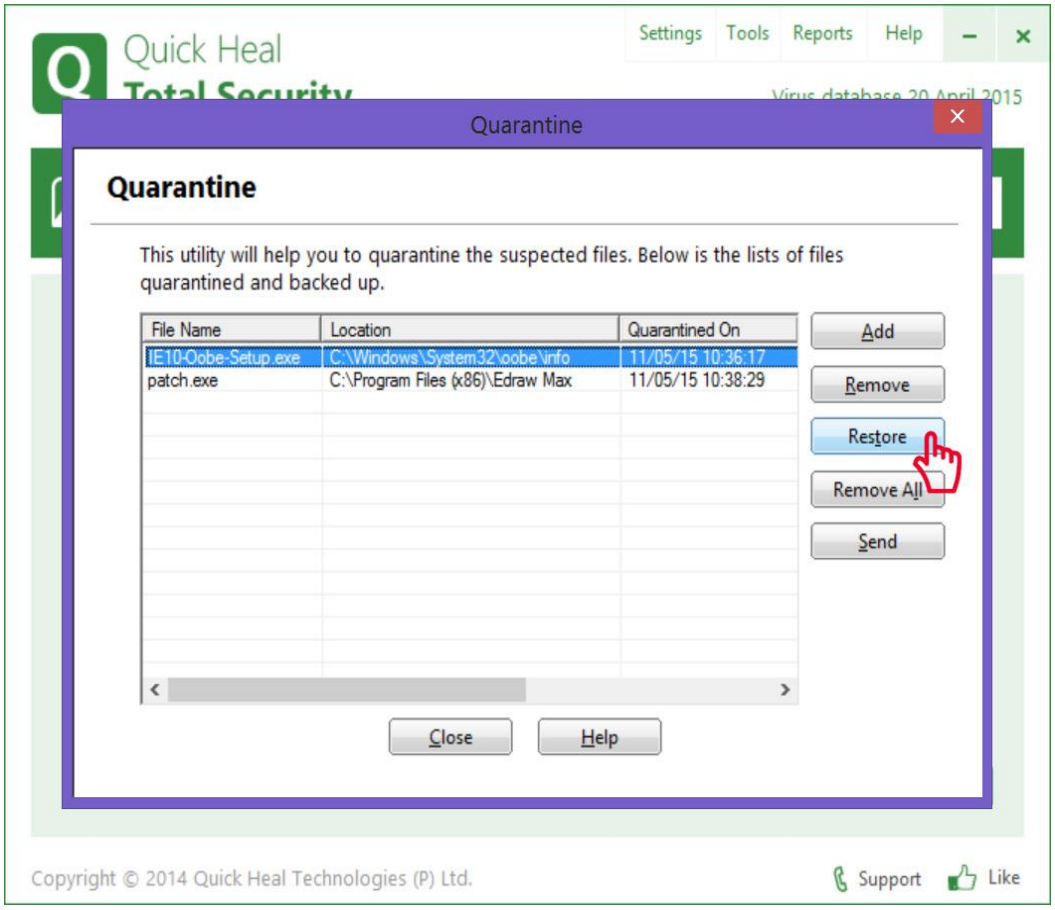
Add: جهت قرنطینه کردن فایل از این گزینه استفاده می‌شود. با این گزینه می‌توانید فایل مشکوک یا فایل خاصی را که خودتان مایلید قرنطینه کنید.

Remove: برای حذف فایل آلوده قرنطینه شده از سیستم، از این بخش استفاده نمایید.

Restore: برای بازیابی فایل قرنطینه شده به حالت عادی، از این گزینه استفاده نمایید.

Remove All: جهت حذف همه فایل‌های آلوده قرنطینه شده از سیستم، از این بخش استفاده کنید.

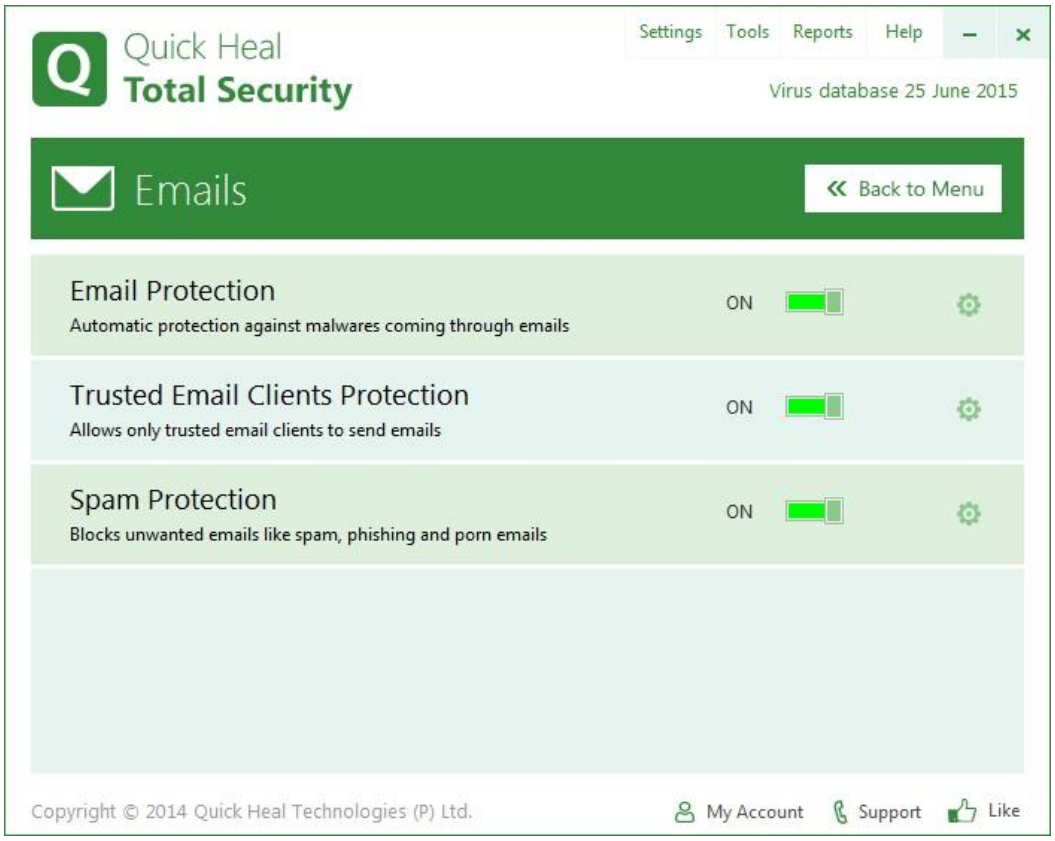
Send: جهت ارسال فایل قرنطینه شده به لابراتوار کوییک‌هیل برای آنالیز بیشتر، از این بخش استفاده می‌کنیم.



Emails (ایمیل‌ها)

با کلیک بر روی دومین هسته امنیتی، شما می‌توانید تنظیمات حفاظتی ایمیل‌های رایانه خود را پیکربندی نمایید.

با استفاده از این ویژگی، می‌توانید قوانین حفاظتی برای ایمیل‌های ورودی به سیستم خود را پیکربندی نمایید. این قوانین شامل مسدود کردن پیوست(های) ایمیل آلوده (بدافزار، هرزنامه و ویروس‌ها) می‌باشد. همچنین می‌توانید اقدامی که در هنگام یافتن بدافزار در ایمیل باید انجام شود را تعیین نمایید.



امنیت ایمیل شامل ویژگی‌های زیر است:

Email Protection: محافظت ایمیل

Trusted Email Clients Protection: محافظت از کلاینت‌های ایمیل مطمئن

Spam Protection: محافظت اسپم و هرزنامه

توجه:

محافظت ایمیل، از برنامه‌های ایمیل زیر پشتیبانی می‌کند:

- Microsoft Outlook Express 5.5 و جدید تر

- Microsoft Outlook 2000 و جدید تر
- Netscape Messenger و جدیدتر
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

محافظت ایمیل، از برنامه‌های ایمیل زیر پشتیبانی نمی‌کند:

- IMAP
- AOL
- Secure Sockets Layer(SSL) با POP3s
- ایمیل‌های مبتنی بر وب مانند Hotmail، Yahoo، Gmail (از آنجا که ایمیل‌ها و پیوست‌های این نوع از ایمیل‌ها وارد رایانه شما نشده –بلکه در سرورهای شرکت‌ها نگهداری می‌شوند- آلودگی وارد رایانه شما نخواهد شد. هرچند که قابلیت‌های Web-Security و Anti-Phishing کوییک‌هیل مانع از ورود بدافزارها از طریق این نوع از ایمیل‌ها به رایانه شما خواهد شد.)
- Lotus Notes

اتصالات SSL پشتیبانی نمی شوند:

آنتی ویروس‌ها از اتصالات ایمیل رمزی که از Secure Sockets Layer استفاده می‌کنند پشتیبانی نمی‌کنند.

برای فرستادن ایمیل از طریق SSL، E-mail protection را خاموش کنید.

در ادامه به شرح ویژگی‌های مختلف این بخش می‌پردازیم.

الف) Email Protection (محافظت ایمیل)

ویژگی محافظت از ایمیل که به صورت پیش فرض فعال است، محافظت بهینه ای برای صندوق پست الکترونیکی (mailbox) در برابر ایمیل‌های مخرب ارائه می دهد.

تنظیمات پیش‌فرض محافظت در برابر بدافزارهای وارده از طریق ایمیل را ارائه می‌دهد.

برای تعریف قوانین محافظتی و تنظیمات بیشتر، بر روی عنوان Email Protection کلیک کنید.

Display alert message: اگر می‌خواهید هنگام شناسایی ویروس در ایمیل یا پیوست ایمیل پیام نمایش داده شود، این گزینه را تیک نمایید.

توجه ۱: اطلاعات پیام ویروس‌ها حاوی اطلاعات: نام ویروس، آدرس ایمیل فرستنده، موضوع ایمیل، نام پیوست و اقدام انجام گرفته روی آن می‌باشد.

Select action to be performed when virus is found: اگر می‌خواهید هنگام شناسایی ویروس در ایمیل یا پیوست، تعمیر صورت گیرد گزینه Repair را انتخاب و اگر می‌خواهید ایمیل‌ها و پیوست‌های آلوده حذف شوند Delete را انتخاب نمایید.

توجه ۲: اگر پیوست قابل تعمیر نباشد، حذف خواهد شد.

Backup before taking action: درصورتی که می‌خواهید پیش از انجام هرگونه اقدام بر روی ایمیل‌ها یا پیوست‌های آلوده، از آنها پشتیبان تهیه شود، این گزینه را تیک کنید.

Attachment control settings: در بخش تنظیمات کنترل پیوست، می‌توانید نوع خاصی از ایمیل یا پیوست را مسدود نمایید.

Block attachments with multiple extensions: کرم‌ها معمولاً از پسوندهای چندگانه استفاده می‌کنند. شما می‌توانید با استفاده از این گزینه، پیوست‌های ایمیل با پسوندهای چندگانه را مسدود نمایید.

Block emails crafted to exploit vulnerability: این گزینه ایمیل‌هایی که تنها هدفشان سوء استفاده از آسیب‌پذیری کلاینت (برنامه) ایمیل است را مسدود می‌کند. مثلاً برخی ایمیل‌ها حاوی نقاط آسیب‌پذیری مانند MIME و IFRAME هستند که با استفاده از این گزینه مسدود خواهند شد.

Enable attachment control: با استفاده از این گزینه می‌توانید نوع خاصی از پیوست یا همه پیوست‌ها را مسدود نمایید.

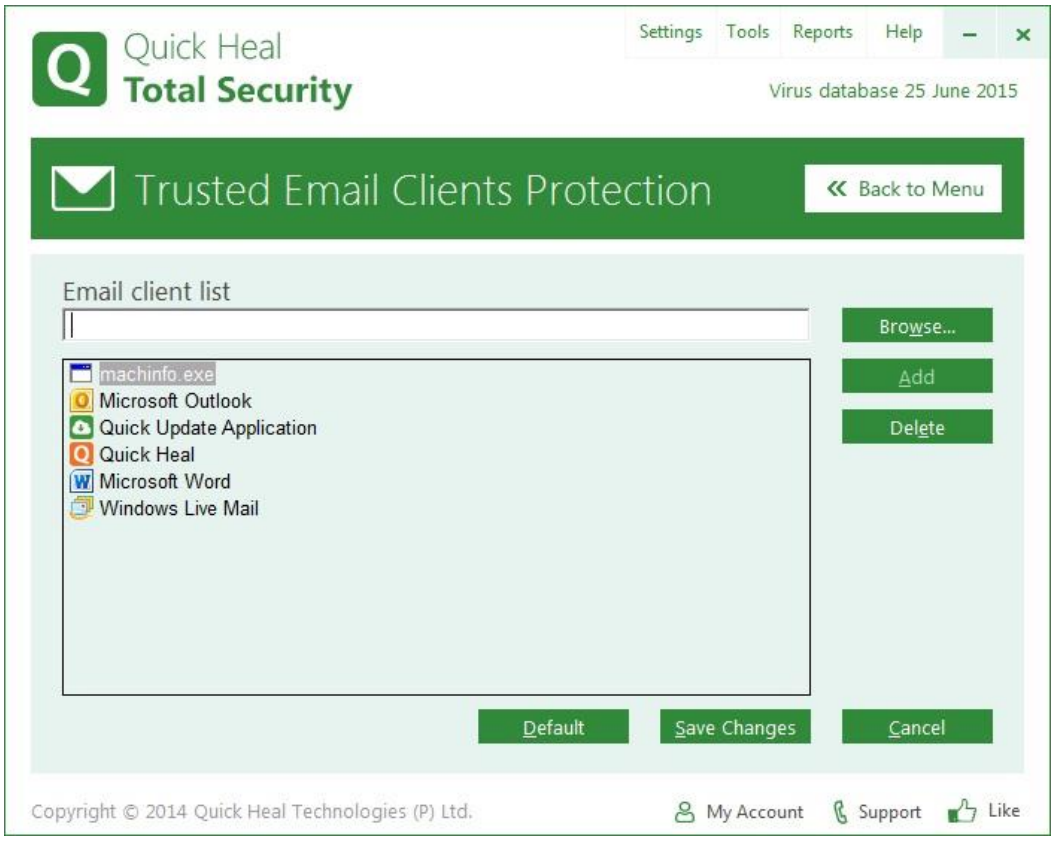
Block all attachments: این گزینه همه انواع پیوست ایمیل را مسدود می‌کند.

Block user specified attachments: با استفاده از این گزینه می‌توانید برخی از پسوندهای خاص پیوست را مسدود نمایید. با انتخاب این گزینه، دکمه ***Configure*** فعال خواهد شد. با فشردن این دکمه، پنجره User specified extensions باز خواهد شد. تعدادی پسوند از پیش تعریف شده در لیست وجود دارند، می‌توانید هر کدام از پسوندهای پیش‌فرض را حذف (***Delete***) و یا پسوند موردنظر خود را اضافه (***Add***) نمایید. دکمه ***Default***، لیست پسوندهای مسدودی را به حالت پیش فرض برمی‌گرداند.

ب) Email Protection (محافظت ایمیل)

از آنجایی که ایمیل به گسترده‌ترین رسانه ارتباطی تبدیل شده است، بدافزارها و دیگر تهدیدات نیز این بستر را به عنوان ساده‌ترین راه انتقال آلودگی برای خود برگزیده‌اند. پدیدآورندگان ویروس همواره به دنبال راه‌های جدیدی می‌گردند تا کدهای ویروسی خود را با استفاده از آسیب‌پذیری‌های برنامه‌های پرطرفدار ایمیل به صورت خودکار اجرا کنند. کرم‌ها نیز برای گسترش آلودگی خود از موتور مسیریابی SMTP (پروتکل ارسال ایمیل) استفاده می‌کنند.

این ویژگی که به صورت پیش‌فرض فعال است، به شما امکان می‌دهد که برخی برنامه‌های ارسال/دریافت کننده ایمیل (کلاینت‌های ایمیل) را در لیست برنامه‌های مطمئن قرار دهید. در صورتی که برنامه‌هایی غیر از برنامه های مورد اعتماد، بخواهند ایمیل ارسال یا دریافت کنند، پیغامی مناسب نمایش داده و تایید و یا مسدود کردن ارسال / دریافت ایمیل را از کاربر می‌پرسد.



برای افزودن، ابتدا فایل اجرایی (exe) برنامه‌ی ایمیل مورد اعتماد خود را با استفاده از دکمه *Browse* انتخاب کرده، سپس بر روی دکمه *Add* کلیک کنید تا به لیست مورد اعتمادها افزوده شود. برای حذف یک برنامه کلاینت ایمیل، آن را از لیست انتخاب و بر روی دکمه Delete کلیک کنید. تغییرات را با Save Changes ذخیره کنید.

ج) Spam Protection(محافظت هرزنامه)

محافظت هرزنامه (اسپم) امکان تمایز ایمیل‌های معتبر و فیلتر کردن ایمیل‌های ناخواسته مانند هرزنامه، فیشینگ (کلاهبردارانه) و غیراخلاقی را فراهم میکند. توصیه می‌کنیم که فعال بودن ***Spam Protection*** را حفظ کنید.

برای پیکربندی تنظیمات گام های زیر را دنبال کنید:

Tag subject with text (Recommended): اگر این گزینه فعال باشد، موضوع ایمیل‌ها با برچسب [SPAM]- آغاز می‌شود. امکان تعویض متن برچسب نیز وجود دارد.

Spam protection level: در این بخش سطح حفاظت اسپم تعیین می‌گردد.

Soft: اگر شما تعداد کمی ایمیل هرزنامه و اسپم دریافت می‌کنید، یا می‌خواهید تنها ایمیل‌های به وضوح هرزنامه را مسدود نمایید، این گزینه را انتخاب کنید. احتمال شناسایی ایمیل‌های اصیل به عنوان اسپم در این حالت خیلی کم می‌باشد.

Moderate (Recommended): اطمینان از فیلترینگ بهینه را به همراه می‌آورد. اگر شما تعداد زیادی ایمیل اسپم دریافت می‌کنید، این گزینه را انتخاب کنید. اگرچه ممکن است تعدادی ایمیل اصیل را به عنوان اسپم شناسایی کند. انتخاب این گزینه توصیه می‌شود هرچند به صورت پیش فرض فعال است.

Strict: این گزینه معیارهای فیلترینگ سخت‌گیرانه‌ای را اعمال می‌کند. اگرچه احتمال اینکه ایمیل‌های اصیل را به عنوان اسپم شناسایی کند، بالاست. تنها زمانی این گزینه را انتخاب کنید که تعداد زیادی ایمیل هرزنامه دریافت می‌کنید، یا بهتر است از ابزارهای دیگر برای قطع شدن اسپم استفاده کنید.

Enable email black list: با استفاده از این ویژگی، کاربر می‌تواند لیستی از ایمیل‌های سیاه ساخته و دریافت ایمیل از این لیست را به عنوان اسپم در نظر گیرد. در مواردی که سرور شما از یک بازپخش کننده ایمیل آزاد (open mail relay) استفاده می‌کند، می‌تواند مفید باشد. با استفاده از لیست سیاه می‌توانید ایمیل‌های ورودی ناخواسته یا از فرستنده‌های ناشناخته را فیلتر کنید. امکان افزودن یک آدرس ایمیل و دامنه (همه آدرس‌های ایمیل تحت دامنه) وجود دارد. لیست سیاه لیستی است که حاوی آدرس‌های ایمیل ناخواسته می‌باشد. محتویات آدرس‌های ایمیل لیست سیاه فیلتر شده و با برچسب -[SPAM] نشاندار می‌شود.

با انتخاب این گزینه و کلیک بر روی دکمه ***Customize*** پنجره لیست سیاه باز می‌شود.

Add: برای افزودن یک آدرس ایمیل به لیست سیاه، آن را وارد کادر متنی Black List کرده و بر روی این دکمه کلیک کنید.

توجه: در زمان افزودن به لیست سیاه، توجه نمایید که یک آدرس ایمیل را قبلا در لیست سفید وارد نکرده باشید، در غیر اینصورت پیام مناسب نشان داده خواهد شد.

Edit: برای ویرایش، آدرس ایمیل را انتخاب و بر روی این دکمه کلیک می‌کنید.

Remove: برای حذف یک آدرس ایمیل، آن را انتخاب و با دکمه ***Remove*** آن را حذف کنید.

Import List: شما می‌توانید یک لیست سیاه را با استفاده از این دکمه وارد نمایید.

توجه: این گزینه زمانی که یک لیست سیاه استخراج شده (export) و یا اطلاعات ذخیره شده آنتی‌اسپم را در اختیار دارید و می‌خواهید آنها را در لیست سیاه خود قرار دهید بسیار مفید است.

Export List: این گزینه از لیست سیاه خروجی گرفته و می‌توانید آن را بر روی کامپیوتر خود ذخیره کنید.

توجه: این ویژگی از همه آدرس های ایمیل موجود در لیست، خروجی تهیه می‌کند. استخراج لیست زمانی که می‌خواهید کوییک‌هیل توتال سکیوریتی خود را حذف و نصب مجدد نمایید، یا از این لیست در سیستم دیگر استفاده کنید، مفید است.

Enable email white list: با استفاده از این ویژگی، کاربر می‌تواند لیستی از ایمیل‌های سفید ساخته و دریافت ایمیل از این لیست را به عنوان ایمیل اصیل و معتبر در نظر گیرد. لیست سفید حاوی آدرس‌های ایمیل مورداعتماد است. سیاست‌های فیلترینگ محافظت اسپم (هرزنامه) بر روی محتویات آدرس‌های ایمیل لیست سفید اعمال نشده و به عنوان SPAM برچسب دار نخواهند شد.

این ویژگی زمانی که چندین آدرس ایمیل معتبر و اصیل می‌یابید که با عنوان SPAM نشاندار می‌شود، مفید است. همچنین اگر یک دامنه را در لیست سیاه قرار داده‌اید اما می‌خواهید ایمیل‌های وارد شده از یک آدرس ایمیل خاص تحت آن دامنه را دریافت کنید، می‌توانید از این ویژگی استفاده نمایید.

Enable AntiSpam plugin: با انتخاب این گزینه، قوانین محافظتی بر روی پلاگین آنتی‌اسپم فعال می‌شود.

افزودن دامنه‌ها به لیست سیاه / سفید

برای افزودن کلیه آدرس‌های یک دامنه به جای درج آدرس دقیق یک ایمیل، در کادر متنی آدرس ایمیل مربوط به لیست سیاه یا سفید (مثلا MyEmail2@ mytest.com) آدرس دامنه را به فرمت زیر وارد نمایید:

*@mytest.com

Internet & Network (اینترنت و شبکه)

با کلیک بر روی سومین هسته امنیتی، شما می‌توانید تنظیمات حفاظتی ارتباطات اینترنتی و شبکه‌ای را پیکربندی نمایید.

با استفاده از این ویژگی، می‌توانید قوانین امنیتی را طوری تنظیم نمایید تا سیستم شما در برابر فایل‌های مخرب و آلوده که می‌توانند به صورت پنهانی در زمان فعالیت های آنلاین مانند بانکداری اینترنتی، فروش اینترنتی، وارد سیستم شوند، محافظت شود. همچنین با استفاده از کنترل خانواده (Parental Control) می‌توانید فعالیت‌های آنلاین فرزندان خود و دیگر کاربران را رصد کرده و دسترسی به سایت‌های ناخواسته را محدود نمایید.

بخش اینترنت و شبکه شامل ویژگی‌های زیر است:

الف) Firewall Protection (محافظت فایروال)

محافظت فایروال با فیلتر کردن ترافیک‌های ورودی و خروجی شبکه، مانند سپری از سیستم شما در برابر هکرها و مهاجمان حفاظت می‌کند.

همه برنامه‌های مشکوک که می‌توانند به رایانه‌ها یا سیستم‌های شما آسیب رسانند مسدود می‌شوند. فایروال از رایانه شما در برابر برنامه‌های مخرب چه از ارتباطات اینترنتی خارجی و چه از شبکه‌های داخلی که قصد نفوذ به سیستم شما را دارند، محافظت می‌کند.

پیکربندی فایروال به شرح زیر می‌باشد:

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن فایروال نمایید. فایروال به صورت پیش‌فرض روشن است.

برای پیکربندی سیاست‌گذاری‌های فایروال بر روی *Firewall Protection* کلیک کنید.

Firewall Level: در این بخش سطح امنیتی فایروال مشخص می‌شود. این سطوح شامل:

Low: همه ترافیک‌های ورودی و خروجی مجاز بوده، مگر اینکه شما ترافیکی را در لیست استثناها (exception) غیرمجاز (deny) کرده باشید.

Medium: همه ترافیک‌های ورودی را مسدود کرده، اما ترافیک‌های خروجی را مجاز می‌کند، مگر اینکه شما در لیست استثناها (exception)، یک ترافیک خروجی را غیرمجاز (deny) و یا یک ترافیک ورودی را مجاز (Allow) کرده باشید.

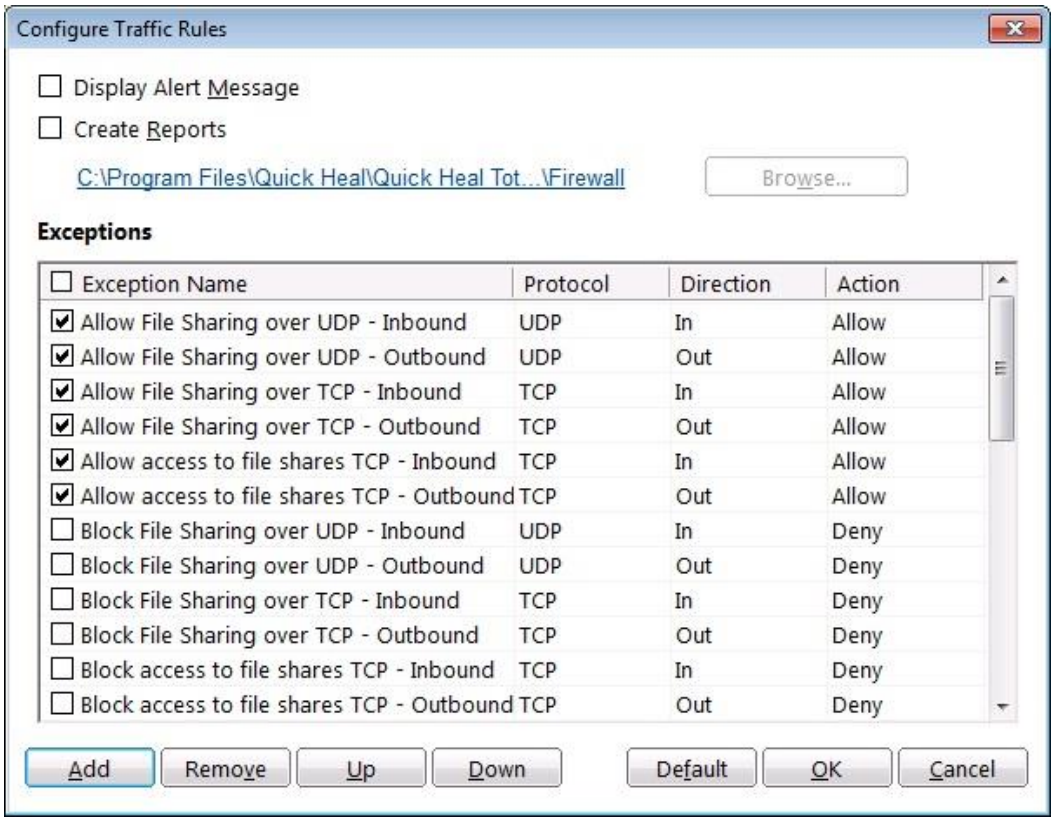
High: همه ترافیک‌های ورودی و خروجی را مسدود می‌کند، مگر اینکه شما ترافیکی را در لیست استثناها (exception) مجاز (Allow) کرده باشید.

Block all: همه اتصالات ورودی و خروجی را مسدود می‌کند.

Traffic Rules: می‌توانید قوانینی برای ترافیک‌های ورودی و خروجی تعریف نمایید.

برای ایجاد یک قانون (rule) جدید برای ترافیک‌های شبکه به صورت زیر عمل می‌کنیم:

ابتدا بر روی دکمه *Configure* کلیک کنید تا صفحه پیکربندی قوانین باز شود.



Display Alert Message: اگر اتصالی مطابق با قوانین استثناء بود، یک پیغام اخطار به کاربر نمایش داده می‌شود.

Create Reports: اگر می‌خواهید گزارشی از فعالیت‌های فایروال تهیه شود، این گزینه را تیک کنید. ضمناً می‌توانید مسیری که گزارش ذخیره می‌شود را نیز تعیین کنید.

Exceptions: در این بخش لیستی از استثناهای از پیش تعریف شده و استثناهای تعریف شده توسط کاربر نشان داده می‌شود. با دوبار کلیک بر روی اسم استثناء می‌توانید آن را ویرایش کنید. قوانینی فعالند که

در ابتدای نام آنها تیک داشته باشد. با قوانین استثناء می‌توانید ترافیک‌های شبکه‌ای را مجاز یا مسدود نمایید. همچنین می‌توانید یک استثناء برای ارتباطات ورودی یا خروجی به رایانه، از طریق آدرس IP و پورت بسازید.

امکانات این بخش عبارتند از:

Add: برای ایجاد یک قانون جدید بر روی این دکمه کلیک کنید.

Remove: برای حذف یک قانون، ابتدا آن را انتخاب سپس بر روی این دکمه کلیک کنید. قوانین پیش‌فرض را نمی‌توان حذف کرد.

Up: با انتخاب یک قانون و کلیک بر روی این دکمه می‌توانید آن را به موقعیت یک ردیف بالاتر برده و درنتیجه اولویت اجرای آن را افزایش دهید.

Down: با انتخاب یک قانون و کلیک بر روی این دکمه می‌توانید آن را به موقعیت یک ردیف پایین‌تر برده و درنتیجه اولویت اجرای آن را کاهش دهید.

Default: تنظیمات همه قوانین را به حالت پیش‌فرض بر می‌گرداند.

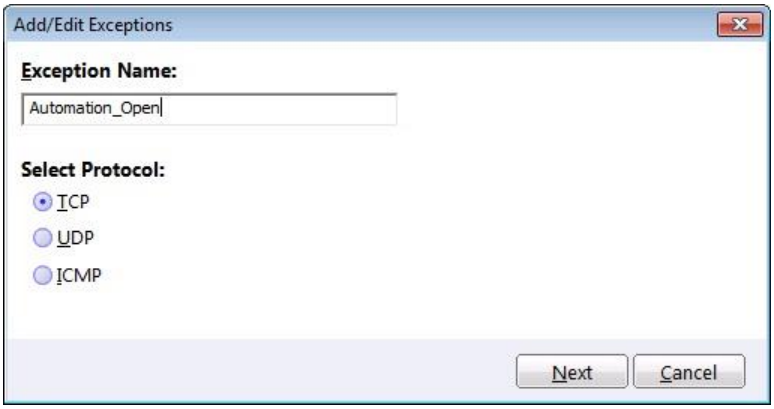
OK: موجب ذخیره شده تغییرات می‌گردد.

Cancel: همه تغییرات صورت گرفته را لغو کرده و پنجره *Configure Traffic Rule* را می‌بندد.

افزودن / ویرایش یک قانون

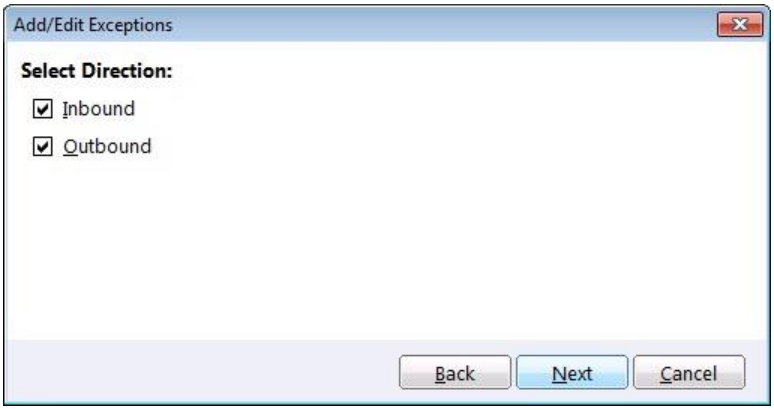
در صفحه افزودن یا ویرایش استثناها (*Add/Edit Exceptions*)، شما می‌توانید یک قانون جدید ایجاد و یا قوانین فعلی را ویرایش نمایید.

برای افزودن یک قانون جدید بر روی دکمه *Add* کلیک کنید.

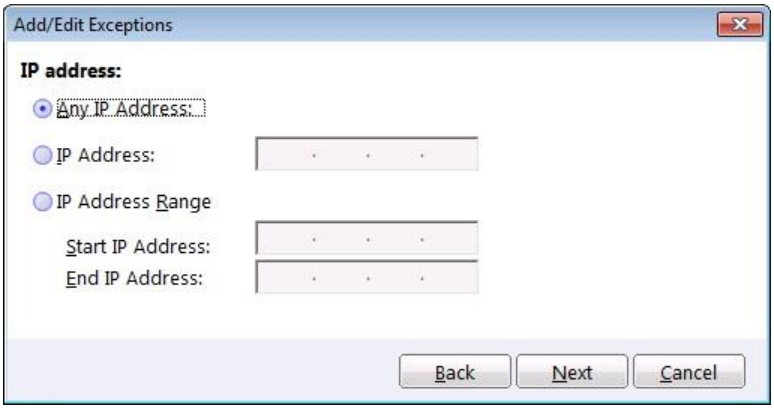


Exception Name: یک نام دلخواه برای قانون خود وارد نمایید.

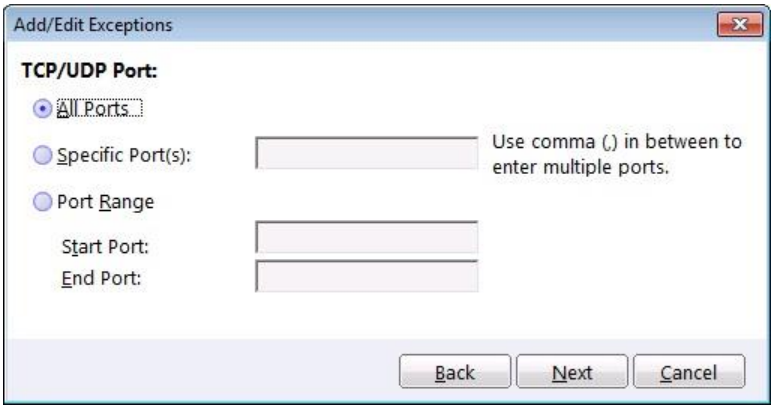
Select Protocol: پروتکلی که می‌خواهید این قانون بر روی آن اعمال شود را انتخاب کنید. پروتکل‌ها شامل TCP، UDP و ICMP است. برای هر قانون تنها یک نوع پروتکل قابل انتخاب است. اگر می‌خواهید چندین پروتکل را برای یک قانون مجاز یا مسدود کنید، باید برای هر پروتکل یک قانون مجزا بسازید.



Select Direction: در این صفحه می‌توانید مسیرهای ترافیکی را تعیین نمایید. مسیر می‌تواند ورودی (*Inbound*) یا خروجی (Outbound) و یا هر دو باشد.

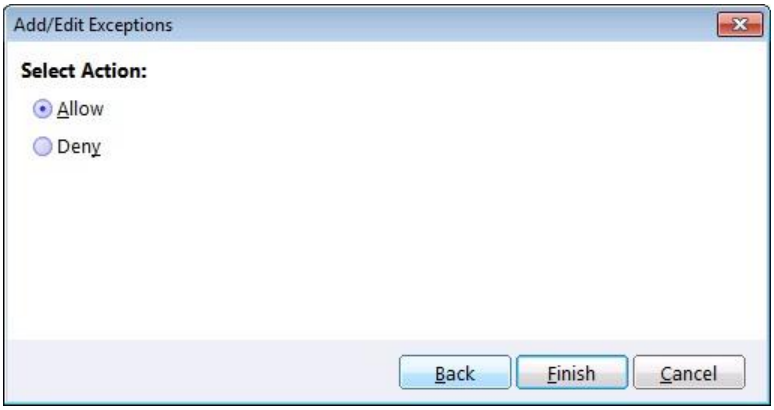


IP Address: شما می‌توانید همه‌ی آدرس‌های IP (Any IP Addresses) یا یک آدرس IP خاص (IP Address) و یا رنجی از آدرس IP (IP Address Range) را برای مسدود شدن یا مجاز شدن ترافیک انتخاب کنید.



TCP/UDP Port: می‌توانید پورت‌هایی که می‌خواهید قانون بر روی آن اعمال شود را تعیین کنید. همه پورت‌ها (All Ports)، یک یا چند پورت خاص (Specific Port(s)) که با , (کاما) جدا می‌شوند، یا یک بازه از پورت‌ها (Port Range) را انتخاب کنید.

اگر همه پورت‌ها (All Ports) را انتخاب کنید، نیازی به تایپ شماره پورت‌ها نیست و همه پورت‌ها انتخاب می‌شوند.



Select Action: می‌توانید اقدام این قانون را مجاز (*Allow*) یا مسدود (*Deny*) نمایید.

درصورت انتخاب Allow، اگر ترافیک یا اتصالی مطابق با تنظیمات ذکرشده باشد، مجاز می‌شود.

درصورت انتخاب Deny، اگر ترافیک یا اتصالی مطابق با تنظیمات ذکرشده باشد، مسدود می‌شود.

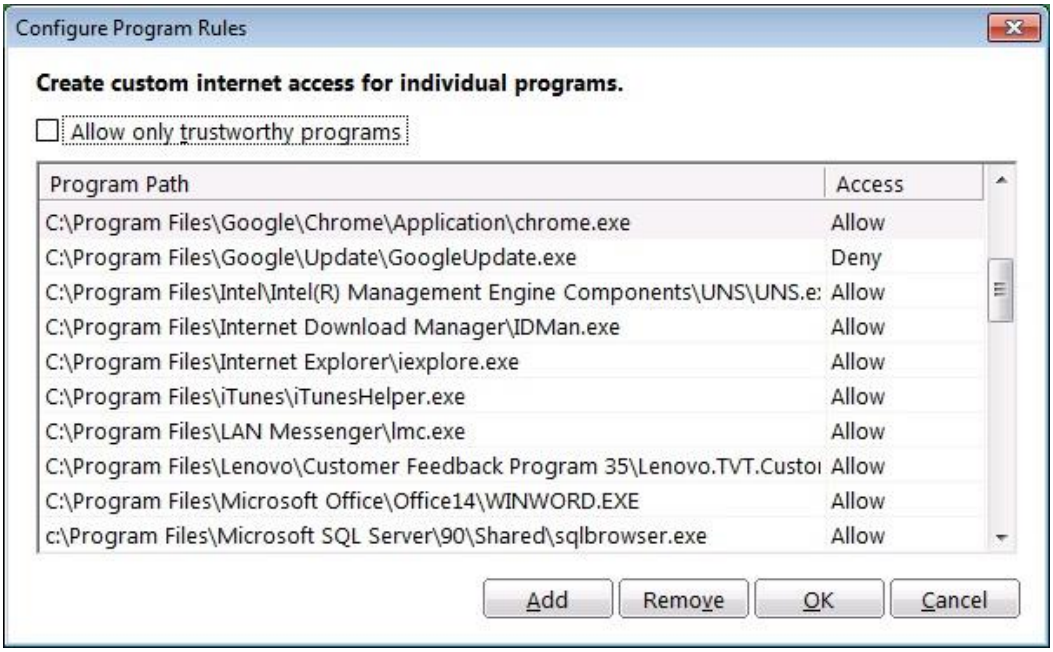
Program Rules: شما می‌توانید با تعریف قوانین، دسترسی برنامه به اینترنت و شبکه را کنترل کنید. مثلاً می‌توانید دسترسی یک برنامه به اینترنت برای دریافت آپدیت و یا بررسی لایسنس آن را مسدود نمایید.

توجه: با استفاده از این قابلیت می‌توانید با مسدود کردن دسترسی ناخواسته برخی از برنامه‌ها به اینترنت، در مصرف پهنای باند صرفه‌جویی نمایید. همچنین با مسدود کردن برخی از برنامه‌های غیراورجینال به اینترنت مانع از بررسی صحت لایسنس و از کار افتادن آنها شوید.

قانون برنامه

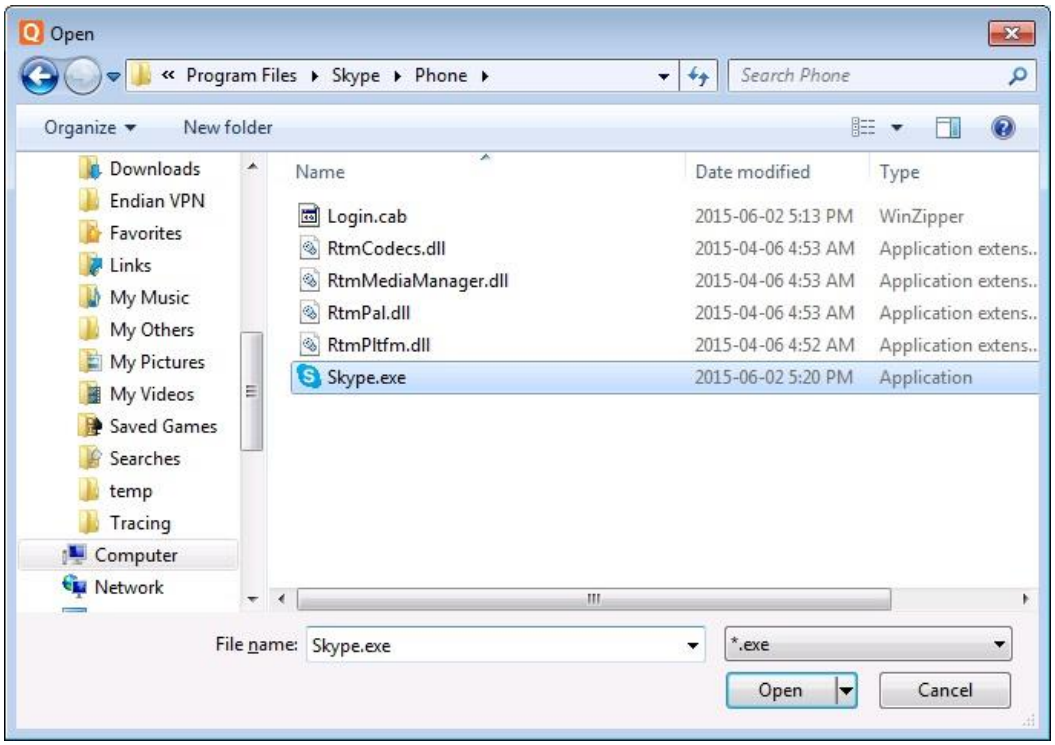
با استفاده از قوانین برنامه (Program Rules)، می‌توانید دسترسی برنامه‌ها به اینترنت را مجاز یا مسدود کنید.

با کلیک بر روی *Configure* لیست برنامه‌های موجود در رایانه شما که به اینترنت دسترسی داشتند نمایش داده می‌شود.



دسترسی هر یک از برنامه‌ها را می‌توانید ممنوع (*Deny*) یا مجاز (*Allow*) کنید. پنجره انتخاب فایل اجرایی باز می‌شود. شما می‌توانید فایل اجرایی (exe) برنامه‌ای را که می‌خواهید دسترسی به آن را مسدود کنید انتخاب کنید.

Add: برای افزودن یک برنامه جدید –که در لیست وجود ندارد– بر روی *Add* کلیک کنید.



با کلیک بر روی *Open* نام برنامه به لیست افزوده می‌شود. در ستون Access با انتخاب گزینه *Deny* می‌توانید دسترسی برنامه به اینترنت را مسدود کنید.

Remove: برای حذف یک قانون برنامه، ابتدا آن را انتخاب سپس بر روی این دکمه کلیک کنید.

OK: موجب ذخیره شده تغییرات می‌گردد.

Cancel: همه تغییرات صورت گرفته را لغو کرده و پنجره *Configure Program Rule* را می‌بندد.

Allow only trustworthy programs: برنامه‌های قابل اعتماد (Trustworthy)، برنامه‌هایی هستند که راستی‌آزمایی شده و هویت آنها شناخته شده می‌باشند در حالی که برنامه‌های غیرقابل اعتماد (untrustworthy) برنامه هایی هستند که راستی‌آزمایی نشده یا مشکوک می‌باشند. برنامه‌های مخرب هویت خودشان را پوشانده و یک عملیات مخفیانه انجام می‌دهند. چنین برنامه‌هایی ممکن است برای شبکه و کامپیوترها مضر باشد.

تیک بودن این گزینه تنها به برنامه‌های تاییدشده و مورداعتماد اجازه ی دسترسی به شبکه و اینترنت داده و همه برنامه‌های غیرمعتبر را مسدود می‌کند.

Stealth Mode: با انتخاب گزینه حالت پنهان، سیستم شما در شبکه مخفی و نامرئی شده و درنتیجه مانع حملات و نفوذ هکرها می‌گردد.

ب) Browsing Protection (محافظت مرور)

زمانی که کاربران از سایت‌های آلوده بازدید می‌کنند، ممکن است برخی فایل‌های آلوده بر روی سیستم آنها نصب شود. ممکن است این فایل‌ها موجب انتشار بدافزار شده، سرعت سیستم را کاهش داده، یا حتی موجب تخریب فایل‌های دیگر شوند. این حملات ممکن است موجب آسیب‌دیدگی قابل توجه سیستم گردد.

محافظت مرور (*Browsing Protection*) اطمینان می‌دهد که هنگام دسترسی کاربران به اینترنت، وب‌سایت‌های آلوده مسدود خواهند شد. زمانی‌که این ویژگی فعال باشد، وب‌سایت‌های در حال بازدید، ابتدا اسکن شده و در صورت وجود بدافزار در آنها، مسدود خواهند شد.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن محافظت مرور نمایید. این ویژگی به صورت پیش‌فرض فعال است.

ج) Malware Protection (محافظت بد افزار)

این ویژگی کمک می کند تا هنگام اتصال به اینترنت سیستم شما در برابر تهدیداتی مانند جاسوس افزارها، تبلیغ افزارها، کلیدنگارها و ریسک افزارها محافظت گردد.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن محافظت بدافزار نمایید. این ویژگی به صورت پیش‌فرض فعال است.

د) Phishing Protection (محافظت فیشینگ)

فیشینگ یک اقدام کلاهبردارانه می باشد که تلاش می کند از طریق ایمیل یا وب سایت اطلاعات شخصی شما را سرقت کند. ایمیل های فیشینگ، به نظر می رسد از سازمان‌های معتبر برای شما ارسال شده است و قصد دارند یک خدمت یا وجهی را به حساب شما واریز کنند. وب سایت های جعلی، شبیه وب‌سایت‌های معتبر بانک‌ها یا شرکت‌های خدماتی می باشند که قصد دارند اطلاعات شخصی شما مانند اطلاعات حساب بانکی، رمزهای عبور، شماره حساب‌ها را سرقت کنند.

محافظت فیشینگ، از دسترسی کاربران به وب سایت‌های جعلی و کلاهبردارانه جلوگیری می کند. به محض دسترسی به وب‌سایت، بلافاصله برای وجود هرگونه رفتار فیشینگ اسکن می شود و در صورت یافتن فعالیت فیشینگ و کلاهبردارانه، مسدود خواهد شد.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن محافظت فیشینگ نمایید. این ویژگی به صورت پیش‌فرض فعال است.

هـ) Browser Sandbox (سندباکس مرورگر)

در هنگام مرور اینترنت، راهنمایی وجود ندارد که متوجه شوید کدام وب‌سایت‌ها مورداعتماد و بازبینی شده‌اند و کدام نیستند. سایت‌های مورداعتماد (Trusted)، وب‌سایت‌هایی هستند که هویت و شناسنامه خود را به اشتراک می‌گذارند. اگرچه همه سایت‌های غیرمطمئن (untrusted) سایت‌های جعلی، کلاهبردارانه یا فیشینگ نیستند. وب‌سایت‌های تجاری، فروشندگان و تأمین کنندگان، بازرگانی، تبلیغاتی، سرگرمی ممکن است جزء سایت‌های غیرمطمئن باشند.

سایت‌های مخرب هویت خود را تغییر داده و یک فعالیت سیستمی مخفی را اجرا می‌کنند. این سایت‌ها می‌توانند اطلاعات محرمانه و مهم شما را هک نمایند، رایانه شما را آلوده سازند، و نیز با استفاده از سیستم شما اقدام به ارسال هرزنامه و ایمیل های مخرب، کلاهبردارانه یا تبلیغاتی نمایند.

مرورگر سندباکس کمک می‌کند تا شما در برابر هر نوع حمله مخرب ایمن بمانید.

این قابلیت سیاست‌های سخت‌گیرانه‌ای برای همه سایت‌های غیرمطمئن و بازبینی نشده اعمال می‌کند. اگر گزینه Browser Sandbox فعال بوده و شما برای اولین بار از یک وب‌سایت بازدید می‌کنید و آن وب‌سایت مورداعتماد و مطمئن (trusted) نباشد، امنیت شما همچنان محفوظ خواهد بود.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن سندباکس مرورگر نمایید. این ویژگی به صورت پیش‌فرض فعال است.

اجرای سندباکس مرورگر

برای اجرای مرورگر امن سندباکس کوییک‌هیل، بر روی آیکن *Quick Heal Secure Browse* که بر روی دسکتاپ ویندوز قرار دارد کلیک کنید. با اجرای این برنامه، مرورگر پیش‌فرض سیستم شما به همراه سندباکس اجرا می‌شود. سندباکس کمک می‌کند تا امنیت وبگردی و مرور اینترنتی شما تأمین گردد، حتی اگر گزینه *Browser Sandbox* خاموش باشد.

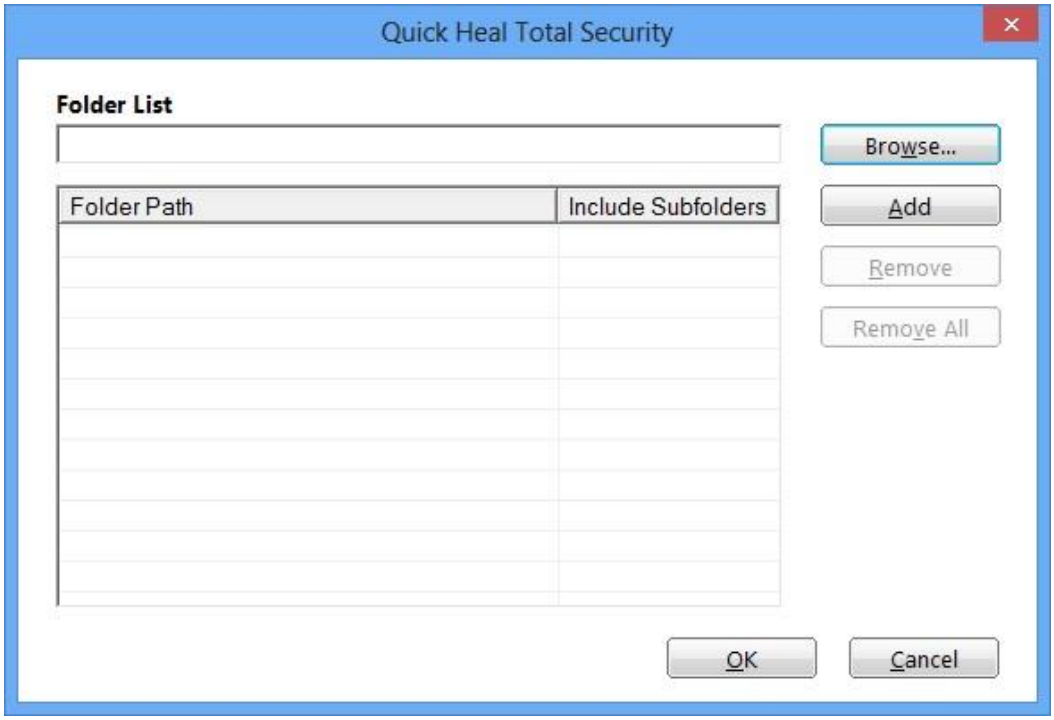
توجه: تنظیمات پیش‌فرض برای کاربران عادی، مطلوب و ایده‌آل بوده و نیازی به تنظیمات بیشتر نیست.

برای پیکربندی سندباکس مرورگر بر روی عنوان Browser Sandbox کلیک نمایید تا صفحه ی تنظیمات بیشتر نمایش داده شود:

Select Browser Sandbox security level: شما می‌توانید سطح امنیتی سندباکس مرورگر را تعیین نمایید. این سطوح امنیتی می‌تواند ***Strict*** (سخت‌گیرانه)، ***High*** (بالا) یا ***Moderate*** (متوسط) باشد که سطح پیش‌فرض **High** می‌باشد.

Prevent browser from accessing confidential folders: برای محافظت از اطلاعات محرمانه خود (مانند اطلاعات بانکی، تصاویر شخصی و اسناد مهم) در زمان وبگردی، شما می‌توانید پوشه‌هایی که حاوی اطلاعات محرمانه هستند را با استفاده از این گزینه اضافه کنید تا از دسترسی مرورگر اینترنتی به آنها جلوگیری به عمل آید. این گزینه مانع دسترسی مرورگرها و دیگر برنامه‌های اجرا شده تحت سندباکس مرورگر به پوشه‌های حاوی اطلاعات محرمانه می‌شود. بنابراین اطلاعات شما از سرقت ایمن خواهد ماند.

با تیک کردن این گزینه دکمه **Folders** فعال می‌شود که با کلیک بر روی آن پنجره لیست پوشه‌ها نشان داده خواهد شد.



با استفاده از دکمه Browse پوشه ی موردنظر (حاوی اطلاعات محرمانه) را انتخاب کرده و برای افزودن آن بر روی دکمه Add کلیک کنید. می‌توانید چندین پوشه را از این طریق اضافه کنید. در نهایت برای ذخیره شدن بر روی OK کلیک نمایید. برای حذف یک پوشه از "لیست جلوگیری از دسترسی مرورگر" به آنها از دکمه Remove و برای حذف همه از Remove All استفاده کنید.

Prevent browser from modifying the protected data: برای محافظت از ویرایش داده‌ها از این گزینه استفاده می‌شود. اطلاعات موجود در پوشه‌های محافظت شده در دسترس بوده اما قابل دستکاری و ویرایش نمی‌باشد.

Allow browser to store all downloads in the specified folder: برای دانلود اطلاعات و محتویات سایت‌های درحال بازدید در یک پوشه خاص از این گزینه استفاده می‌شود.
اگر در آینده نیاز به محتویات دانلودی خود دارید، این گزینه مفید خواهد بود.

Show border around browser window: این گزینه، یک کادر دور مرورگرهای شما کشیده که نشان می‌دهد سندباکس مرورگر بر روی آن مرورگر درحال اجراست.
توجه: این ویژگی یک گزینه اجباری و مهم برای برقراری امنیت نبوده و در صورت تمایل می‌توانید این گزینه را غیرفعال کنید.

Delete: اطلاعات حافظه پنهان کش (cache) سندباکس را حذف می‌کند. این گزینه فایل‌های موقتی را حذف می‌کند.

Save Changes: برای ذخیره تغییرات، بر روی این دکمه کلیک کنید.

و) Safe Banking (بانکداری امن)

با استفاده از بانکداری آنلاین و اینترنتی، شما می‌توانید حساب خود را چک کنید، قبوض و صورتحساب‌های خود را پرداخت کنید، خریدهای اینترنتی کنید، خرید و فروش سهام داشته باشید، و انتقال وجه بین حساب‌های مختلف انجام دهید.

برای انجام این موارد می‌بایست وارد وب‌سایت بانک شده، اطلاعات هویتی (نام کاربری و رمز عبور) خود را وارد کرده و در نهایت تراکنش مالی موردنیاز خود را انجام دهید.

اگر چه در زمان بازدید وب‌سایت بانک‌ها ممکن است شما قربانی وب‌سایت‌های جعلی بانکی شده یا هنگام ورود اطلاعات مهم حساب کاربری یا رمزهای حساب بانکی خود، این اطلاعات توسط مجرمان به سرقت (فیشینگ) رود. در نتیجه متحمل زیان مالی خواهید شد.

بانکداری امن کوییک‌هیل از شما در برابر همه شرایط ممکن که می‌تواند باعث به خطر افتادن اطلاعات محرمانه بانکی و هویتی شما شود، محافظت می‌کند. بانکداری امن، کل نشست بانکی شما را در یک محیط امن باز کرده و از اطلاعات حیاتی شما محافظت می‌کند.

بانکداری امن شامل ویژگی‌های زیر می‌باشد:

- مرورگر در یک محیط امن اجرا شده تا از آلودگی رایانه‌ها به بدافزارهای روز-صفر (هنوز کشف نشده) محافظت کند.
- فعالیت بانکداری شما از تهدیدات اینترنتی مجزا و ایزوله می‌باشد.
- همه انواع ابزارهای ثبت‌کننده‌های کلید و کلیدنگارها مسدود شده و در برابر ذخیره‌کننده‌های کلید اطلاعات محرمانه محافظت می‌شود.
- برای جلوگیری از هک از یک DNS امن استفاده می‌شود.
- اطمینان می‌دهد که وب‌سایت‌هایی که شما در حال بازدید آنها هستید، بازبینی شده و امن هستند.

تنظیمات بانکداری امن

شما می‌توانید با استفاده از تنظیمات پیش‌فرض از بانکداری امن استفاده کنید. همچنین می‌توانید براساس نیازمندی‌های امنیتی خود، تنظیمات Safe Banking را سفارشی سازید.

Protect against DNS based attacks: از سیستم شما در برابر بازدید از وب‌سایت‌های جعلی و کلاهبردارانه محافظت می‌کند.

Allow clipboard sharing: اگر می‌خواهید بین محیط ویندوز رایانه و محیط ایمن بانکداری امن اطلاعات کلیپ‌بورد (Copy و Paste) رد و بدل کنید، این گزینه را فعال نمایید.

Keyboard shortcut for switching between Windows desktop and Safe Banking desktop: با استفاده از این گزینه می‌توانید برای سوئیچ کردن و تعویض محیط دسکتاپ بانکداری امن و دسکتاپ ویندوز کلید میانبر ایجاد کنید. از آنجا که بانکداری امن در یک محیط مجزا و ایزوله اجرا می‌شود، شما نمی‌توانید به هیچ یک از فایل‌ها یا پوشه‌های کامپیوتر خود دسترسی یابید.

اجرای بانکداری امن

شما می‌توانید به ویژگی‌های بانکداری امن به صورت جداگانه دسترسی یابید. هنگامی که آنتی‌ویروس کوییک‌هیل نصب می‌شود، بانکداری امن نیز به صورت خودکار نصب خواهد شد. یک آیکن میانبر برای دسترسی به Safe Banking در دسکتاپ ساخته خواهد شد.

برای اجرا بر روی آیکن Safe Banking که در دسکتاپ رایانه شما قرار دارد کلیک کنید.

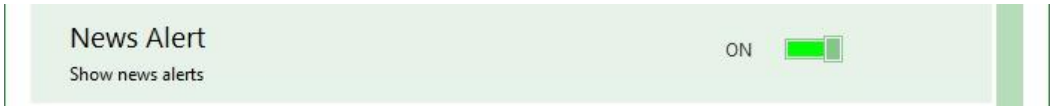
شما می‌توانید با استفاده از مرورگرهای قابل پشتیبانی که در نوار وظیفه (task bar) قرار دارد، اقدام به بازدید از وب‌سایت موردنظر خود نمایید.

همچنین می‌توانید با استفاده از دکمه *Add Bookmark*، وب‌سایت‌هایی که زیاد به آنها مراجعه می‌کنید را نشان‌دار کنید تا در آینده راحت‌تر به آنها دسترسی یابید.

برای نشان‌دار کردن وب‌سایت، در پنجره Add Bookmark آدرس اینترنتی وب‌سایتی را که می‌خواهید در محیط امن بازدید کنید را وارد کرده و بر روی *Save* کلیک کنید.

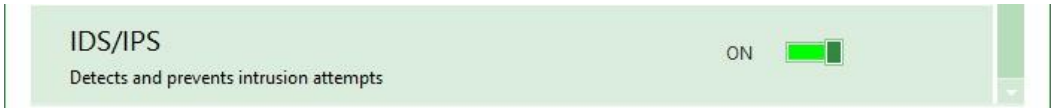
برای مشاهده وب‌سایت‌های نشان‌دار، بر روی View Bookmark کلیک کرده و بر روی آدرس اینترنتی وب‌سایتی که می‌خواهید در محیط امن اجرا شود کلیک کنید.

ز) News Alert (هشدار اخبار)



با استفاده از این ویژگی، آخرین اخبار امنیت سایبری، تهدیدات و هشدارهای ویروس‌ها، و دیگر اطلاعات مهم محافظت از رایانه به اطلاع شما می‌رسد. آخرین اخبار در داشبورد کوییک‌هیل نیز نمایش داده می‌شود. اگر نمی‌خواهید آخرین اخبار را دریافت کنید، این ویژگی را OFF کنید.

ح) IDS/IPS (شناسایی / جلوگیری از نفوذ مجاز)



با استفاده از ویژگی IDS/IPS ، حملات از منابع مختلف نفوذ غیرمجاز به سیستم (IDS/IPS) مانند حملات پویشگر پورت (Port scanning)، حملات توزیع شده اخلال در خدمت (Distributed Denial of Service (DDOS) و غیره شناسایی و از آنها جلوگیری می‌شود.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن IDS/IPS نمایید. این ویژگی به صورت پیش‌فرض فعال است.

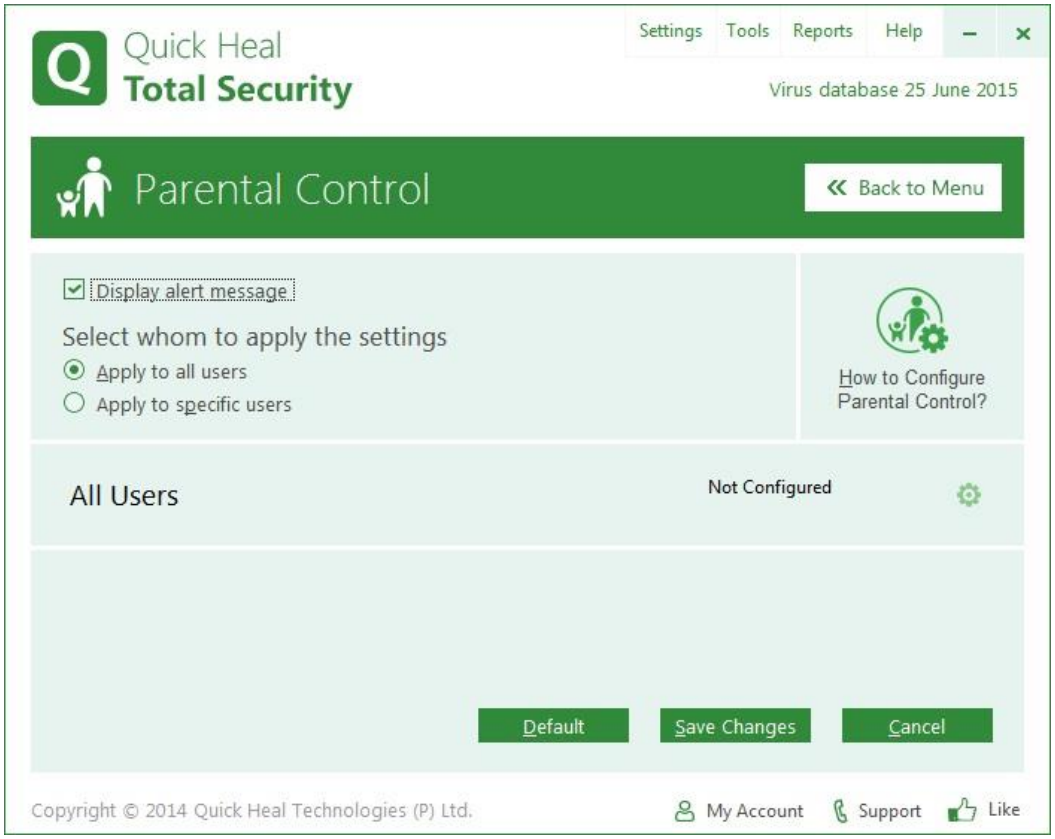
Parental Control (مدیریت خانواده)

با کلیک بر روی چهارمین هسته امنیتی، شما می‌توانید تنظیمات حفاظتی مدیریت خانواده را پیکربندی نمایید.

با استفاده از کنترل خانواده (Parental Control)، والدین می‌توانند فعالیت‌های آنلاین فرزندان خود و دیگر کاربران را به صورت کامل کنترل نمایند. والدین می‌توانند تصمیم بگیرند که فرزندانشان از چه سایت‌هایی بتوانند بازدید کنند و چه وب‌سایت‌هایی باید مسدود شوند. آنها می‌توانند دسترسی به سایت‌ها را بر اساس دسته‌بندی از پیش تعیین شده یا به صورت دلخواه محدود کنند. همچنین می‌توانند دسترسی فرزندان به اینترنت را زمانبندی نمایند تا فرزندان زمان‌های زیادی را پای استفاده از اینترنت تلف نکنند.

کنترل خانواده کوییک‌هیل، به صورت هوشمند با دقت بسیار بالا وب‌سایت‌ها را مطابق محتویات آنها دسته‌بندی می‌کند. اگر شما یک دسته از وب سایت‌ها را مسدود کنید، همه وب‌سایت‌های متعلق به آن گروه یا طبقه بندی مسدود خواهد شد. همچنین می‌توانید مستقیماً وب‌سایت‌های مورد نظر خود را مسدود نمایید.

علاوه بر آن، والدین می‌توانند اجازه دسترسی به برخی از وب‌سایت‌های طبقه‌بندی مسدود شده را بدهند. برای مثال، اگر شما دسترسی به همه وب‌سایت‌های پخش و دانلود رسانه‌ای (Streaming Media and Downloads) را مسدود کردید، می‌توانید دسترسی به یک یا چند سایت عضو این گروه (مثلا aparat.com) را مجاز نمایید. این ویژگی برای والدینی که می‌خواهند کودکاشان تنها به وب‌سایت‌های درست وصل شده و موارد نامناسب به آنها نشان داده نشود، بسیار مناسب است.



نکات مهم پیش از پیکربندی کنترل خانواده!

برای استفاده حداکثری از مزایای ویژگی‌های کنترل خانواده، توصیه می‌شود گام‌های زیر را بردارید:

گام اول:

بررسی کنید که حساب کاربری شما بر روی رایانه‌ای که کوییک‌هیل توتال سکیوریتی در آن نصب شده، دسترسی ادمین و مدیریتی (Administrative) داشته باشد. اگر حساب کاربری شما دسترسی ادمین ندارد، توصیه می‌شود یک حساب کاربری ادمین (Administrator) ساخته و آن را پیکربندی نمایید.

نام کاربری و رمز عبور حساب ادمین را با دیگر کاربران که می‌خواهید محدودیت برای حساب کاربری آنها ایجاد کنید، درمیان نگذارید.

گام دوم:

حساب‌های کاربری استاندارد (کاربر محدود شده یا Restricted) برای فرزندانتان و یا دیگر کاربران بسازید. با این کار آنها دسترسی محدود به سیستم خواهند داشت.

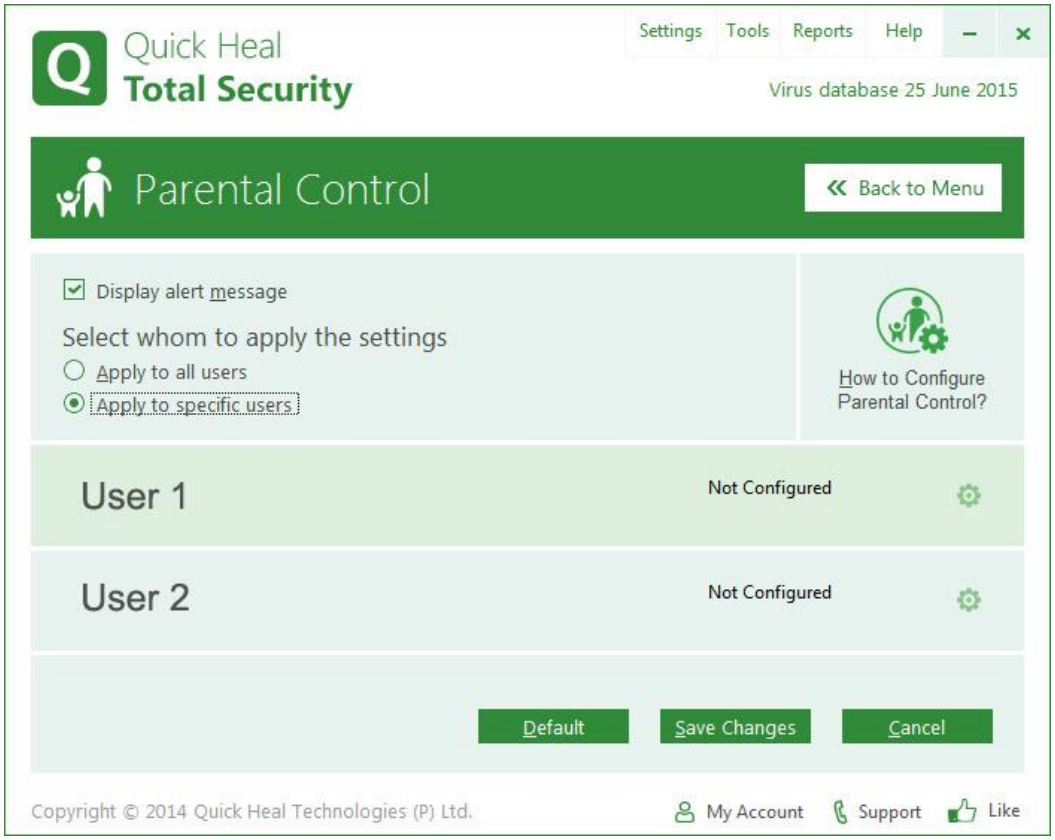
همچنین این قابلیت کمک می‌کند تا سیاست‌های محافظتی مختلف برای کاربران مختلف اعمال نمایید. این سیاست‌ها می‌تواند شامل تنظیمات وب‌سایت برای هر کاربر محدود شده و زمانبندی و برنامه‌ریزی دسترسی به اینترنت باشد.

گام سوم:

محافظت رمز عبور (Password Protect) برای تنظیمات کنترل خانواده، دسترسی غیرمجاز کاربران برای حذف کوییک‌هیل توتال سکیوریتی از سیستم و یا تغییر تنظیمات آن را محدود می‌کند. بنابراین برای کوییک‌هیل با استفاده از منوی *Settings* گزینه *Password Protect* رمز عبور تعیین نمایید.

پیکربندی Parental Control به شرح زیر می‌باشد:

Display alert message: اگر این گزینه تیک باشد، زمانی که کاربران می‌خواهند به یک وب‌سایت مسدود شده دسترسی یابند، پیغام مسدود بودن دسترسی به آنها نمایش داده می‌شود.



Select whom to apply the settings: کاربر یا کاربران قابل محدود کردن در این بخش پیکربندی می‌گردد. این بخش شامل دو گزینه است:

Apply to all users: اگر می‌خواهید تنظیمات (محدودیت) یکسان برای همه کاربران انجام دهید، این گزینه را انتخاب نمایید. اگر این گزینه فعال باشد، در بخش پایینی گزینه All Users نمایش داده خواهد شد که با کلیک بر روی آن می‌توانید کنترل خانواده را بر روی آن اعمال کنید.

Apply to specific users: اگر می‌خواهید برای کاربران مختلف تنظیمات (محدودیت‌های) متفاوت اعمال کنید، این گزینه را انتخاب نمایید. اگر این گزینه فعال باشد، در بخش پایینی لیستی از کاربران موجود

در ویندوز نمایش داده خواهد شد که با کلیک بر روی هر کاربر می‌توانید تنظیمات کنترل خانواده را بر روی آن اعمال کنید.

اگر می‌خواهید برای همه کاربران این رایانه، محدودیت دسترسی به وب‌سایت‌ها یا زمانبندی دسترسی اینترنت قرار دهید، در بخش Select whom to apply the settings، گزینه *Apply to all users* را انتخاب و بر روی *All Users* در ادامه کلیک کنید.

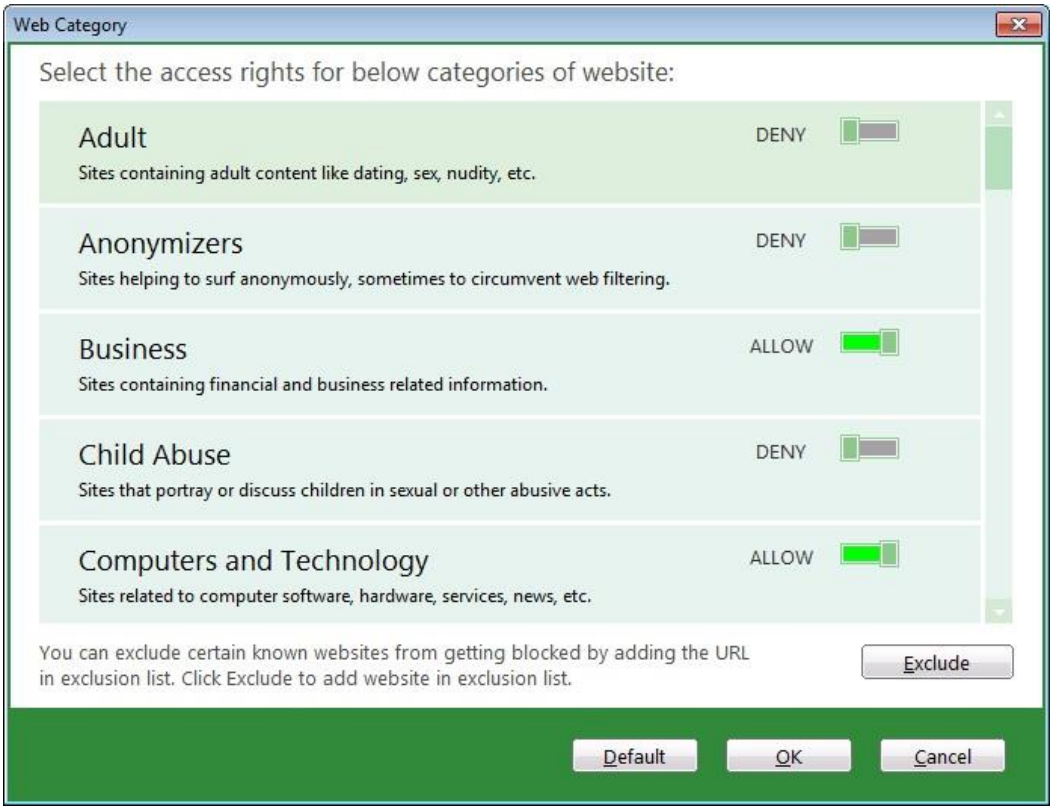
در صورتی که می‌خواهید محدودیت دسترسی بر روی یک یا چند کاربر اعمال شود، گزینه *Apply to specific users* را انتخاب و از لیست پایین صفحه، بر روی نام کاربری موردنظرتان کلیک کنید.

با کلیک بر روی نام کاربری موردنظر (یا همه کاربران) صفحه زیر نمایش داده می‌شود.

صفحه قوانین محافظت نمایش داده خواهد شد.

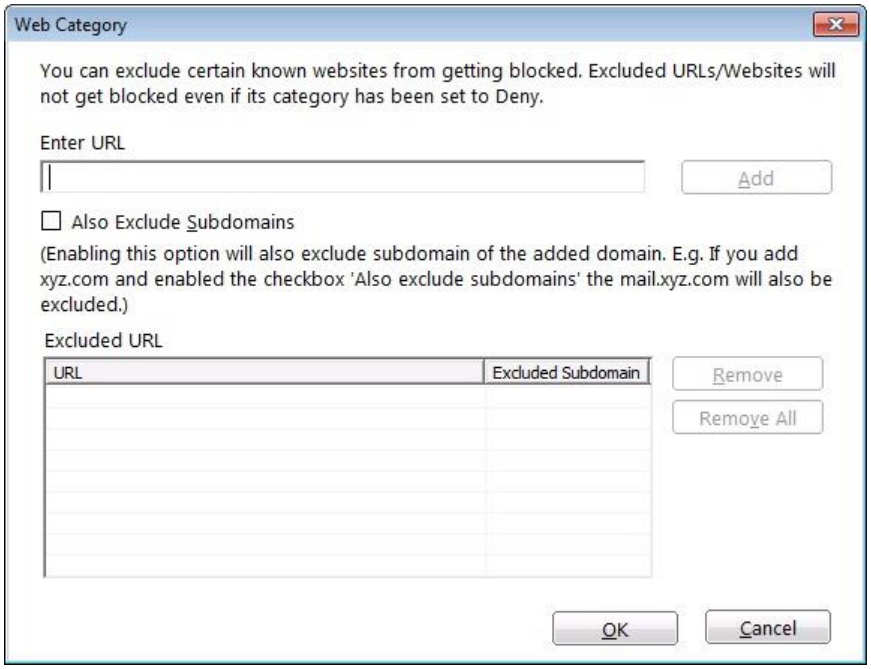
بر اساس نیاز خود می‌توانید هر یک یا همه گزینه‌های زیر را پیکربندی نمایید.

Restrict access to particular categories of website: با انتخاب این گزینه، می‌توانید وب‌سایت‌ها را بر اساس طبقه‌بندی عضو آن مسدود یا مجاز نمایید. مثلاً همه وب‌سایت‌های عضو گروه بازی (Games) را برای فرزندتان غیرمجاز کنید. با کلیک بر روی دکمه Categories... صفحه مربوط به پیکربندی دسته‌بندی‌ها برای مجاز یا مسدود شدن نمایش داده می‌شود.



با کلیک بر روی دکمه خاموش/ روشن می‌توانید طبقه‌بندی مورد نظرتان (مثلا Game) را *Allow* (مجاز) یا *Deny* (غیرمجاز) کنید.

Exclude می‌توانید یک یا چند وب‌سایت (دامنه) را از لیست ممنوع‌ها استثناء کنید. مثلا دسته‌بندی سایت‌های پخش و دانلود چندرسانه‌ای Streaming Media and Downloads را غیرمجاز (Deny) کرده ولی سایت aparat.com را در لیست استثناها قرار دهید تا این سایت توسط کاربر قابل مشاهده باشد. با فشردن دکمه Exclude پنجره لیست استثناها نمایش داده می‌شود:



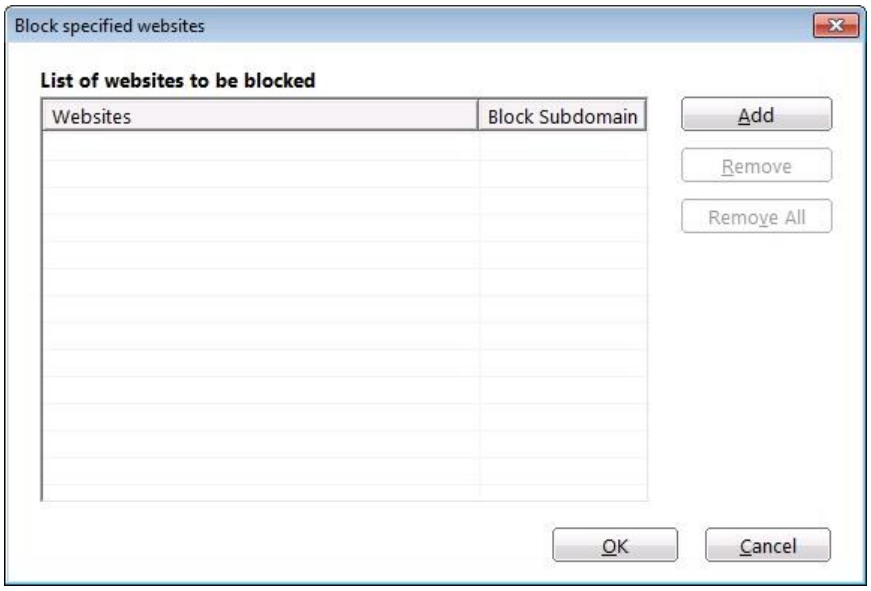
Enter URL: نشانی سایت خود را وارد نمایید. (مثلاً aparat.com)

Also Exclude subdomains: اگر این گزینه تیک باشد، همه زیردامنه های سایت مربوطه نیز مجاز می‌شوند (مثلا images.aparat.com نیز توسط کاربر قابل مشاهده خواهد بود).

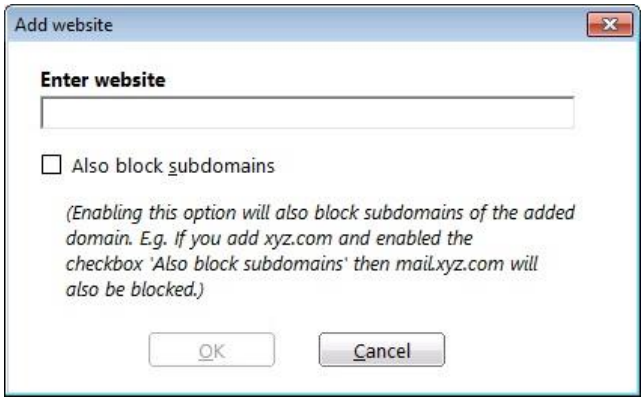
Add: پس از وارد کردن آدرس برای افزودن بر روی این دکمه کلیک کرده و سپس OK می‌کنید.

برای حذف یک آدرس استثناء می‌توانید آدرس سایت مربوطه را انتخاب و گزینه Remove را کلیک کنید. Remove All همه لیست استثناها را حذف می‌کند.

Restrict access to particular website: اگر می‌خواهید یک یا چند وب‌سایت خاص موردنظرتان را مسدود کنید، از این گزینه استفاده کنید. با انتخاب این گزینه و کلیک بر روی *Block List* صفحه پیکربندی مسدود کردن وب‌سایت‌های خاص نمایش داده می‌شود:



برای افزودن یک وب‌سایت خاص بر روی *Add* کلیک کنید.

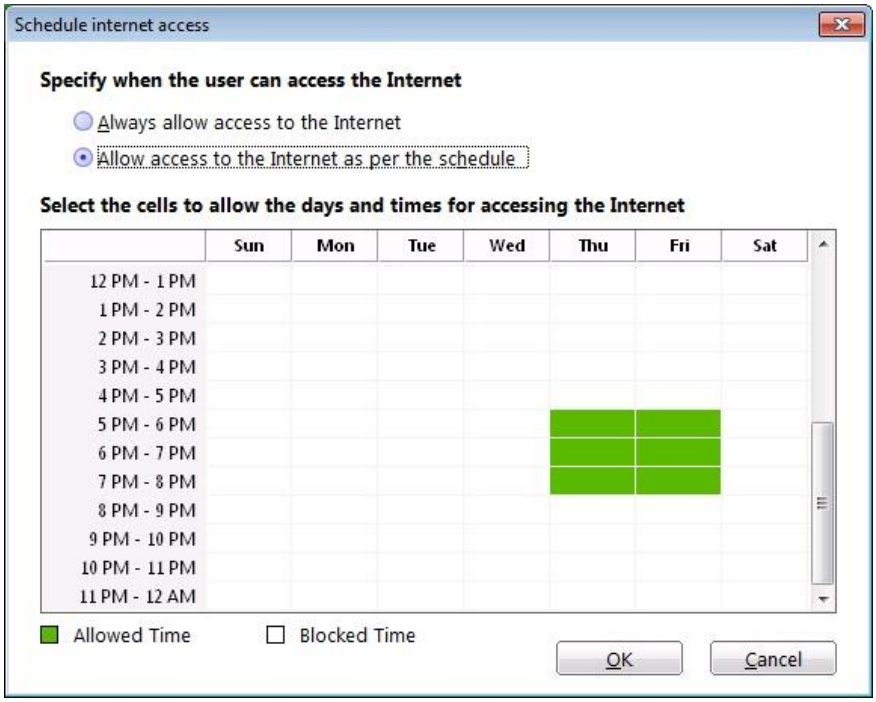


در بخش *Enter website* آدرس وب‌سایت موردنظرتان (مثلاً gmail.com) را نوشته و اگر می‌خواهید همه زیردامنه‌های آن نیز مسدود شوند گزینه *Also block subdomains* را نیز تیک و OK کنید.

حذف یک وب‌سایت از لیست مسدودی با دکمه Remove و حذف همه لیست مسدودی‌ها با دکمه Remove All ممکن می‌باشد.

Schedule Internet access: در این بخش می‌توانید زمان دسترسی فرزندان و یا دیگر کاربران به اینترنت را مدیریت و محدود نمایید. در این صورت فرزندتان تنها در روزها و ساعاتی که شما تعیین می‌کنید می‌تواند به اینترنت متصل گردد.

برای پیکربندی زمان دسترسی به اینترنت، این گزینه را انتخاب و بر روی دکمه Configure… کلیک کنید.



Always allow access to the Internet: اگر این گزینه فعال باشد، محدودیتی برای زمان دسترسی به اینترنت اعمال نشده و همواره امکان ارتباط به اینترنت وجود دارد.

Allow access to the Internet as per the schedule: برای اعمال محدودیت زمانی استفاده از اینترنت این گزینه را انتخاب کنید. با انتخاب این گزینه، بخش پایینی صفحه فعال می‌شود.

در ابتدا همه روزها و ساعت ها غیرفعال می‌باشند. ستونها نشان دهنده روزهای هفته و ردیف‌ها نمایانگر ساعات هفته می‌باشد. ساعات روزهایی از هفته که تمایل دارید کاربر به اینترنت دسترسی داشته باشد، را کلیک می‌کنید تا به رنگ سبز درآید. (مثلا طبق شکل فوق کاربر در ساعات ۵ تا ۸ عصر روزهای پنج‌شنبه و جمعه می‌تواند به اینترنت دسترسی یابد.)

ایجاد حساب کاربری ادمین (Administrator):

حساب کاربری Administrator، امکان نصب و حذف برنامه‌ها و تغییر تنظیمات سیستمی و کنترل خانواده را می‌دهد. با بررسی گام‌های زیر می‌توانید مطمئن شوید که به عنوان والدین، نوع حساب کاربری شما ادمین می‌باشد.

برای بررسی حساب کاربری وارد کنترل پنل شوید (*Control Panel < Start*).

بر روی *User Accounts* کلیک کنید.

پایین نام کاربری شما، نوع حساب کاربری نمایش داده می‌شود. مطمئن شوید که نوع حساب کاربری *Administrator* می‌باشد. اگر حساب کاربری شما Administrator نبود، آن را به Administrator تغییر دهید.

ایجاد حساب کاربری محدود شده (restricted user):

یک حساب کاربری محدود شده تنها می‌تواند به حساب کاربری خود دسترسی داشته باشد و امکان دسترسی کامل به رایانه را ندارد. این کار باعث می‌شود تا کاربران نتوانند تغییراتی در کامپیوتر ایجاد نموده و سیاست‌های امنیتی را تغییر دهند.

برای ایجاد حساب کاربری محدود گام‌های زیر را دنبال کنید:

برای سیستم‌عامل ویندوز XP:

۱. بر روی *Start < Control Panel < User Accounts* کلیک کنید.
۲. در زیر *User Accounts*، بر روی *Create a New User Account* کلیک نمایید.
۳. نام کاربری را در بخش Account Name تکمیل کرده بر روی Next کلیک کنید.
٤. گزینه Limited را تیک کنید.
٥. بر روی Create Account کلیک کنید.

برای سیستم‌عامل ویندوز Vista / Windows 7:

۱. بر روی *Start < Control Panel < User Accounts* کلیک کنید.
۲. در زیر *User Accounts*، بر روی *Manage Other Account* کلیک نمایید.
۳. بر روی گزینه *Create a New User Account* کلیک کنید.
٤. نام کاربری را در *Account Name* درج کرده و گزینه *Standard user* را تیک کنید.
٥. بر روی *Create Account* کلیک کنید تا حساب کاربری جدید ایجاد شود.

External Drives and Devices (درایوها و ابزارهای خارجی)

با کلیک بر روی آخرین هسته امنیتی، شما می‌توانید تنظیمات حفاظتی مربوط به درایوها و ابزارهای خارجی قابل اتصال به رایانه را پیکربندی نمایید.

زمانی که یک ابزار خارجی مانند دیسک‌های فلش USB، یا هارد اکسترنال را به سیستم خود متصل می‌کنید، سیستم خود را در معرض خطر نفوذ آلودگی ویروس‌ها و بدافزارها از طریق آنها قرار می‌دهید.

این ویژگی کمک می‌کند تا با قوانین حفاظتی مناسب برای ابزارهای خارجی مانند CDها، DVDها و انواع حافظه‌ها و درایوهای ذخیره‌سازی مبتنی بر USB اعمال نمایید.

الف) Autorun Protection (محافظت آتوران)

ویژگی آتوران (autorun) که در ابزارهای USB یا CD/DVD ها استفاده می‌شود موجب می‌شود تا به محض اتصال فلش USB یا وارد کردن CD/DVD به رایانه، به صورت خودکار اجرا شود. بدافزارهای آتوران نیز با استفاده از این ویژگی همزمان با اتصال ابزار به صورت خودکار اجرا شده و موجب گسترش بدافزار و ویروس شده و به سیستم آسیب جدی می‌رساند. ویژگی محافظت آتوران (اجرای خودکار) از رایانه در برابر بدافزارهای آتوران محافظت می‌کند.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن ویژگی محافظت در برابر بدافزارهای Autorun نمایید. محافظت آتوران به صورت پیش‌فرض روشن است.

ب) Scan External Drives (محافظت آتوران)

ابزارهای مبتنی بر USB، ابزارهای خارجی می‌باشند که می‌توانند بدافزار را به سیستم منتقل نمایند. با این ویژگی، به محض اتصال درایوهای مبتنی بر USB به رایانه، به صورت خودکار اسکن و ویروسیابی می‌شوند.

توجه ۱: اگر این گزینه غیرفعال باشد، درایو USB شما ویروسیابی و پاکسازی نشده، اما به محض دسترسی به فایل درون USB جهت اجرا یا کپی به داخل رایانه، به صورت خودکار اسکن و ویروسیابی می‌شود.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه ON/OFF اقدام به فعال کردن یا غیرفعال کردن ویژگی اسکن درایوهای خارجی نمایید. این ویژگی به صورت پیش‌فرض روشن است.

برای تنظیمات بیشتر بر روی عنوان Scan External Drives کلیک کنید.

Scan files on the root of the drive only: اگر این گزینه انتخاب باشد، تنها فایل‌های ریشه‌ی درایو USB اسکن شده و فایل‌های داخل پوشه‌ها اسکن نمی‌شوند. این نوع اسکن زمان کمتری را گرفته اما امنیت پایین‌تری را ارائه می‌دهد.

Scan full drive: اگر می‌خواهید همه فایل‌های درون درایو USB اسکن شوند، این گزینه را انتخاب نمایید. این نوع اسکن زمان بیشتری را گرفته اما امن‌تر می‌باشد. اگرچه به صورت پیش‌فرض این گزینه فعال است.

توجه ۲: اگر ویژگی محافظت ضد سرقت (Data Theft Protection) روشن و گزینه مسدود کردن کامل دسترسی به درایوهای خارجی (Block complete access to external drives) انتخاب شده باشد، چون دسترسی به این درایوها مسدود شده، بنابراین امکان اسکن درایوهای USB وجود ندارد.

ج) Data Theft Protection (محافظت از سرقت داده)

با استفاده از این ویژگی می‌توانید نقل و انتقال اطلاعات بین رایانه و درایوهای USB و ابزارهای CD/DVD را مسدود کنید. با استفاده از محافظت از سرقت اطلاعات (Data Theft Protection) مطمئن می‌شوید که اطلاعات شخصی درون رایانه شما به هیچ درایو یا ابزار خارجی کپی نمی‌شود. همچنین می‌توانید انتقال اطلاعات از درایوهای USB و ابزارهای CD/DVD به سیستم خود را مسدود نمایید. بنابراین می‌توانید هم از سرقت اطلاعات خود جلوگیری نمایید و هم از ورود فایل‌های مخرب به رایانه خود جلوگیری نمایید.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه *ON/OFF* اقدام به فعال کردن یا غیرفعال کردن ویژگی محافظت از سرقت داده نمایید. این ویژگی به صورت پیش‌فرض خاموش است.

برای پیکربندی محافظت از سرقت داده ابتدا این ویژگی را ON کرده سپس بر روی عنوان *Data Theft Protection* کلیک کنید.

Read only and no write access to external drives: امکان انتقال اطلاعات از درایوهای USB و ابزارهای CD/DVD به رایانه را می‌دهد، اما اجازه کپی برعکس (سرقت اطلاعات از رایانه به درایو USB و CD/DVD) را نمی‌دهد. به صورت پیش فرض این گزینه انتخاب شده است.

Block complete access to external drives: هرگونه نقل و انتقال بین رایانه و انواع ابزارهای خارجی را مسدود می‌کند. (نه امکان کپی اطلاعات از فلش به سیستم وجود دارد نه کپی از سیستم به فلش)

Authorize USB drive: اگر می‌خواهید تنها کاربران مجاز بتوانند به درایوهای USB و ابزارهای CD/DVD دسترسی یابند این گزینه را انتخاب نمایید. اگر این گزینه انتخاب شود، هنگام اتصال ابزار خارجی به رایانه، با نمایش پیامی از کاربر درخواست رمزعبور می‌گردد. در صورت وارد کردن صحیح رمزعبور کاربر می‌تواند به اطلاعات ابزار خارجی دسترسی یابد.

توجه: زمانی این گزینه فعال است که برای آنتی‌ویروس خود از منوی Settings گزینه Quick Heal Password Protection، رمز عبور تعیین کرده باشید.

د) Scan Windows Mobile (اسکن ویندوز موبایل)

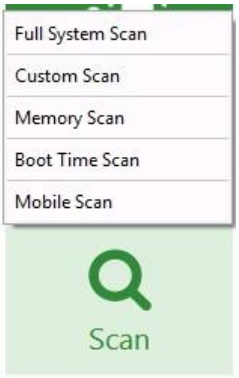
این ویژگی موجب می‌گردد تا به محض اتصال موبایل با سیستم عامل Windows Mobile phone، با استفاده از کابل USB یک پیغام برای اسکن گوشی ویندوز موبایل نمایش داده شود.

ON/OFF: شما می‌توانید با کلیک بر روی دکمه *ON/OFF* اقدام به فعال کردن یا غیرفعال کردن ویژگی اسکن ویندوز موبایل نمایید. این ویژگی به صورت پیش‌فرض روشن است.

ویژگی دسترسی سریع

بخش انتهایی صفحه داشبورد (اول) برخی ویژگی‌های مهم مانند گزینه‌های اسکن (Scan)، بهینه‌سازی سیستم (PCTuner) و آخرین اخبار امنیتی را ارائه می‌دهد.

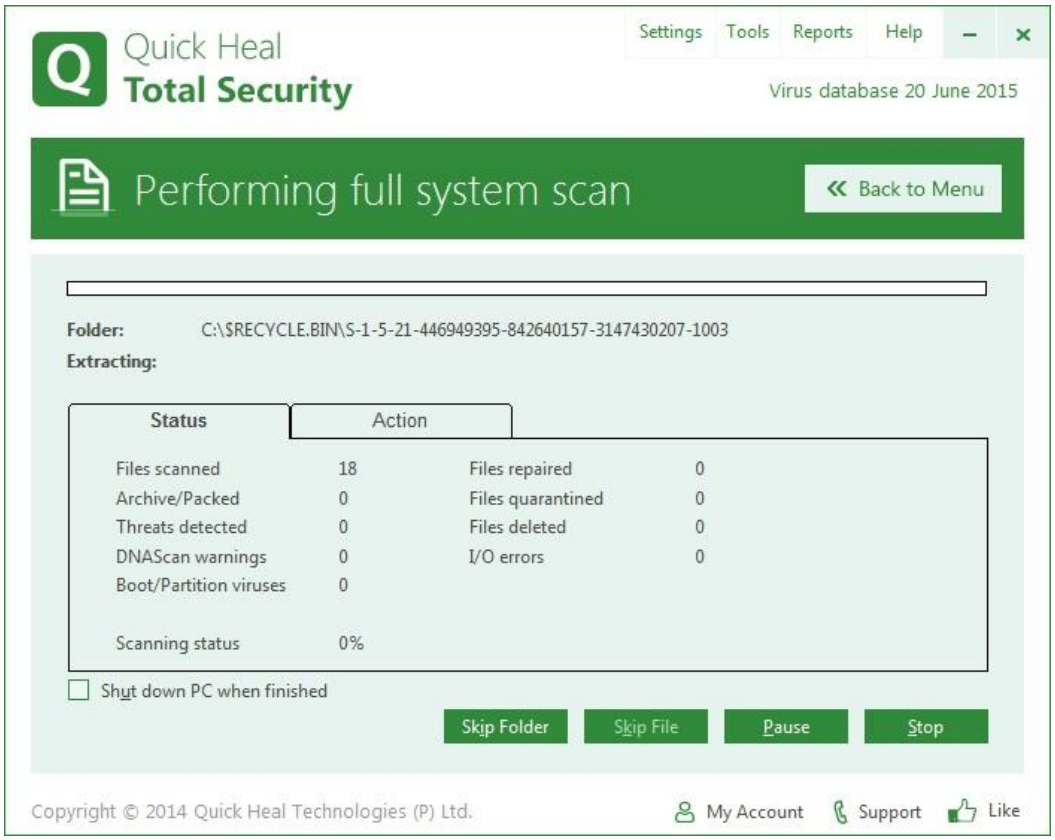
الف) گزینه‌های اسکن (Scan)



گزینه‌های مختلف اسکن که در داشبورد کوییک‌هیل توتال سکیوریتی وجود دارد، امکان اسکن‌های متنوع سیستم را بر اساس نیازهای کاربر ارائه می‌دهد.

شما می‌توانید کل سیستم، درایوها، درایوهای شبکه، درایوهای USB، پوشه‌های یا فایل‌ها، مکان‌ها و درایوهای خاص، حافظه اصلی (RAM)، زمان راه‌اندازی (boot time) را اسکن کنید. اگرچه تنظیمات پیش‌فرض برای اسکن دستی معمولا کافی است، اما می‌توانید تنظیمات اسکن دستی را به صورت دلخواه تغییر دهید.

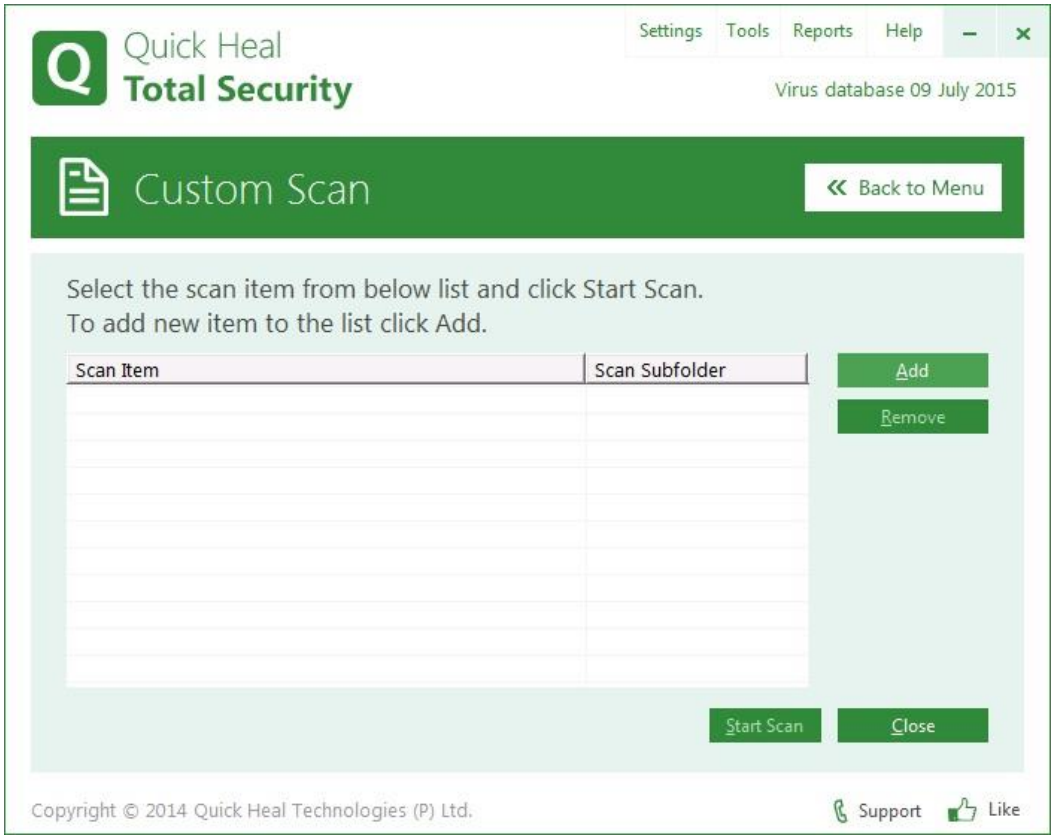
Full System Scan: این گزینه به صورت کامل همه رکوردهای راه‌انداز، درایوها، پوشه‌ها، فایل‌ها و حفره‌ها و آسیب‌پذیری‌های سیستم شما را اسکن می‌کند (به غیر از درایوهای شبکه map شده).



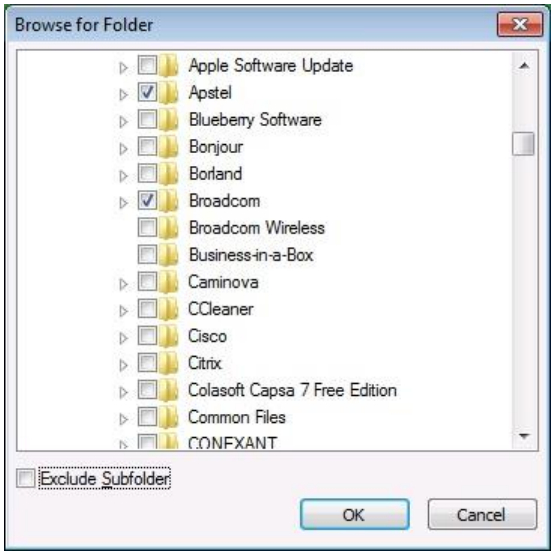
توجه ۱: پس از پایان اسکن، می‌توانید گزارش کامل اسکن را از منوی *Reports* مشاهده نمایید..

توجه ۲: در صورت اجرا اسکن کامل سیستم، به صورت خودکار اسکن آسیب‌پذیری (Vulnerability Scan) در پس‌زمینه اجرا می‌شود.

Custom Scan: اگر می‌خواهید تنها برخی درایوها یا پوشه‌های خاص –نه کل- سیستم خود را اسکن کنید، از این گزینه استفاده نمایید.



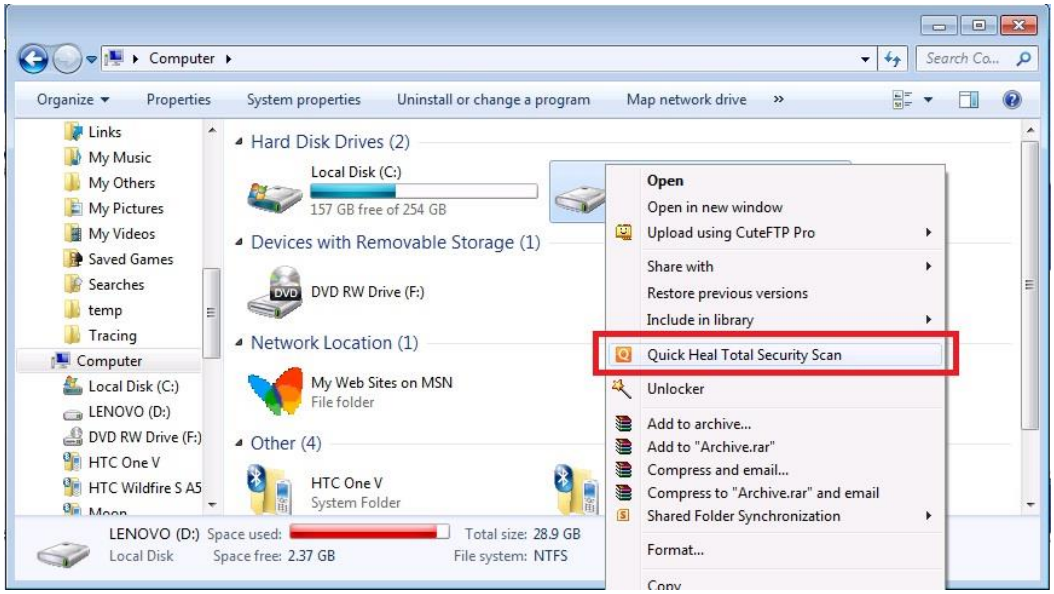
در صفحه Custom Scan لیستی از آیتم‌های اسکن نمایش داده می‌شود. برای افزودن یک آیتم به اسکن سفارشی، بر روی دکمه *Add* کلیک کنید. صفحه Browse a Folder نمایش داده می‌شود. از لیست درایوها و پوشه‌های سیستم، درایوها یا پوشه‌هایی که قصد اسکن آنها را دارید تیک کنید. اگر می‌خواهید فقط فایل‌های درون پوشه‌ی اصلی اسکن شده و زیرپوشه‌های داخلی آن اسکن نشود، گزینه *Exclude Subfolder* را تیک کنید.



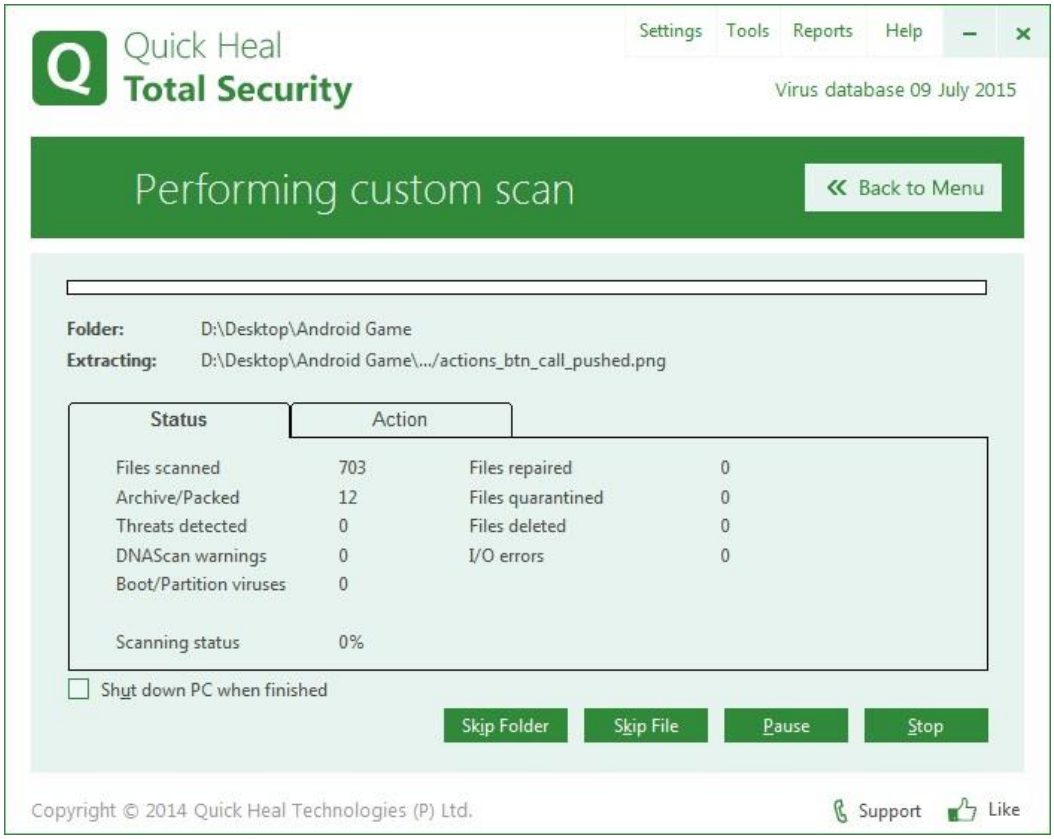
پس از افزودن به لیست، آیتم اسکن موردنظر را انتخاب بر روی دکمه *Start Scan* کلیک کنید.

Memory Scan: اگر می‌خواهید تنها حافظه اصلی (RAM) سیستم اسکن گردد، از این گزینه استفاده نمایید.

روش اسکن انتخابی



اسکن فایل‌ها، پوشه‌ها و یا درایوها از چند طریق ممکن است. یکی از روش‌ها کلیک راست بر روی درایو یا پوشه یا فایل موردنظر و انتخاب گزینه *Quick Heal Total Security Scan* می‌باشد. با انتخاب این گزینه، آیتم انتخابی اسکن و ویروسیابی می‌گردد.



نمایش اطلاعات اسکن

در زمان اسکن، اطلاعات زیر نمایش داده می‌شود:

Files scanned	مجموع تعداد فایل‌های اسکن شده را نمایش می‌دهد.
Archive/Packed	تعداد فایل‌های بسته‌ای یا آرشیوی (فشرده) اسکن شده را نشان می‌دهد.
Threats detected	تعداد تهدیدات و آلودگی‌های کشف شده را نشان می‌دهد.
DNAScan warnings	تعداد فایل‌های شناسایی شده توسط DNAScan را نشان می‌دهد.
Boot/Partition viruses	تعداد ویروس‌های پارتیشن/راه‌انداز (Boot) را نشان می‌دهد.
Files repaired	تعداد فایل‌های مخربی که تعمیر شده‌اند را نشان می‌دهد.
Files quarantined	تعداد فایل‌های مخربی که قرنطینه شده‌اند را نشان می‌دهد.
Files deleted	تعداد فایل‌های مخربی که حذف شده‌اند را نشان می‌دهد.
I/O errors	تعداد خطاهای ورودی/خروجی اتفاق افتاده در طول اسکن را نشان می‌دهد.
Scanning status	وضعیت جاری اسکن درحال اجرا را نشان می‌دهد.

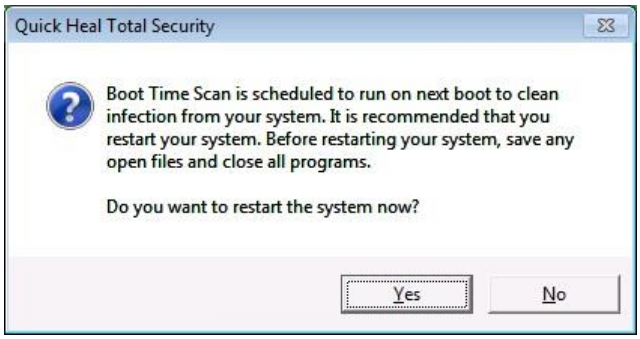
Boot Time Scan: زمانی که سیستم به شدت آلوده باشد، این گزینه بسیار مفید است. برخی از ویروس‌ها زمانی که سیستم درحال اجراست، فعال می‌شوند و امکان پاکسازی آنها در محیط ویندوز ممکن نیست. اگرچه می‌توانید با استفاده از *Boot Time Scan* (اسکن زمان راه‌اندازی) چنین ویروس‌های خطرناک را از بین ببرید. پس از اجرای این گزینه، پس از راه‌اندازی مجدد سیستم (Restart)، پیش از بارگذاری ویندوز در محیط پوسته بوت ویندوز اسکن و پاکسازی صورت می‌گیرد.

پس از اجرا این اسکن، پنجره‌ای باز شده و نوع اسکن را از شما می‌پرسد:

Quick Scan: اسکن سریع که تنها محل‌های از پیش‌تعریف شده که دارای ریسک و خطر بالایی از ویروس‌های هستند را اسکن می‌کند.

Full System Scan: سیستم را به صورت کامل اسکن می‌کند. این گزینه ممکن است زمان بیشتری را صرف کند.

پس از کلیک بر روی دکمه Yes، پنجره‌ی دیگری باز شده و از شما می‌پرسد که آیا می‌خواهید همین الان سیستم راه‌اندازی مجدد گردد یا خیر. برای تعویق اسکن دکمه No و برای اسکن فوری دکمه Yes را کلیک کنید.



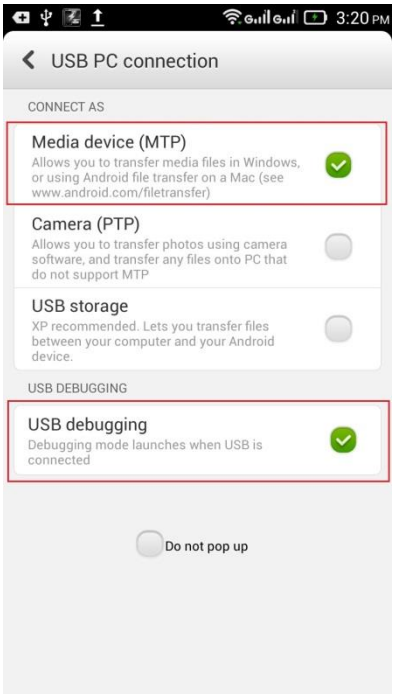
توجه: در صورتی که اسکن زمان راه‌اندازی (Boot Time Scan) زمان زیادی را صرف می‌کند و یا به اشتباه این گزینه را انتخاب کردید، برای خروج از اسکن کلید ESC صفحه کلید را بفشارید.

Mobile Scan: با استفاده از تکنولوژی انحصاری PC2Mobile کوییک‌هیل می‌توانید بسیاری از گوشی‌های موبایل را بدون نیاز به نصب آنتی‌ویروس بر رو آنها اسکن و از ویروس‌های کامپیوتری و موبایلی پاکسازی نمایید. پیش از شروع به اسکن، شرایط زیر را مشاهده فرمایید:

- ویژگی اسکن موبایل از سیستم‌عامل‌های Windows XP، Windows Vista، Windows 7، Windows 8 و Windows 8.1 پشتیبانی می‌کند.
- برای دستگاه‌های مبتنی بر ویندوز موبایل (Windows Mobile نسخه ۳.۰ و جدیدتر تا نسخه ۷.۰) باید نرم‌افزار Microsoft Active Sync 4.5 یا جدیدتر را بر روی ویندوز XP (نسخه ۳۲ بیتی) نصب نمایید؛ برای سیستم‌عامل‌های ویندوز ویستا، ویندوز ۷، ویندوز ۸ و ویندوز ۸.۱ برنامه Windows Mobile Device Center باید نصب باشد.
- برای گوشی‌های قدیمی‌تر، نرم‌افزار PCSuite و درایور دستگاه (موبایل) را بر روی کامپیوتر خود نصب کنید. زمانی که دستگاه شما به PCSuite متصل گردید، از PCSuite خارج شوید.

  توصیه می‌شود نرم‌افزار PCSuite صحیح و متناظر با دستگاه خود را نصب کنید. مثلا برای گوشی‌های سامسونگ برنامه Kies (PCSuite) و برای گوشی‌های نوکیا نرم‌افزار Nokia PCSuite را نصب کنید.
- برای اتصالات Bluetooth، سیستم شما باید دارای ابزار بلوتوث بوده و درایورهای مناسب آن نصب شده باشد.
- برای ابزارهای بلوتوث تنها از درایورهای Microsoft، Broadcom و Widcomm پشتیبانی می‌شود.

  برای دریافت نتایج بهتر، توصیه می‌شود درایورهای Microsoft را بر ای ابزار بلوتوث خود نصب کنید.
- برای اتصالات بلوتوثی و کابلی بین دستگاه‌های موبایل و کامپیوتر، در برخی از مدل‌های گوشی، نیاز است که Quick Heal Connector بر روی دستگاه موبایل نصب گردد. ویزارد اتصال موبایل کوییک‌هیل راهنمایی لازم برای نصب برنامه اتصال دهنده کوییک‌هیل بر روی موبایل را ارائه می‌دهد.
- برای اسکن دستگاه‌های اندروید، مطمئن شوید که دستگاه از طریق کابل USB به رایانه متصل شده، و گزینه‌های USB debugging و Stay awake و نوع ارتباط Media Device (MTP) می‌بایست فعال باشند.

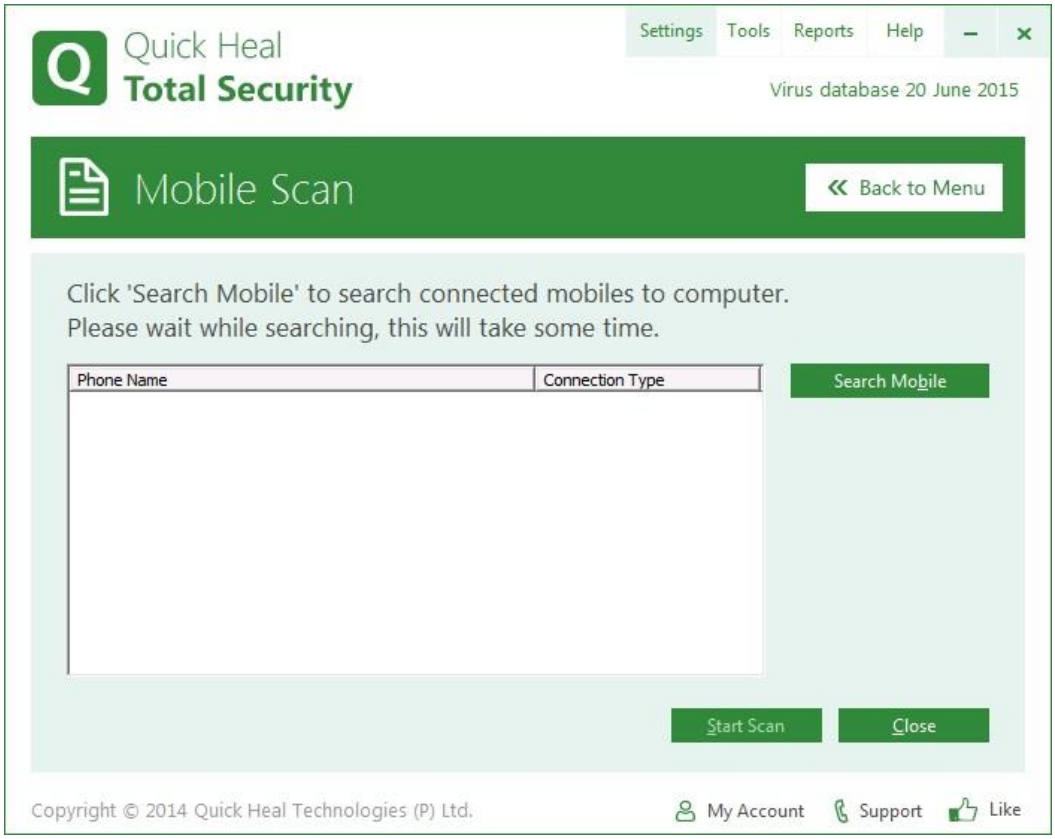


توجه ۱: شما می‌توانید برای دریافت لیست گوشی‌های قابل پشتیبانی به نشانی http://www.quickheal.co.ir/pc2mobile مراجعه فرمایید.

توجه ۲: ویژگی PC2Mobile با نرم‌افزار کوییک‌هیل توتال سکیوریتی برای اندروید متفاوت می‌باشد. این ویژگی آلودگی‌ها و ویروس‌های موجود در موبایل را پاکسازی می‌کند. اما نرم‌افزار Quick Heal Total Security for Android با جلوگیری از ورود و نفوذ ویروس‌ها، محافظت و امنیت پیشگیرانه را ارائه می‌دهد. همچنین ویژگی‌های مختلف امنیتی و کاربردی دیگر مانند ضد سرقت، کنترل مصرف شبکه، بهینه‌سازی موبایل و... را ارائه می‌دهد.

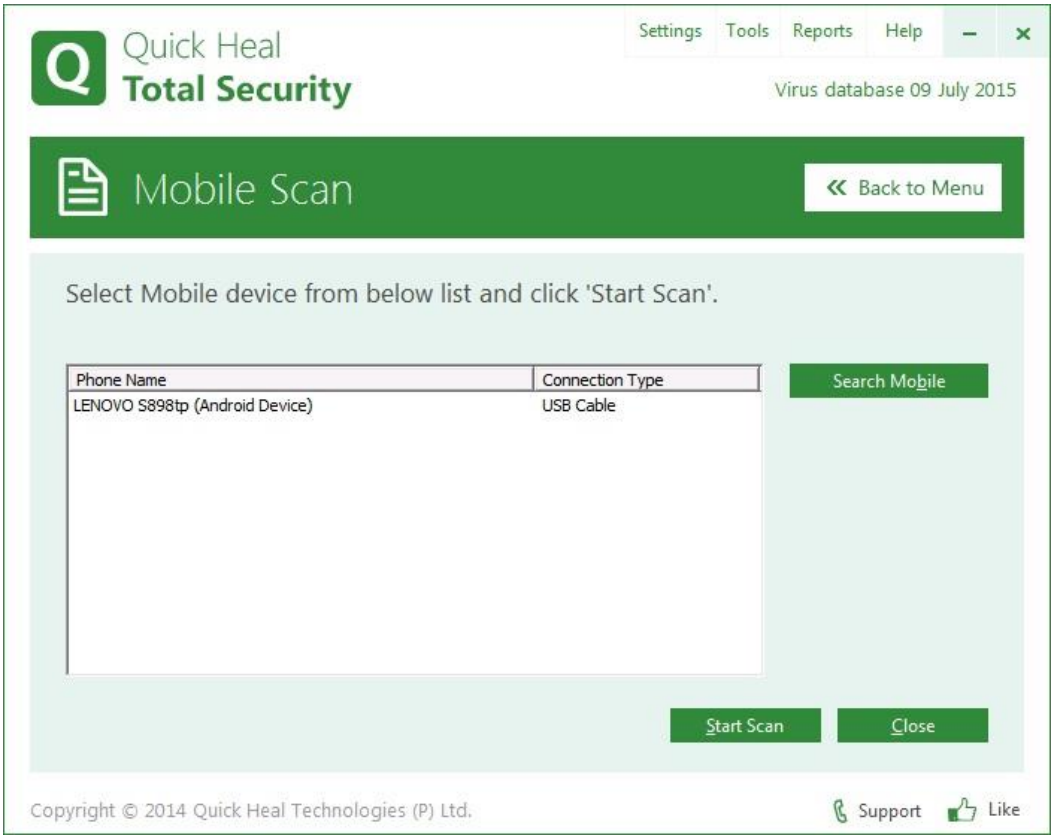
برای اجرای اسکن موبایل:

۱. بر روی دکمه *Mobile Scan* کلیک کنید.
۲. گوشی موبایل را از طریق کابل USB یا بلوتوث به کامپیوتر متصل کنید.
۳. به شرایط ذکر شده در مورد تنظیمات نوع اتصالات گوشی توجه کنید.

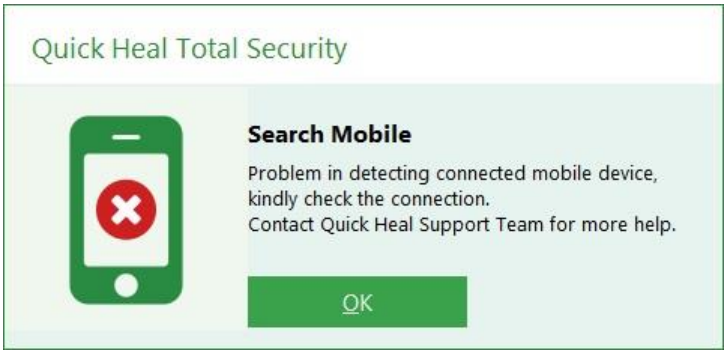


٤. صفحه اسکن موبایل اجرا می‌شود. بر روی دکمه ***Search Mobile*** کلیک کنید.

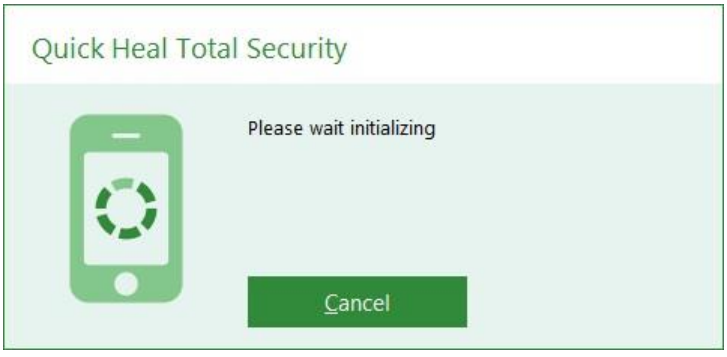
٥. بر روی دکمه ***Start Search*** کلیک کنید. مدتی منتظر بمانید تا جستجو خاتمه یابد.



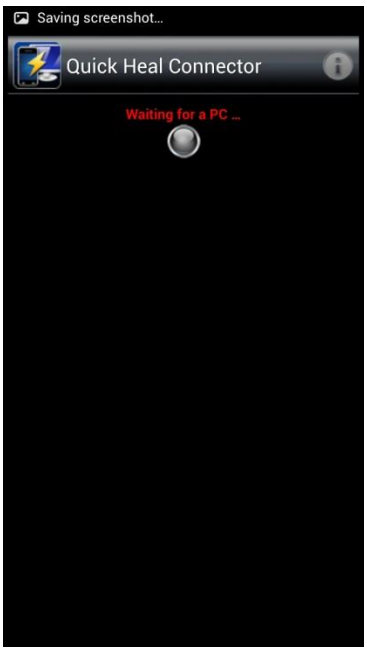
٦. پس از یافته شدن گوشی نام آن در لیست نمایش داده خواهد شد. با انتخاب دستگاه مورد نظر بر روی دکمه ***Start Search*** کلیک کنید.



برنامه جادویی اتصال موبایلی توتال سکیوریتی، بررسی می‌کند که آیا مدل موبایلی که انتخاب کرده‌اید به کامپیوتر متصل است یا خیر. اگر موبایل به سیستم متصل نباشد، اسکنی آغاز نخواهد شد.



اگر موبایل به سیستم متصل باشد، دکمه *Install Connector* در دسترس قرار می‌گیرد. برای ارتباط بین رایانه و موبایل، رابط کوییک هیل باید بر روی موبایل نصب باشد.



اگر Connector کوییک‌هیل از قبل بر روی موبایل شما نصب شده است، آنرا اجرا نمایید.

۷. اگر گوشی موبایل شما نیاز دارد تا برنامه رابط کوییک هیل (Quick Heal Connector) بر روی آن نصب شود، پیام نصب رابط نمایش داده می‌شود. برای نصب برنامه رابط کوییک هیل بر روی دکمه *Install Connector* کلیک کنید.

در گوشی‌های اندروید، پس از نصب برنامه رابط کوییک هیل، اسکن موبایل آغاز می‌شود. برای بستن پنجره Mobile Scan بر روی دکمه *Close* کلیک کنید.

پس از پایان اسکن، گزارشی از نتایج اسکن نمایش داده خواهد شد.

فعال کردن گزینه Stay awake در اندروید:

برای فعال کردن گزینه *Stay awake* در اندروید از مسیر زیر عمل کنید:

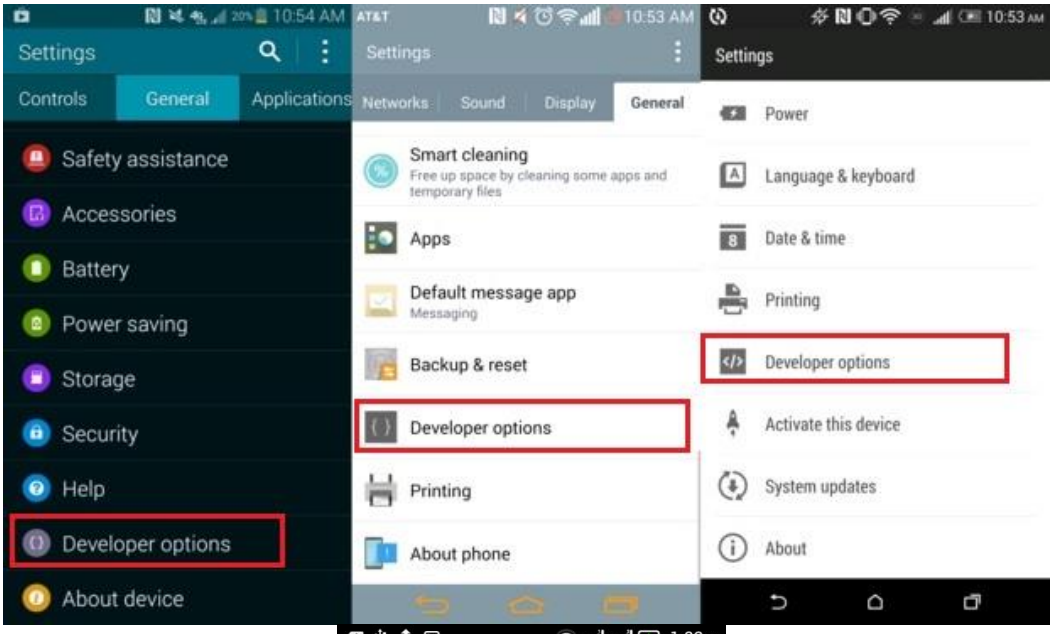
۱. بسته به مدل گوشی از یکی از مسیرهای زیر وارد تنظیمات گوشی شوید:

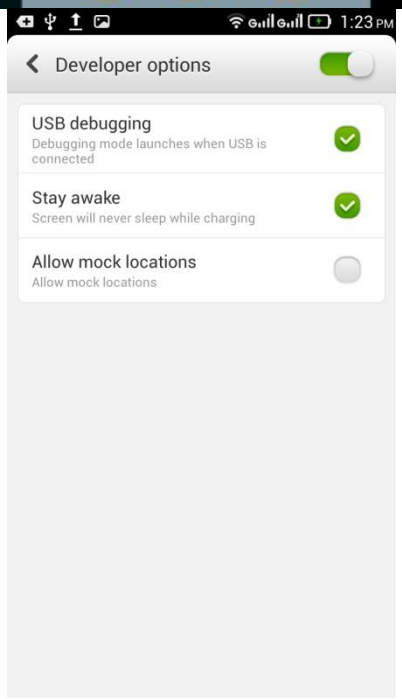
Settings > About Devive > Version Infos
Settings > About phone > Build number
Setings > About device > Build number

Settings > About phone > Software information > Build number
Settings > About > Software information > More > Build number

۲. چندین بار بر روی *Build number* کلیک کنید تا گزینه *Develper Option* فعال شود. معمولاً این گزینه در *Settings* یا تنظیمات قرار می‌گیرد.

۳.





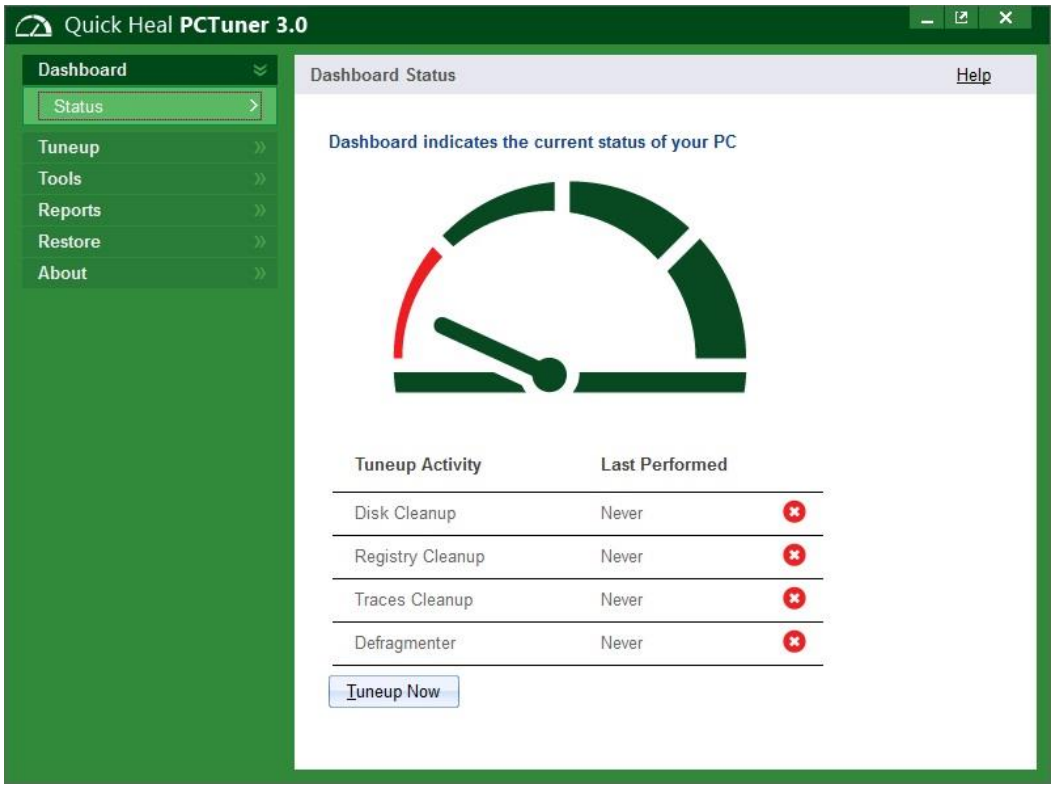
٤. در بخش گزینه های توسعه دهنده (Developer) می‌توانید گزینه های USB debugging و Stay awake را فعال نمایید.

ب) PCTuner (بهینه سازی سیستم)

نرم‌افزار Quick Heal PCTuner یک نرم‌افزار مستقل می‌باشد که به همراه کوییک هیل توتال سکیوریتی به صورت درونساز و رایگان ارائه می‌گردد. با استفاده از این برنامه می‌توانید کارایی کامپیوتر خود را افزایش داده و با پاکسازی آثار ردیابی اینترنتی و برنامه‌های مختلف، از حریم خصوصی خود محافظت نمایید.

استفاده منظم از ابزار PCTuner موجب حفظ حداکثری کارایی سیستم می‌گردد.

با کلیک بر روی آیکن PCTuner (پی.سی.تیونر) بر روی داشبورد کوییک‌هیل برنامه اجرا می‌شود.



در صفحه داشبورد برنامه بهینه‌ساز رایانه، می‌توانید وضعیت کارایی سیستم را به صورت خلاصه ملاحظه نمایید. با کلیک بر روی دکمه *Tuneup Now* برنامه به صورت پیش‌فرض، اقدام به پاکسازی اطلاعات زائد دیسک، پاکسازی اطلاعات زائد رجیستری، پاکسازی آثار ردیابی، یکپارچه‌سازی (deragment) بخش‌های مهم هارددیسک پس از راه اندازی مجدد سیستم نمایید.

امکانات پیشرفته‌تر از منوی سمت چپ قابل پیکربندی می‌باشد.

توجه: همه‌ی فایل‌هایی که از کامپیوتر حذف می‌شوند یا هارددیسک‌هایی که فرمت می‌شوند، به سادگی توسط برنامه‌های بازیابی کننده قابل بازیابی هستند. یکی دیگر از امکانات این برنامه حذف فایل به صورت رمز شده می‌باشد. با این امکان مطمئن می‌شوید که فایل‌های شخصی و محرمانه شما پس از حذف توسط هیچ کس قابل بازیابی نیست.

ج) News (اخبار)

بخش اخبار کوییک‌هیل، آخرین اخبار امنیت سایبری، تهدیدات ویروس‌ها، هشدارها و دیگر اطلاعات مهم مربوط به امنیت و رایانه را به اطلاع کاربران می‌رساند. برای دریافت آخرین اطلاعات باید از لایسنس معتبر کوییک‌هیل استفاده نمایید.

منوی Settings

در این صفحه تنظیمات کلی آنتی‌ویروس پیکربندی می‌گردد.

الف) Importing and Exporting Settings (استخراج و وارد کردن تنظیمات)

با استفاده از دکمه *Imoprt / Export* شما می‌توانید از تنظیمات انجام شده بر روی آنتی‌ویروس خروجی گرفته و یا تنظیماتی که قبلا خروجی گرفته اید را وارد نمایید. این ویژگی زمانی که می خواهید آنتی‌ویروس را مجدداً نصب نمایید و یا تنظیمات یکسان را بر روی چندین رایانه اعمال کنید مفید است. نوع محصول و نسخه دو نرم‌افزاری که از تنظیمات آن استخراج و وارد می‌شوند، باید یکی باشد (مثلا محصول Quick Heal Total Security نسخه 16)

Export settings to a file: یک فایل خروجی با پسوند .dat ایجاد می‌کند.

Import settings from a file: می‌توانید فایل تنظیمات با پسوند .dat را وارد نمایید.

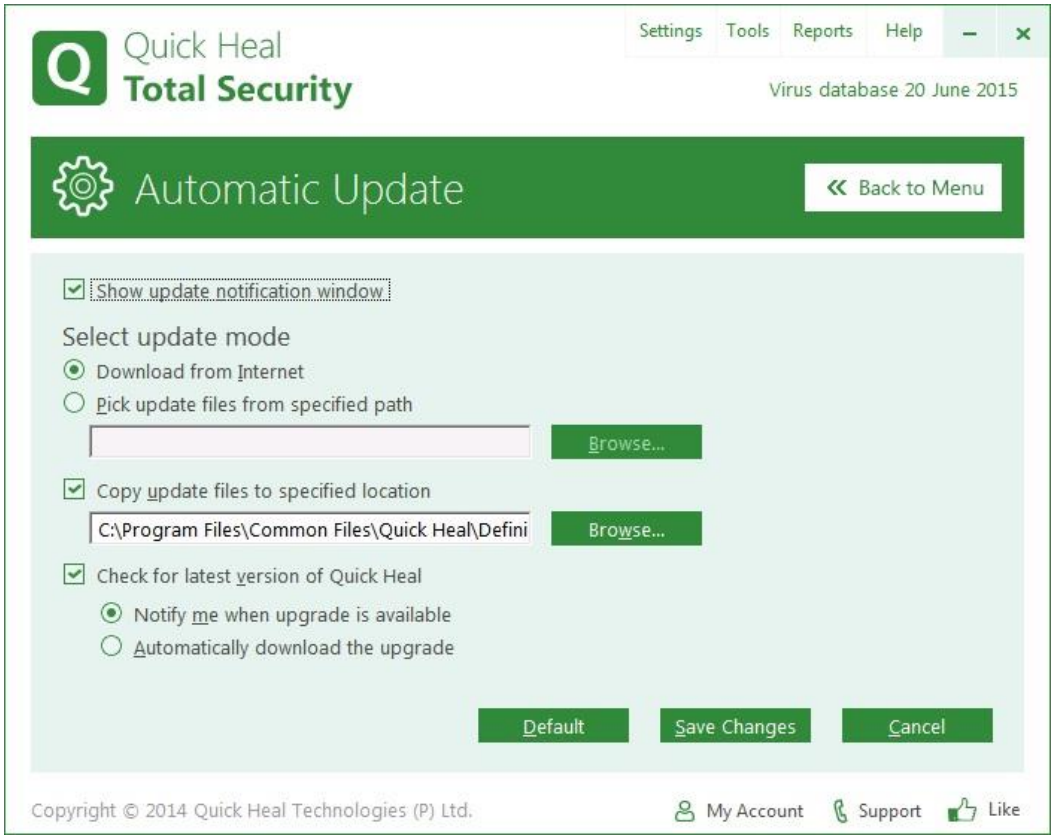
توجه ۱: در صورت وارد کردن تنظیمات، همه تنظیمات قبلی از بین می‌روند.

توجه ۲: تنظیمات Scheduled Scans، Browser Sandbox و Password Protection قابل استخراج و وارد کردن نمی‌باشند.

ب) Automatic Update (بروزرسانی خودکار)

با روشن (ON) بودن این ویژگی به محض اتصال به اینترنت آنتی ویروس به صورت خودکار بروزرسانی می‌شود. اگر چه به صورت پیش فرض این گزینه خاموش است، اما مؤکداً پیشنهاد می شود این گزینه را روشن نمایید تا سیستم شما آخرین ویروس‌های منتشر شده را شناسایی نماید.

گزینه‌هایی که علامت چرخدنده (⚙) دارند، تنظیمات بیشتری بر روی آنها قابل اعمال است. برای باز شدن صفحه تنظیمات بر روی عنوان گزینه (Automatic Update) کلیک کنید.



Show update notification window: در صورت فعال بودن، پس از بروزرسانی، پیغام دریافت موفق آپدیت به کاربر نشان داده خواهد شد.

Download from Internet: انتخاب این گزینه، آپدیت‌ها را از اینترنت دریافت خواهد کرد.

Pick update files from the specified path: در صورتی که مایلید بروزرسانی به صورت آنلاین صورت نپذیرد، می‌توانید یک مسیر آفلاین برای آپدیت‌های خود تعیین نمایید، (مثلا یک فولدر به اشتراک گذاشته شده شبکه) (و یا یک مسیر محلی و آفلاین که آپدیت‌ها را از رایانه دیگر دانلود و به صورت دستی به این مسیر کپی می‌کنید) مسیر را *Browse* کرده و آن را انتخاب می‌کنید (مثل C:\QHUpdate).

Copy update files to specified location: می‌توانید فایل‌های آپدیت دانلود شده را در یک فولدر شبکه (\\192.168.0.1\qhupdate) و یا محلی (مثل C:\QHUpdate) ذخیره نمایید تا در صورت لزوم توسط افراد دیگر و یا در زمان نصب مجدد، دوباره استفاده شوند.

Check for the latest version of Quick Heal: در صورتی که این گزینه فعال باشد، کوییک‌هیل انتشار نسخه جدید نرم‌افزار را بررسی می‌کند (مثلا نسخه ۲۰۱۷). توجه نمایید که ارتقای نسخه در زمان فعال بودن لایسنس به صورت کاملا رایگان صورت می‌پذیرد.

Notify me when upgrade is available: در صورت انتشار نسخه جدید، نرم‌افزار به شما اطلاع‌رسانی می‌کند.

Automatically download the upgrade: اگر این گزینه فعال باشد، در زمان انتشار نسخه جدید نرم‌افزار، به صورت خودکار دانلود نسخه جدید صورت می‌پذیرد.

Save Change: تنظیمات انجام شده را ذخیره می‌کند.

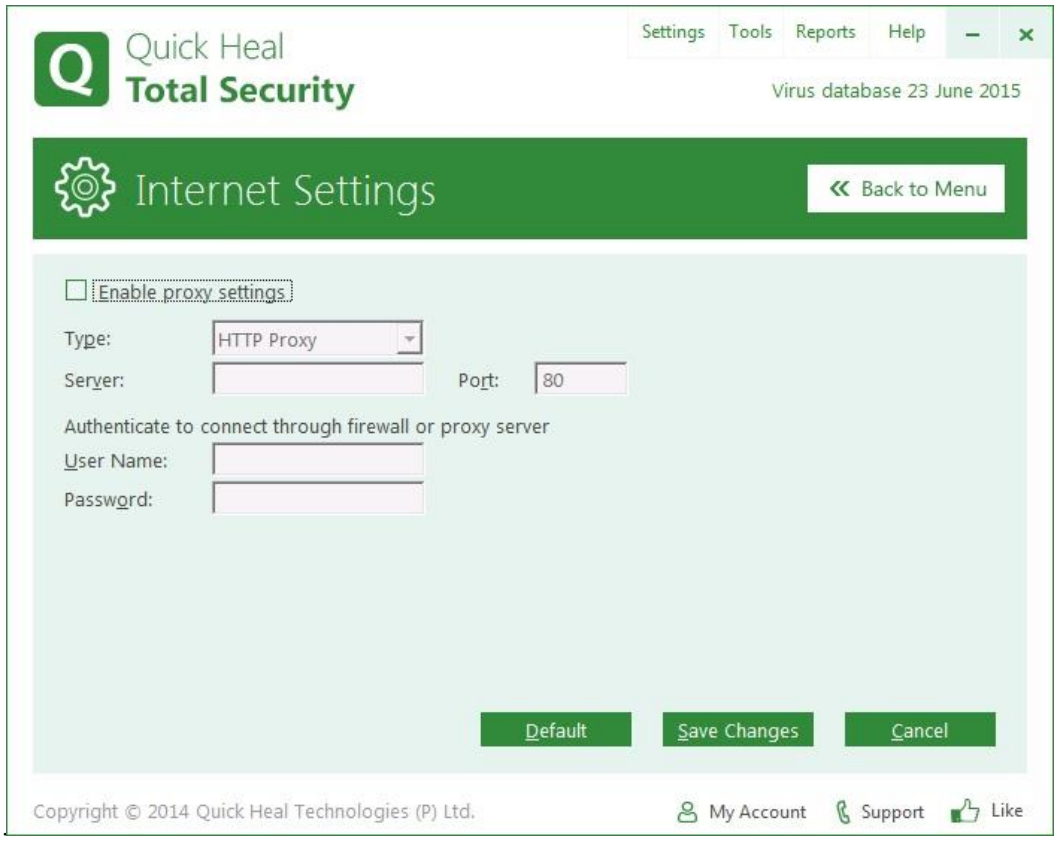
Cancel: تنظیمات انجام شده، ذخیره نشده و به صفحه قبل بر می‌گردد.

Default: تنظیمات صفحه، به تنظیمات پیش‌فرض نرم‌افزار بر می‌گردد.

Back to Menu: به صفحه قبلی (اصلی) بر می‌گردد.

ج) Internet Settings (تنظیمات اینترنت)

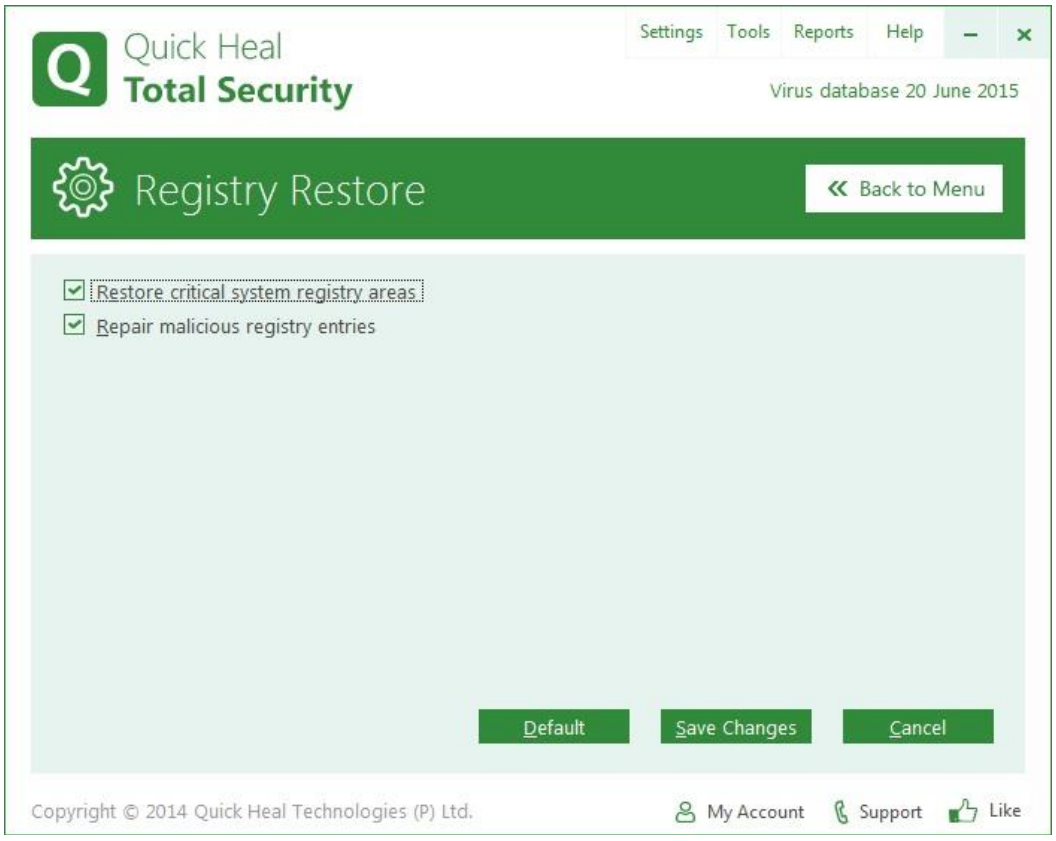
اگر رایانه شما از طریق پراکسی به اینترنت متصل می‌شود می‌توانید تنظیمات مربوط به سرور پراکسی را در این بخش وارد نمایید تا ارتباط آنتی‌ویروس با سرور کوییک‌هیل برای دریافت آپدیت و یا دریافت اخبار فراهم گردد. (تنظیمات پراکسی در مرورگر اینترنت اکسپلورر IE > Tools > Internet Options > Connections > Lan Settings قابل مشاهده می‌باشد. سه نوع مختلف پراکسی شامل HTTP، SOCKS V4 و SOCKS V5 قابل اعمال می‌باشد.



د) Registry Restore(بازیابی رجیستری)

در صورتی که تنظیمات مهم و حیاتی رجیستری ویندوز شما توسط ویروس‌ها یا بدافزارها تغییر یابد، کوییک‌هیل آنها را به حالت اول بر می‌گرداند. همچنین رجیستری سیستم را تعمیر می‌کند.

توجه: رجیستری، پایگاه داده سیستمی ویندوز می‌باشد که اطلاعات مهم نرم‌افزاری و سخت افزاری سیستم عامل و برنامه ها در آن ذخیره می‌گردد.



تنظیمات بازیابی رجیستری شامل:

Restore critical system registry areas: مناطق حیاتی و مهم رجیستری که توسط بدافزارها تغییر می‌کند معمولاً برای اجرای خودکار یک کار، یا جلوگیری از شناسایی بدافزار یا دستکاری برخی برنامه‌های سیستمی مانند غیر فعال کردن Task manager یا ویرایشگر رجیستری (Registry Editor) ویندوز صورت می‌پذیرد. این گزینه اطلاعات مهم رجیستری ویندوز را به حالت اولیه بازنشانی می‌کند.

Repair malicious registry entries: با اسکن رجیستری، بخش‌های مربوط به بدافزار را یافته و آنها را تعمیر می‌کند.

هـ) Self Protection (محافظت از خود)

این ویژگی در صورت روشن بودن، از هرگونه تغییر در پوشه‌ها، فایل‌ها، مدخل‌های رجیستری، پروسس‌ها، سرویس‌ها، تنظیمات و پیکربندی آنتی‌ویروس کوییک‌هیل توسط بدافزارها محافظت می‌کند. توصیه می‌شود این گزینه فعال باشد.

توجه ۱: این ویژگی از سرویس پک ۲ به بالا و سیستم عامل ویندوز XP پشتیبانی می‌کند.

توجه ۲: قابلیت محافظت از پروسس مربوط به ویژگی Self-Protection تنها از سیستم عامل ویندوز Vista سرویس پک ۱ و سیستم‌عامل‌های جدیدتر پشتیبانی می‌کند.

و) Password Protection (محافظت رمزعبور)

با فعال کردن این گزینه شما می‌توانید یک رمز عبور برای آنتی‌ویروس خود تعیین نمایید تا از دسترسی افراد غیرمجاز به تنظیمات و پیکربندی آنتی‌ویروس جلوگیری نمایید. توصیه می‌شود این گزینه را فعال کنید.

با روشن کردن گزینه محافظت رمزعبور، صفحه ی زیر باز می‌شود:

با فعال کردن این گزینه شما می‌توانید یک رمزعبور برای آنتی‌ویروس خود تعیین نمایید تا از دسترسی افراد غیرمجاز به تنظیمات و پیکربندی آنتی‌ویروس و در نتیجه مخاطرات امنیتی ناشی از آن جلوگیری نمایید. توصیه می‌شود این گزینه را فعال کنید.

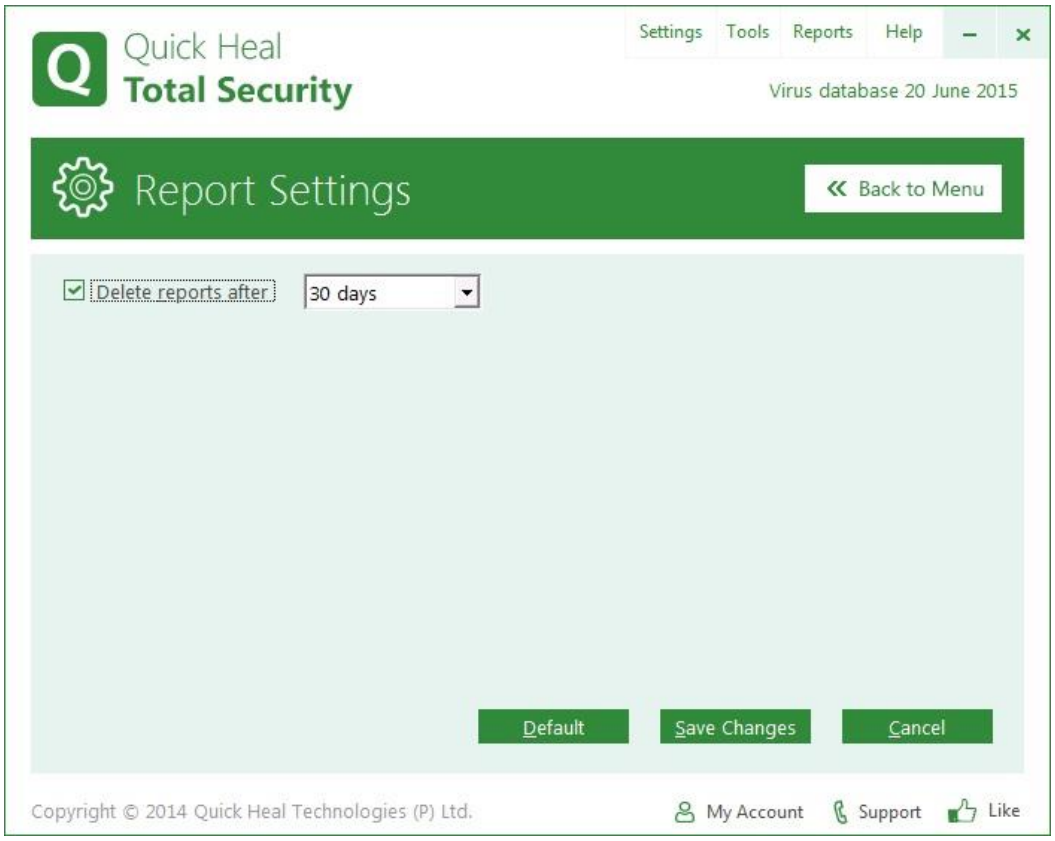
Enter password: رمزعبور مورد نظر خود را وارد نمایید. (حداقل ٦ کارکتر)

Confirm password: مجدداً همان رمزعبور را وارد نمایید.

Enable Safe Mode Protection: زمانی که به محیط Safe Mode ویندوز وارد می‌شوید (با فشردن F8)، تنها فایل‌ها و درایورهای ابتدایی ویندوز بارگذاری شده و ویژگی‌های امنیتی آنتی‌ویروس‌ها غیرفعال می‌باشد. برای جلوگیری از سرقت اطلاعات و یا دستکاری تنظیمات کوییک‌هیل در این حالت، ورود به این محیط را با یک رمزعبور محافظت می‌نمایید. اگر این گزینه فعال باشد، کاربر برای کار کردن در محیط Safe Mode حتما باید رمزعبور را داشته باشد.

ز) Report Settings (تنظیمات گزارش)

تنظیمات گزارش‌گیری کوییک هیل در این بخش قابل پیکربندی می باشد.



از همه فعالیت‌هایی که توسط آنتی‌ویروس کوییک‌هیل صورت می‌پذیرد، گزارش تولید می‌شود. مثلاً شما می‌توانید مشاهده نمایید که آیا سیستم شما به صورت کامل اسکن شده یا نه، اطلاعات ریز ویروس‌هایی توسط کوییک‌هیل شناسایی شده و یا سایت‌های آلوده‌ای که مسدود شده‌اند و شما قصد بازدید از آنها را داشتید. به صورت پیش فرض کلیه گزارش‌های تولیدی تا ۳۰ روز نگهداری شده و پس از آن حذف می‌شوند. اما شما می‌توانید مدت زمان را به ۱۰ یا ۹۰ روز تغییر داده و یا حذف خودکار گزارش‌ها را غیرفعال کنید.

ح) Report Virus Statistics (گزارش آمار ویروس)

این ویژگی آمار ویروس‌هایی که طی اسکن و ویروسیابی شناسایی شده‌اند را به لابراتوار کوییک‌هیل ارسال می‌کند. این اطلاعات تنها شامل آمار ویروس بوده و حاوی هیچ‌گونه اطلاعات کاربر نمی‌باشد.

ط) Remotely Manage Quick Heal (مدیریت از راه دور کوییک‌هیل)

کوییک‌هیل یک پورتال مبتنی بر فناوری ابری را به صورت رایگان در اختیار کاربران خود قرار می‌دهد. با استفاده از پورتال مدیریت از راه دور کوییک‌هیل شما می‌توانید یک یا چند محصول مختلف کوییک‌هیل (شامل نسخه‌های خانگی (توتال سکیوریتی، اینترنت سکیوریتی، آنتی‌ویروس پرو)، توتال سکیوریتی موبایل ویژه اندروید و تبلت سکیوریتی) را به این سامانه معرفی کرده و از راه دور به صورت متمرکز همه را یکجا مانیتور، مدیریت و کنترل نمایید. بسته به نوع محصول، امکاناتی که در اختیار مدیر سامانه مدیریتی قرار می‌گیرد متفاوت است. مثلاً در نسخه موبایل، امکان ردیابی موبایل، قفل کردن و یا حذف اطلاعات از راه دور در صورت سرقت، تنظیم انتقال تماس‌ها (در صورتی که گوشی را در مکانی دیگر جا گذاشته باشید)، دریافت گزارش‌های امنیتی و... مهیا می‌باشد. در نسخه‌های خانگی، امکاناتی نظیر، اطلاعات کلی از رایانه، وضعیت امنیتی، تاریخچه لایسنس و مدت اعتبار، تمدید و... ارائه می‌گردد.

برای اینکه بتوانید کوییک‌هیل خود را با استفاده سامانه تحت وب از راه دور مدیریت کنید، می‌بایست اجازه اینکار را با روشن کردن این گزینه بدهید. درصورتی که تمایل به استفاده از RDM کوییک‌هیل ندارید، می‌توانید این گزینه را غیرفعال کنید.

در صورتی که قبلاً هیچ محصولی را به RDM معرفی نکرده باشید، صفحه‌ی Add your Quick Heal product نمایش داده می‌شود. این صفحه راهنمایی لازم برای افزودن آنتی‌ویروس، به همراه آدرس اینترنتی پورتال مدیریتی ابزار راه دور کوییک هیل (RDM) را ارائه می دهد.

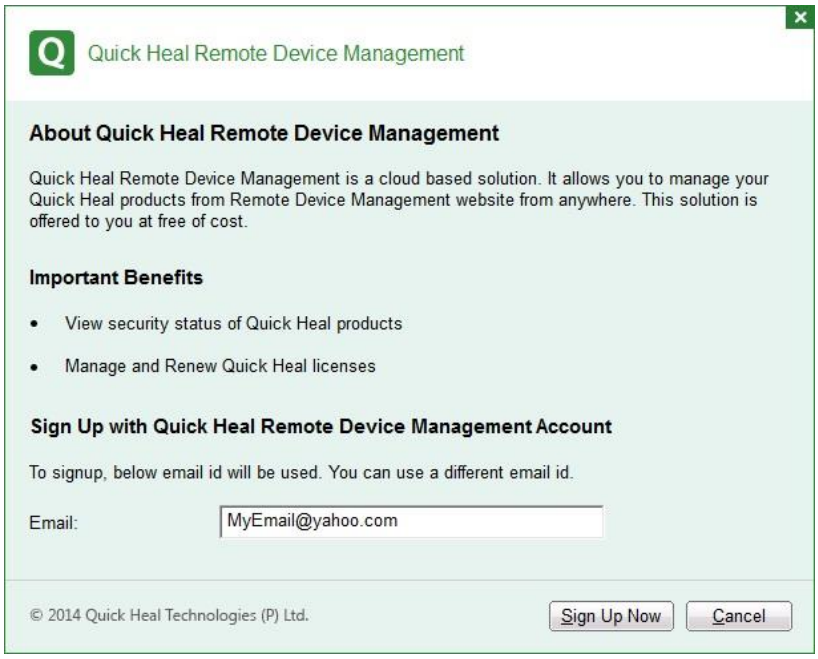
برای برخورداری از مزایای پورتال مدیریت راه دور کوییک هیل و استفاده از آن دو گام زیر ضروری است:

۱. **ایجاد حساب کاربری در پورتال وب RDM کوییک هیل**
۲. **افزودن دیوایس (محصول) به پورتال وب RDM کوییک هیل**

ایجاد حساب کاربری در پورتال وب RDM کوییک هیل

پیش از ساخت حساب کاربری RDM، می‌بایست آنتی‌ویروس خود را ثبت و فعال (Regsiter) کرده باشید. ایجاد یک حساب کاربری برای همه محصولات یک کاربر کافی است. مثلا اگر شخصی از آنتی‌ویروس کوییک‌هیل برای لپتاپ، رایانه شخصی، موبایل و تبلت استفاده می‌کند و می‌خواهد همه را به صورت متمرکز با یک حساب کاربری مدیریت نماید، کافی است یک حساب کاربری ایجاد کرده و محصولات مختلف را به آن بیفزاید.

پس از ثبت نام آنتی‌ویروس کوییک‌هیل، صفحه دعوت به ایجاد حساب کاربری RDM (sign up) ظاهر می‌شود. (در صورتی که این صفحه را مشاهده نکردید، با روشن کردن گزینه ***Remotely Manage*** از منوی ***Quick Heal*** ***Settings*** این صفحه نمایش داده خواهد شد.)



۱. به محض اینکه Quick Heal Total Security بر روی دستگاه شما ثبت شود، صفحه ایجاد حساب کاربری Quick Heal RDM نمایش داده می‌شود. برای دریافت دعوتنامه sign-up، آدرس صحیح ایمیل خود را وارد کرده، و بر روی Next کلیک کنید.

پس از آن، یک ایمیل حاوی راهنمای ایجاد حساب کاربری به آدرس ایمیل شما ارسال خواهد شد.

۲. ایمیل خود را باز کرده و بر روی دکمه *Activate* کلیک کنید. (و یا لینک داده شده را در مرورگر خود کپی کنید).

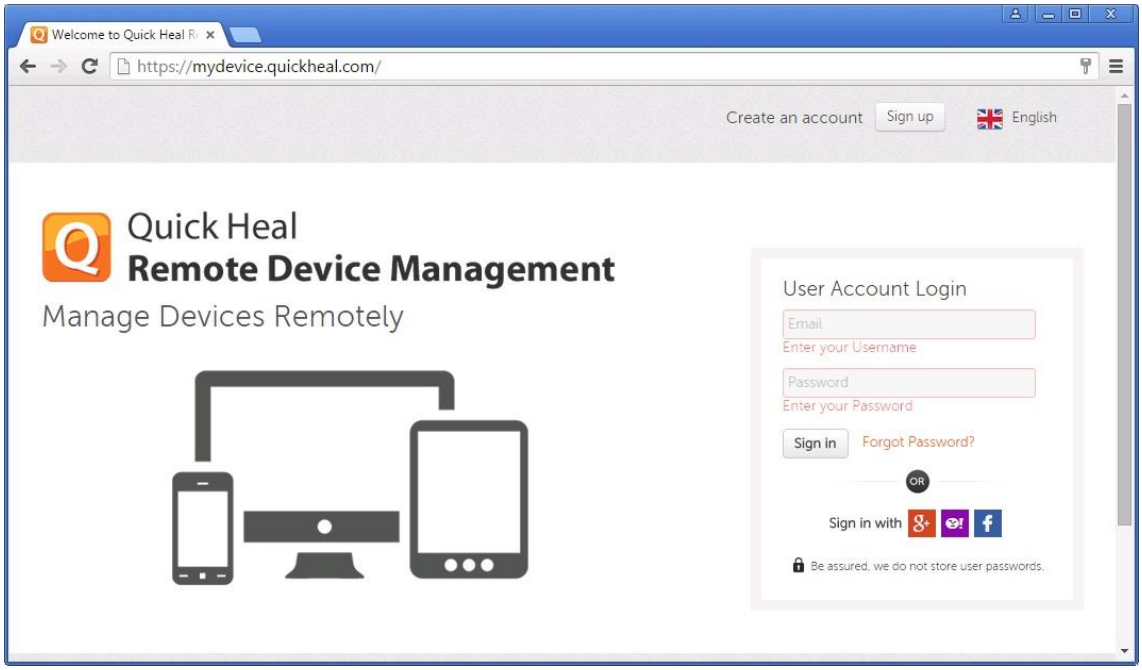
کلیک بر روی دکمه فوق شما را به صفحه تنظیم رمزعبور (Set Password) رهنمون می‌سازد.

۳. رمز عبور خود را وارد کرده و بر روی دکمه *Save* کلیک کنید.

هم اکنون حساب کاربری شما در پورتال RDM کوییک هیل با موفقیت ساخته شد. برای مدیریت دستگاه، ابتدا باید آنتی ویروس (device) خود را در پورتال RDM بیفزایید.

روش ۲: همچنین می‌توانید به صورت مستقیم با ورود به سایت پورتال مدیریت راه دور ابزار کوییک‌هیل اقدام به ایجاد حساب کاربری نمایید:

وارد سایت https://mydevice.quickheal.com شوید. بر روی دکمه Sign up کلیک کنید.



فرم نمایش داده شده را با اطلاعات درست تکمیل نمایید.

Username: ایمیل خود را وارد نمایید.

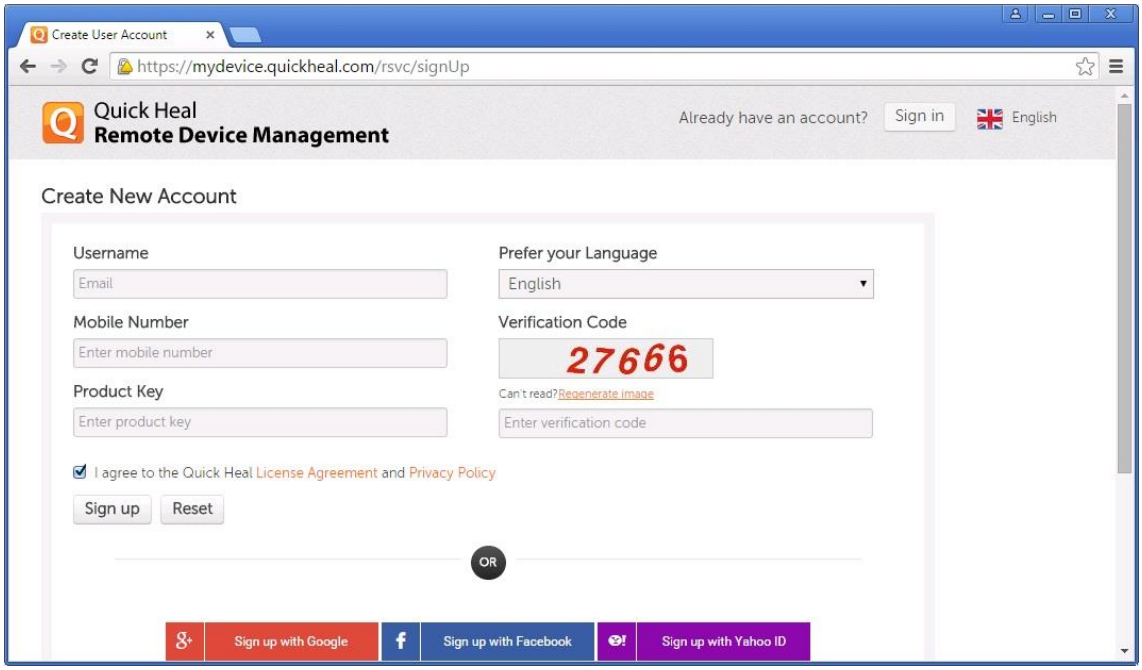
Mobile Number: شماره همراه خود را وارد نمایید. (مثلا 009891112345678)

Product Key: کلید محصول (لایسنس) خود را وارد نمایید. (در صورتی که از چند محصول کوییک‌هیل استفاده می‌کنید، کافی است لایسنس یکی از محصولات را وارد نمایید. پس از ایجاد حساب کاربری، همه محصولات خود را به پورتال می‌افزایید.)

Prefer your Language: زبان پیش‌فرض (English) انتخاب شده باشد.

Verification Code: کد امنیتی نمایش داده شده را دقیق وارد نمایید.

I agree to the Quick Heal License Agreement and Privacy Policy: گزینه قبول توافق‌نامه را تیک کرده و سپس بر روی دکمه Sign up کلیک کنید.



پس از تکمیل و ارسال فرم فوق، یک ایمیل حاوی راهنمایی برای فعالسازی ارسال خواهد شد. بر روی دکمه *Activate* کلیک کرده و در صفحه Set Password، رمز عبور مدنظر خود را وارد کرده و بر روی دکمه *Save* کلیک کنید.

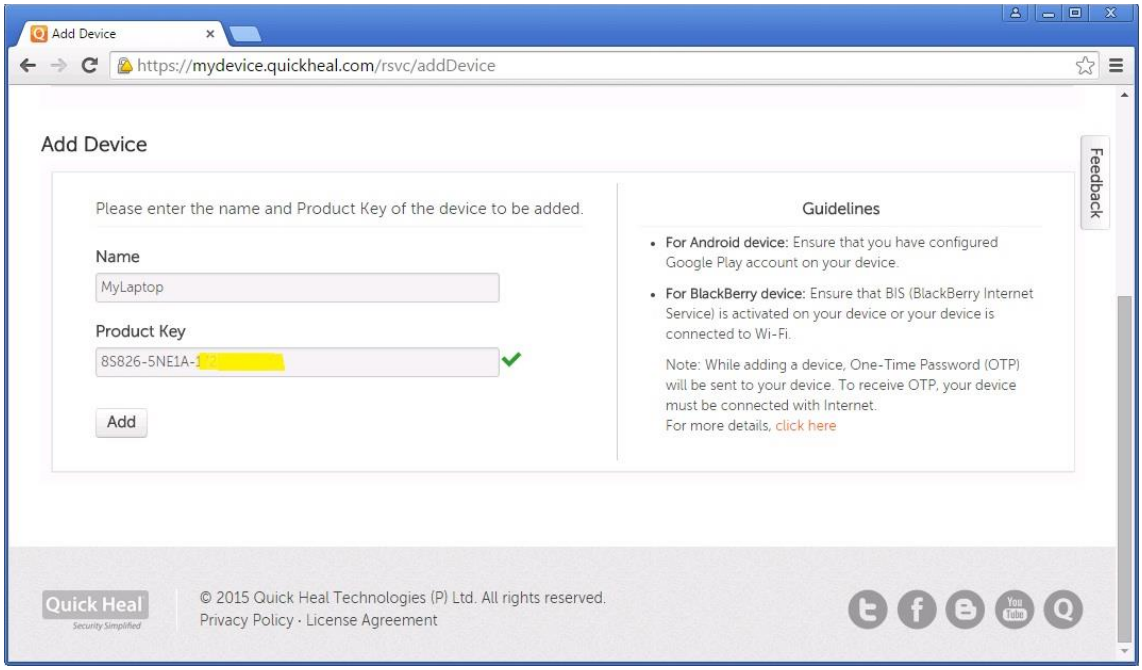
افزودن دیوایس (محصول) به پورتال وب RDM کوییک هیل

برای مدیریت از راه دور محصولات کوییک‌هیل پس از ایجاد حساب کاربری، می‌بایست آنها را به پورتال RDM کوییک هیل معرفی نمایید.

۱. وارد سایت https://mydevice.quickheal.com شوید.

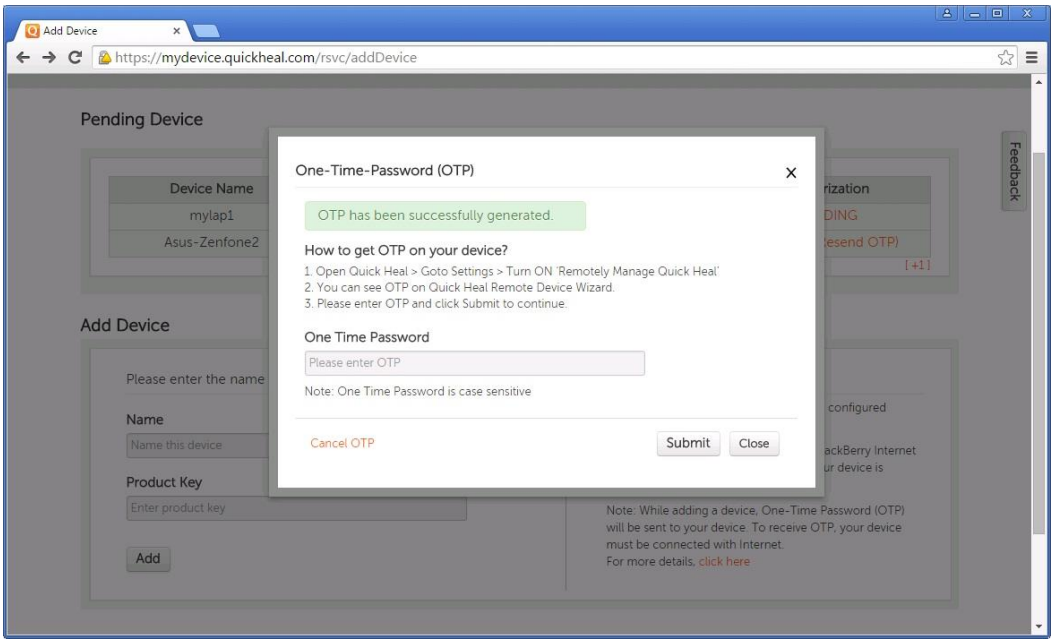
۲. . با وارد کردن ایمیل و رمز عبور وارد پورتال مدیریتی RDM شوید.

۳. نام دستگاه (مثلاً Laptop-Asus) و لایسنس محصول را وارد کنید.

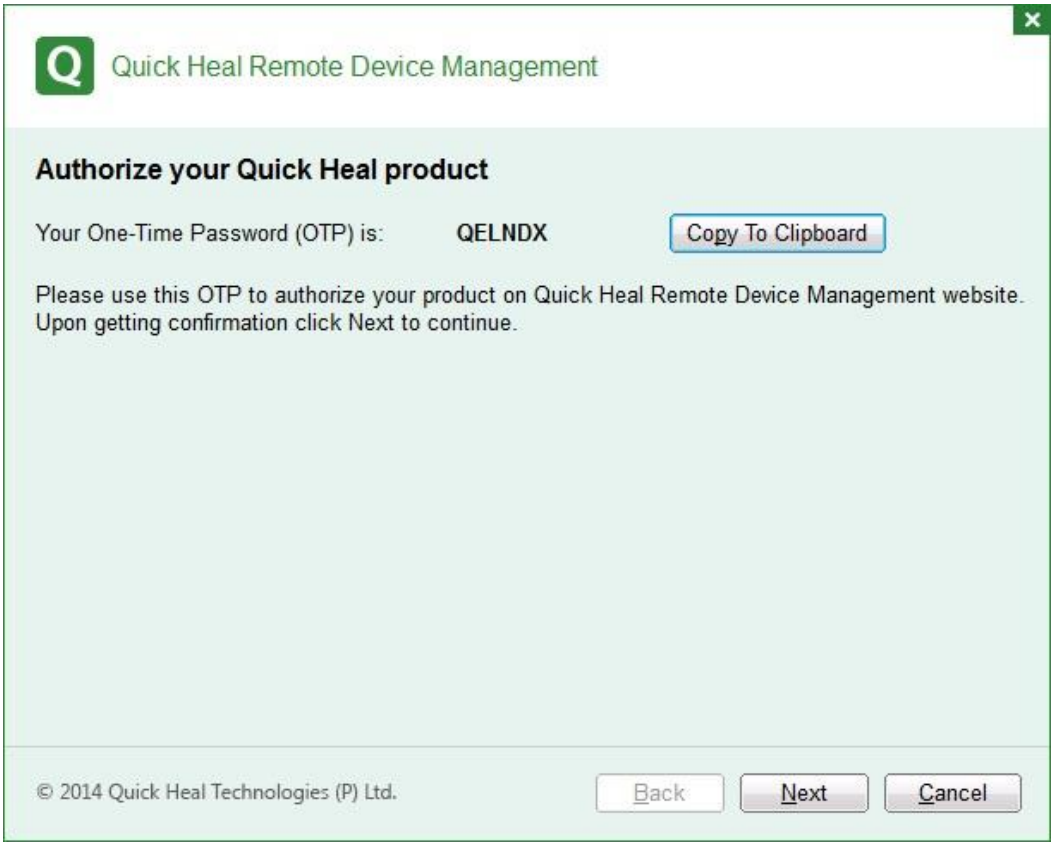


نام دیوایس را به صورت دلخواه وارد نمایید. در صورتی که فرایند ثبت نام RDM از طریق نرم‌افزار صورت پذیرد، کلید محصول به صورت خودکار تکمیل می‌گردد.

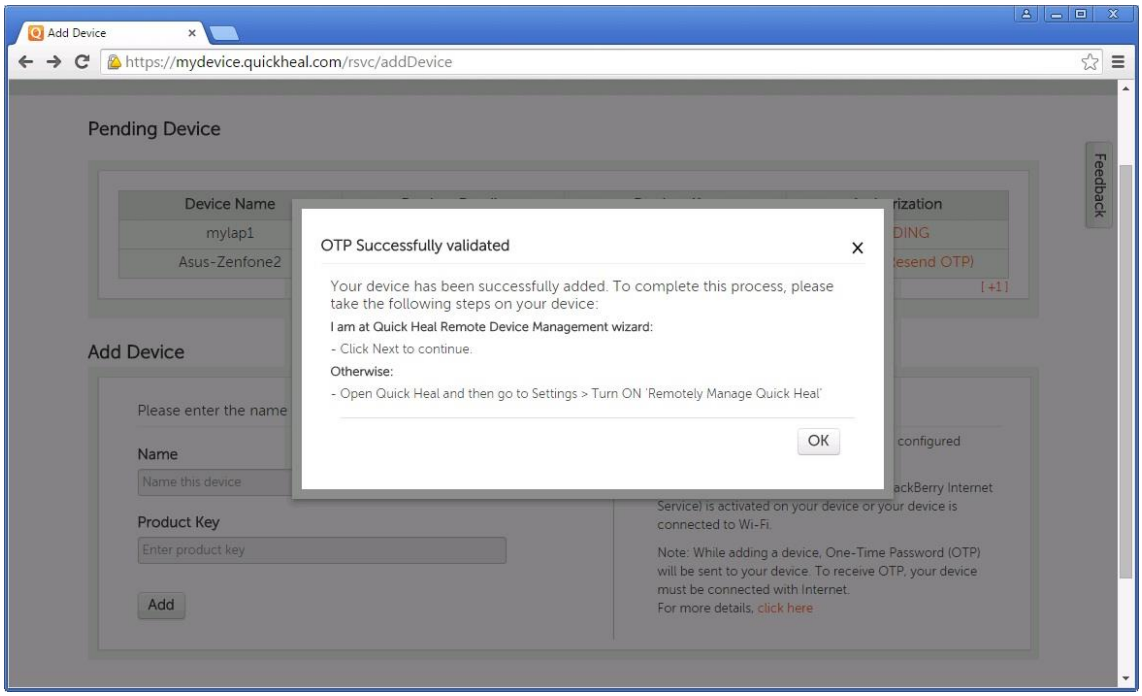
٤. بر روی دکمه *Add* کلیک کنید.



پس از آن رمز یکبار مصرف (One Time Password (OTP) تولید می‌شود. برای دریافت رمزعبور OTP، نرم‌افزار آنتی‌ویروس کوییک هیل نصب شده بر روی رایانه را اجرا و از منوی Settings، گزینه *Remotely Manage Quick Heal* را *ON* کنید.

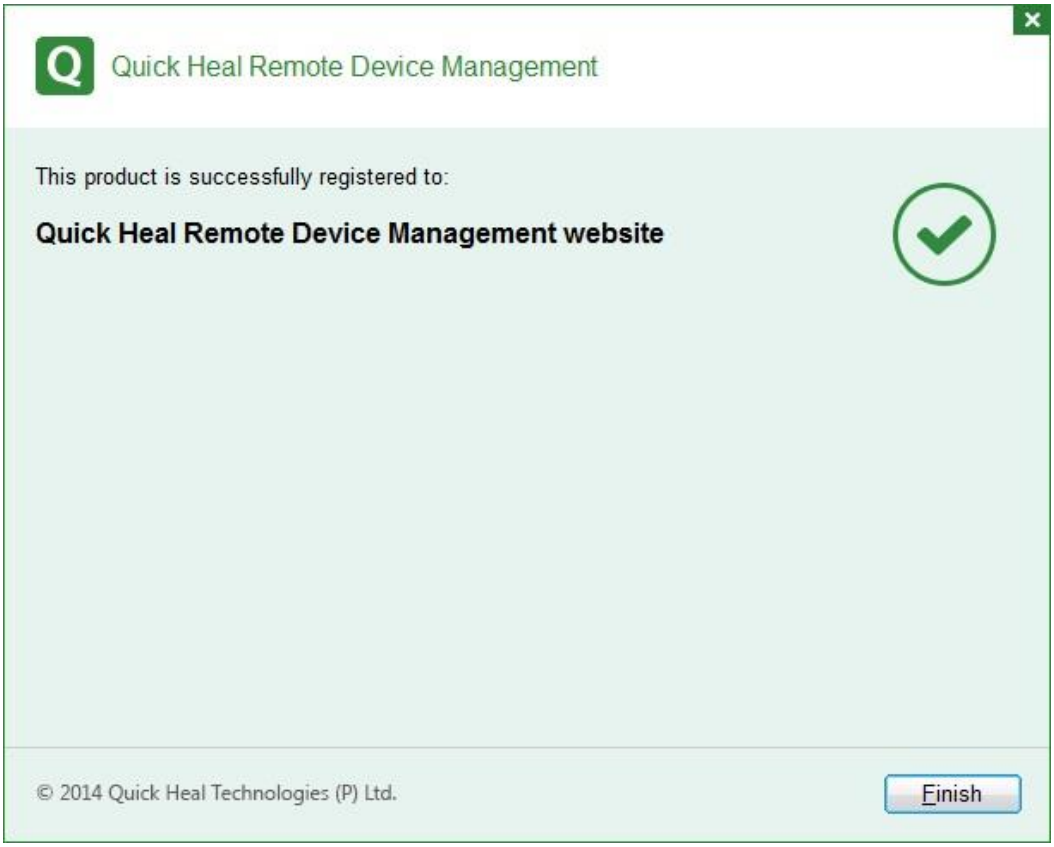


هم اکنون رمز عبور OTP نمایش داده خواهد شد.

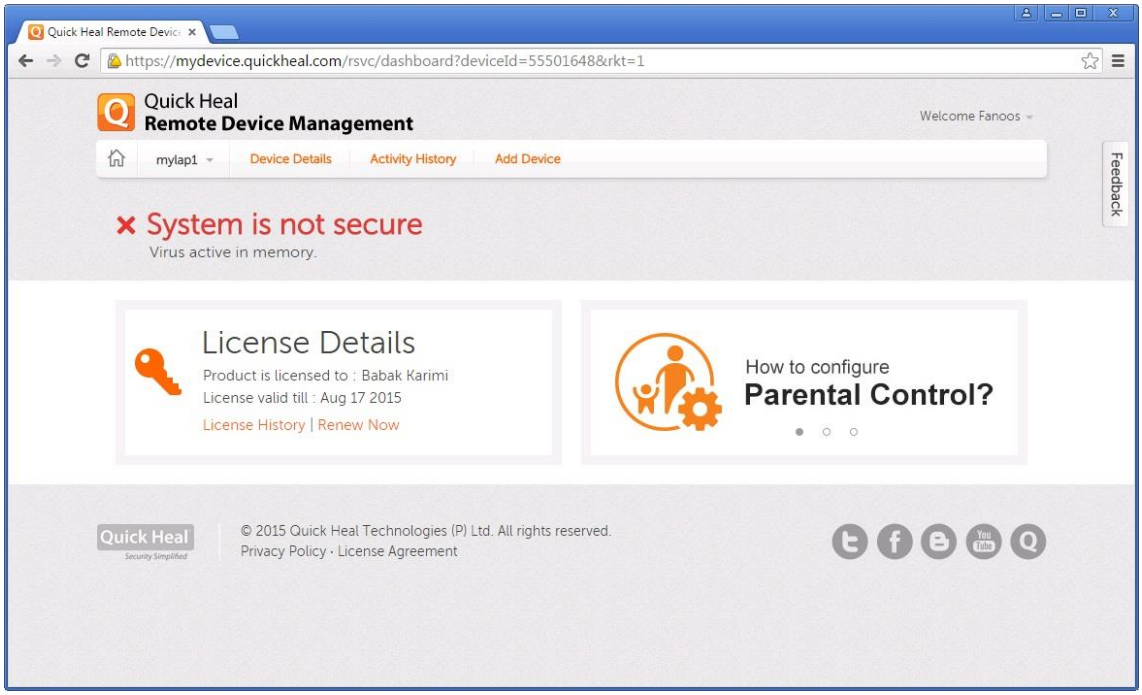


۵. رمز عبور یکبارمصرف (OTP) نمایش داده شده را وارد سایت پورتال RDM کرده و بر روی *Submit* کلیک کنید. محصول با موفقیت به پورتال افزوده شد.

٦. پس از تکمیل احراز اصالت در پورتال آنلاین، بر روی دکمه Next پنجره Quick Heal Remote Device Wizard موجود در رایانه کلیک کنید.



۷. سپس بر روی *Finish* کلیک کنید.

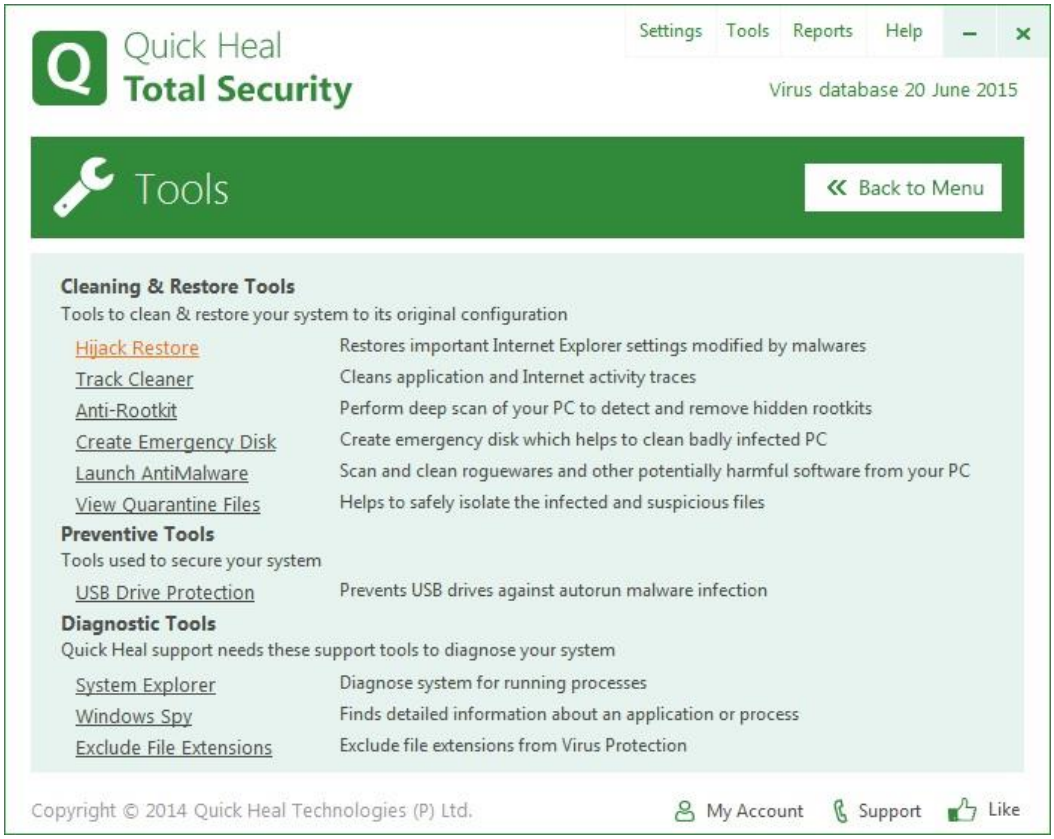


هم اکنون می‌توانید دستگاه (رایانه، موبایل، تبلت، ...) خود را با کلیک بر روی نام آن مدیریت، کنترل و گزارش‌گیری نمایید.

ی) Restore Default Settings (بازیابی تنظیمات پیش فرض)

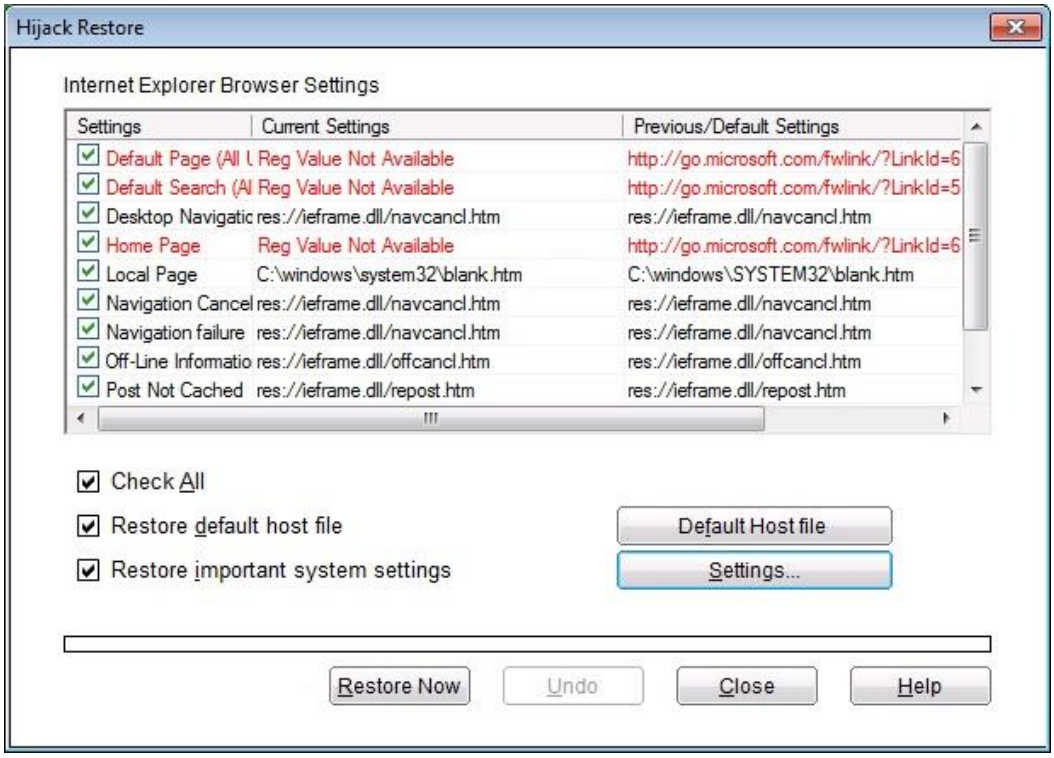
هنگامی که شما تنظیماتی را اعمال کردید، اما از سطح امنیت به وجود آمده راضی نیستید و یا احساس می‌کنید سطح محافظت در برابر تهدیدات کاهش یافته است، می‌توانید با استفاده از این گزینه کلیه تنظیمات را به حالت پیش فرض برگردانید.

منوی Tools



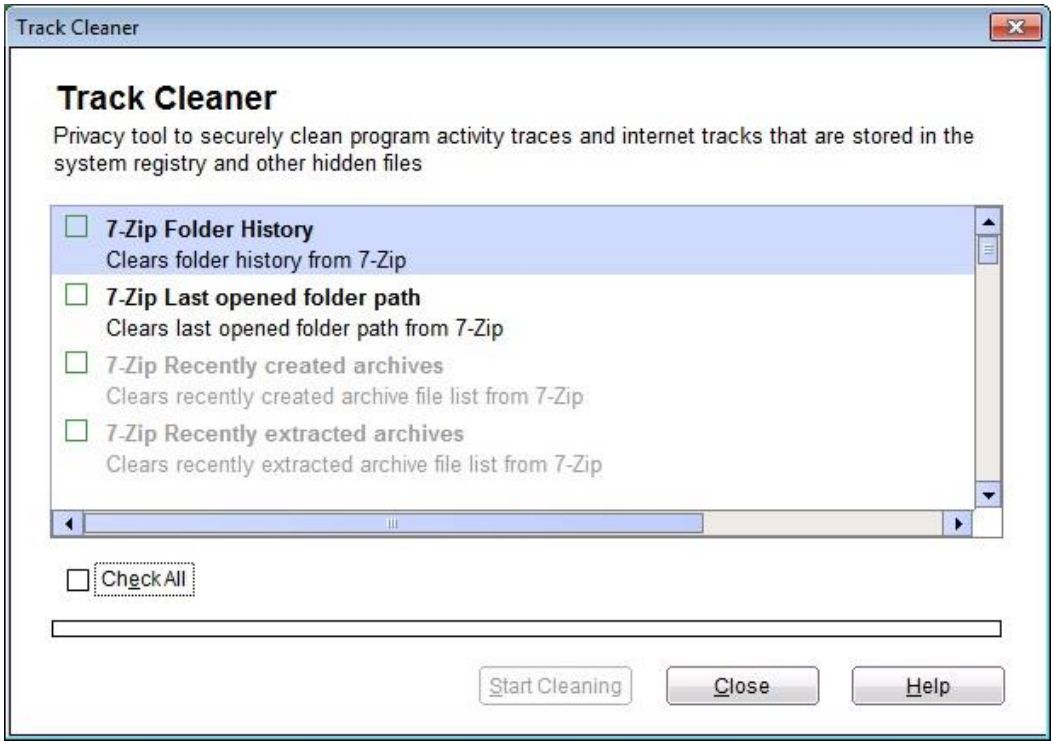
این ویژگی به شما کمک می‌کند تا اقدامات مختلفی نظیر پاکسازی و بازیابی تنظیمات سیستم به حالت اولیه، جلوگیری از دسترسی به درایوهای خاص و عیب‌یابی سیستم را به راحتی انجام دهید.

الف) Hijack Restore (بازیابی سرقت اطلاعات)



اگر تنظیمات پیش‌فرض مرورگر اینترنت اکسپلورر (Internet Explorer) تغییر یابد و یا تنظیمات به وسیله بدافزارها، جاسوس‌افزارها (جهت سرقت اطلاعات شما) و گاهی توسط برنامه‌های معتبر تغییر یابند، شما می‌توانید تنظیمات را به حالت پیش‌فرض برگردانید. این ویژگی، تنظیمات مرورگر IE، تنظیمات مهم سیستم عامل مانند ویرایشگر رجیستری و Task Manager را بازیابی می‌کند.

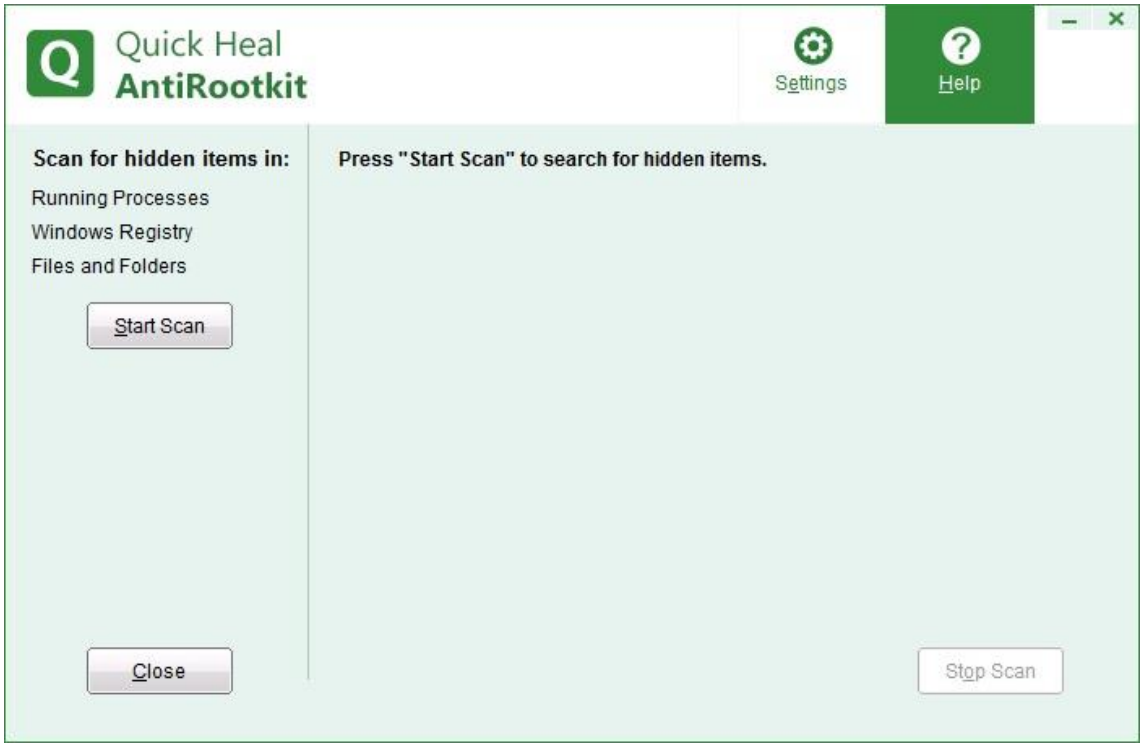
ب) Track Cleaner (پاکسازی آثار ردیابی)



بسیاری از برنامه‌ها یک لیست از آخرین فایل‌های بازشده (Most Recently Used) را به فرمت داخلی خود ذخیره می‌کنند تا کاربران در دفعات بعد با سرعت بیشتری بتوانند به آن فایل دسترسی یابند. اگر یک سیستم توسط بیش از یک نفر استفاده شود، ممکن است حریم خصوصی افراد در معرض خطر قرار گیرد. ویژگی Track Cleaner کوییک‌هیل کمک می‌کند تا کلیه آثار ردیابی مانند لیست فایل‌های استفاده شده اخیر (MRU) به طور کامل حذف گردند.

می‌توانید یکی از برنامه ها را انتخاب و یا با کلیک بر روی Check All همه برنامه‌ها را انتخاب نموده و بر روی *Start Cleaning* کیلک نمایید.

ج) Anti-Rootkit (آنتی روتکیت)



روتیکیت‌ها (Rootkit) برنامه‌های مخرب پیشرفته‌ای هستند که دسترسی سیستمی فراتر از Administrator به سیستم عامل ویندوز را در اختیار هکرها یا بدافزارها قرار می‌دهند.

این قابلیت، روتکیت‌هایی که در سیستم فعال هستند را شناسایی و پاکسازی می‌کند. این برنامه مواردی مانند پروسس‌های در حال اجرا، رجیستری ویندوز، فایل‌ها و پوشه‌ها را برای شناسایی هرگونه رفتار مشکوک اسکن کرده و روتکیت‌های بدون امضا(ناشناخته) را شناسایی می‌کند. آنتی روتکیت اکثر روتیک‌های موجود را شناسایی کرده، همچنین برای شناسایی روتیک‌های جدید و پاکسازی آنها طراحی شده است.

برای شروع اسکن بر روی دکمه *Start Scan* کلیک کنید.

توجه ۱: این تهدید تنها در نسخه‌های ۳۲ بیتی مایکروسافت ویندوز فعال بوده، در نتیجه Anti-Rootkit کوییک‌هیل نیز تنها در نسخه های ۳۲ بیتی اجرا می‌شود.

توجه ۲: استفاده از این انجین نیاز به دانش فنی مناسب از سیستم عامل داشته و یا با کمک مهندسین پشتیبانی کوییک‌هیل صورت پذیرد. استفاده نادرست از این برنامه ممکن است موجب ایجاد ناپایداری در سیستم گردد.

توجه ۳: پیش از اجرای آنتی روتکیت، کلیه برنامه‌های درحال اجرا را ببندید.

هـ) Creating Emergency Disk (ساخت دیسک اورژانسی)

ساخت دیسک بوت اورژانسی (Emergency)، امکان راه‌اندازی (بوت) مستقیم کامپیوتر و اسکن و پاکسازی تمامی درایوها از جمله پارتیشن NTFS را می‌دهد. این ابزار به شما کمک می‌کند تا آلودگی های شدید کامپیوتری که از داخل ویندوز قابل پاکسازی نیستند، در محیط Shell اختصاصی کوییک‌هیل ویروس‌زدایی گردند.

در مواقعی که کامپیوتر شما به شدت توسط ویروسی آلوده شده یا در مواقعی که به علت آلودگی شدید، امکان نصب آنتی‌ویروس وجود ندارد، دیسک اورژانسی می‌تواند ویروس‌های مقیم در حافظه را شناسایی و از بین ببرد. این ابزار، ویروس‌ها را از حافظه و دیگر نقاط حساس پاک می‌کند.

ساخت Emergency Disk

کوییک‌هیل قادر به ایجاد دیسک اورژانسی بر روی انواع سیستم‌عامل‌ها و نیز قابلیت ایجاد بوت با آخرین امضاهای آپدیت بر روی CD/DVD یا فلش/دیسک‌های USB می‌باشد.

۱- برای ساخت دیسک اورژانسی نیاز به بسته‌ی ساخت دیسک اورژانسی می‌باشد که می‌توانید با توجه به نوع سیستم‌عامتان (سیستم عاملی که دیسک را بر روی آن می‌سازید نه سیستم عاملی که می‌خواهید دیسک را برروی آن استفاده کنید) از مسیر زیر دریافت نمایید:

برای سیستم عامل ۳۲ بیتی لطفاً این بسته را دریافت کنید:

http://42722.ir/downloads/tools/emg/emgpkg32.zip

برای سیستم عامل ٦٤ بیتی لطفاً این بسته را دریافت کنید:

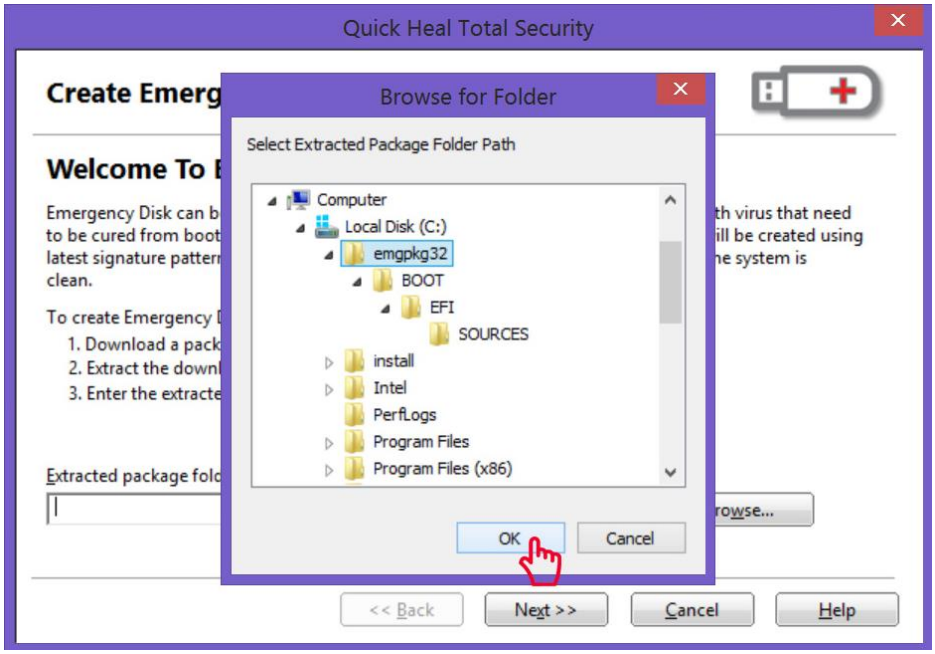
http://42722.ir/downloads/tools/emg/emgpkg64.zip

۲- هنگامی که دانلود بسته به پایان رسید آنرا در یک پوشه استخراج کنید برای مثال C:\qhemgpkg. توصیه می‌کنیم هنگامی که دیسک بوتیبل اورژانسی را ساختید (CD یا DVD یا دیسک USB) این پوشه را پاک نکنید. زیرا این پوشه در آینده در ساخت دیسک بوتیبل اورژانسی بعدی با آخرین به‌روزرسانی استفاده می‌شود.

۳- آدرس پوشه استخراج شده را در ویزارد «Create Emergency Disk» بدهید و طبق دستورالعمل ویزارد پیش روید.

نحوه ساخت دیسک اورژانسی به صورت تصویری شرح داده شده است:

با استفاده از دکمه *Browse...* مسیر پوشه بسته دیسک امرجنسی که از سایت کوییک هیل دانلود و از حالت zip استخراج شده را انتخاب می‌کنیم (مثلا C:\qhemgpkg):

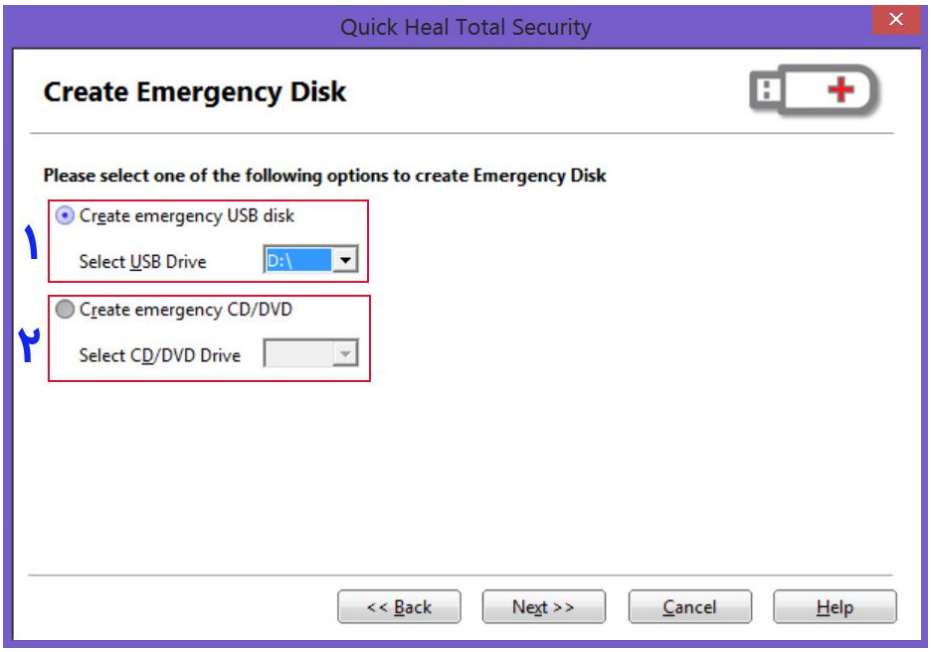

Quick Heal Total Security
Create Emerg
Welcome To E
Emergency Disk can b
to be cured from boot
latest signature pattern
clean.
To create Emergency D
1. Download a pack
2. Extract the down
3. Enter the extracte
Extracted package fold
Browse...
Browse for Folder
Select Extracted Package Folder Path
Computer
Local Disk (C:)
emgpkg32
BOOT
EFI
SOURCES
install
Intel
PerfLogs
Program Files
Program Files (x86)
OK
Cancel
<< Back
Next >>
Cancel
Help


Quick Heal Total Security
Create Emergency Disk
Welcome To Emergency Disk Creation Wizard
Emergency Disk can be used in emergency situation where your system is infected with virus that need to be cured from boot shell. If your AntiVirus is up to date then the Emergency Disk will be created using latest signature pattern files. Before creating the Emergency Disk, please ensure that the system is clean.
To create Emergency Disk please follow the steps below.
1. Download a package from http://www.quickheal.com/emgtool
2. Extract the downloaded package on your system.
3. Enter the extracted package folder path and click Next.
Extracted package folder path:
C:\emgpkg32
Browse...
<< Back
Next >>
Cancel
Help

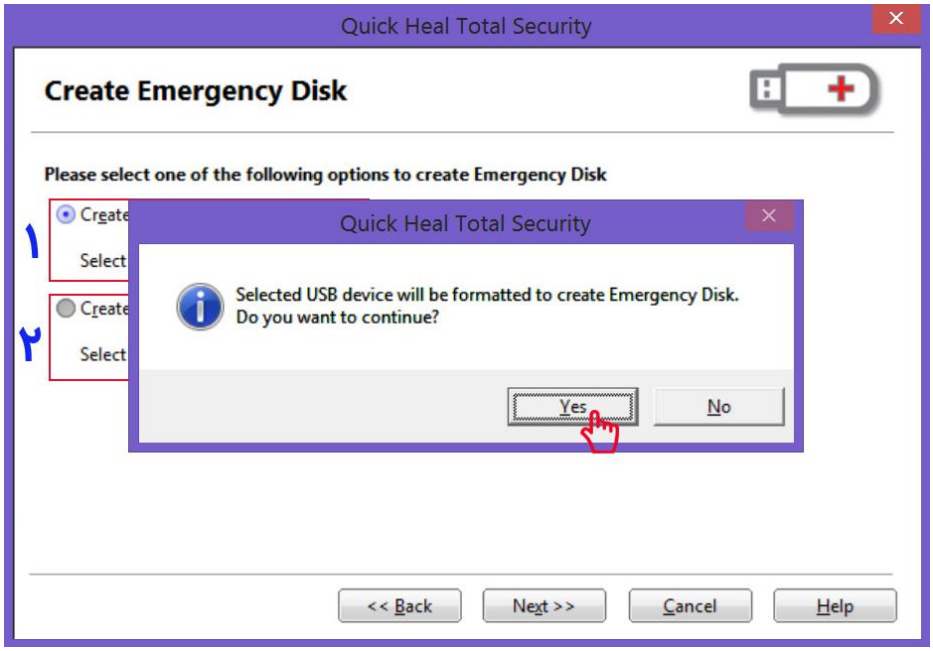
در این بخش می‌توانید نوع دیسک Flash USB یا CD/DVD را انتخاب کنید:

اگر می‌خواهید دیسک USB مانند فلش قابل راه‌اندازی بسازید گزینه (۱) را انتخاب و نام درایو فلش را مشخص کنید.

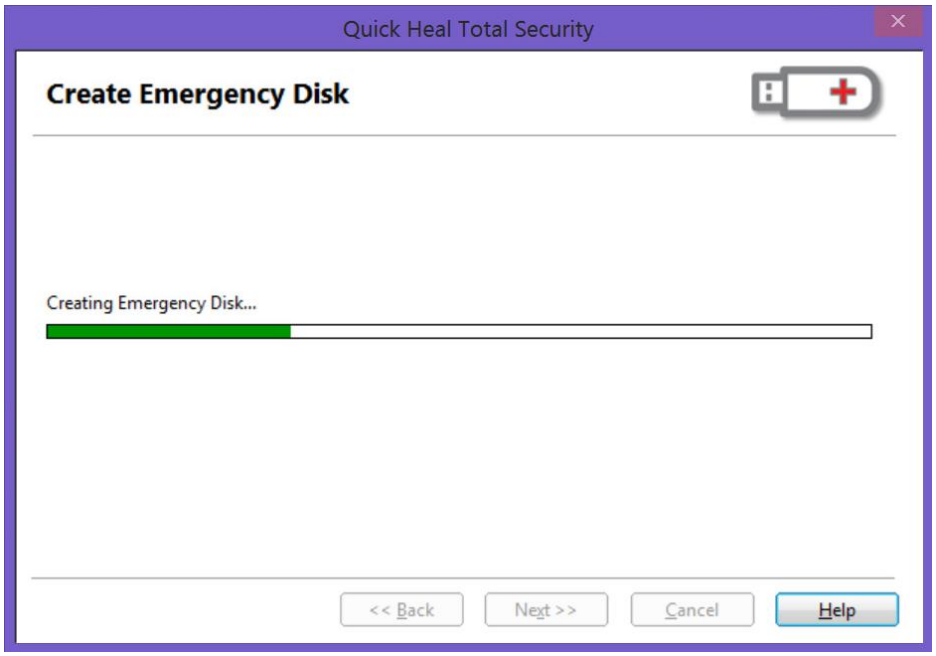
در صورتی که می‌خواهید CD/DVD قابل راه‌اندازی بسازید گزینه (۲) را انتخاب و نام درایو DVD/CD را مشخص کنید.



در صورت انتخاب گزینه USB Disk، فلش شما فرمت خواهد شد. در صورتی که از اطلاعات فلش پشتیبان تهیه کرده اید بر روی Yes و در صورتی انصراف از ادامه فرایند No را انتخاب کنید.



کوییک هیل شروع به ساخت دیسک اورژانسی می‌کند:



پس از پایان فرایند پنجره تکمیل موفقیت آمیز فرایند ساخت دیسک اورژانسی نمایش داده می‌شود. در این پنجره نسخه آنتی ویروس به همراه تاریخ پایگاه داده ویروس نمایش داده می شود:

نحوه استفاده از Emergency Disk:

۱. Emergency CD خود را در درایو CD-Rom/DVD-Rom قرار دهید.

۲. سیستم خود را Restart نمایید.

۳. در صورتی که اولویت اول بوت سیستم شما CD نیست، با فشردن دکمه *Delete* وارد Setup مادربورد شده در تنظیمات اولویت های Boot، اولین اولویت راه اندازی را CD-ROM انتخاب کنید.
٤. Emergency CD بطور خودکار شروع به کار کرده و شروع به اسکن همه درایوها می‌کند. در صورت پیدا کردن آلودگی در سیستم، آلودگی ها را پاکسازی می‌کند.
٥. بعد از یکبار اسکن، سی دی را از درایو خارج نمایید.
٦. سیستم خود را Restart نمایید تا ویندوز مجدداً بارگذاری گردد.

یادآوری:

برای ساختن دیسک بوتیبل بسته‌ی امرجنسی کوییک هیل بر روی CD یا DVD در سیستم عامل‌های XP و Server 2003 باید وصله‌ی Microsoft Imaging API نسخه ی ۲ را نصب نمایید.

برای مایکروسافت ویندوز XP نسخه ۳۲ بیتی:

http://42722.ir/downloads/tools/emg/WindowsXP-KB932716-v2-x86-ENU.exe

برای مایکروسافت ویندوز XP نسخه ٦٤ بیتی:

http://42722.ir/downloads/tools/emg/WindowsServer2003.WindowsXP-KB932716-v2-x64-ENU.exe

برای مایکروسافت ویندوز سرور ۲۰۰۳ نسخه ۳۲ بیتی:

http://42722.ir/downloads/tools/emg/WindowsServer2003-KB932716-v2-x86-ENU.exe

برای مایکروسافت ویندوز سرور ۲۰۰۳ نسخه ٦٤ بیتی:

http://42722.ir/downloads/tools/emg/WindowsServer2003.WindowsXP-KB932716-v2-x64-ENU.exe

اطلاعات کامل:

http://www.quickheal.co.ir/emgtool

و) AntiMalware(ضد بدافزار)

تفاوت عمده بدافزار (Malware) با ویروس (Virus) در نحوه تکثیر آنهاست. انتشار ویروس نیاز به فعالیت انسانی دارد (مثلاً دانلود ایمیل، اتصال فلش و...) اما بدافزار بدون دخالت انسان می‌تواند منتشر گردد.

موتور بهینه‌شده‌ی ضد-بدافزار کوییک‌هیل، رجیستری، فایل ها و پوشه‌ها را با سرعت فوق العاده زیاد اسکن کرده و انواع جاسوس‌افزار (Spywares)، تبلیغ افزار (Adwares)، آنتی‌ویرس‌های جعلی (Roguewares)، شماره‌گیرها (Dialers)، ریسک‌افزارها (Riskwares) و بسیاری دیگر از تهدیدات بالقوه موجود در سیستم شما را شناسایی و پاکسازی می‌کند.

با کلیک بر روی دکمه *Scan Now* فرایند اسکن آغاز می‌گردد. در طول اسکن، فایل‌ها، پوشه‌ها و مدخل‌های رجیستری آلوده شده توسط بدافزارها را نشان می‌دهد. پس از اتمام اسکن، شما می‌توانید همه یا تعدادی از یافته‌ها را پاکسازی نمایید.

پس از پایان اسکن در صورت یافتن بدافزار، گزینه‌های زیر در دسترس خواهد بود:

Clean: بدافزار و بقایای آن بر روی سیستم را پاکسازی می‌کند. اگر یک فایل، پوشه، یا مدخل رجیستری خاصی را پاک کنید، پیغامی به شما نشان می‌دهد که آیا می‌خواهید از اسکن‌های بعدی استثناء شود، اگر می‌خواهید به صورت دائمی از اسکن مستثنی شود *Yes* و اگر می‌خواهید به صورت موقت مستثنی شود *No* را کلیک کنید.

Skip: هیچ اقدامی بر روی بدافزار کشف شده، انجام نمی‌دهد.

Stop Scan: فرایند اسکن بدافزار را متوقف می‌کند.

Set System Restore point before cleaning: این گزینه کمک می‌کند پیش از پاکسازی بدافزارها توسط آنتی‌مالویر کوییک‌هیل، یک نقطه بازیابی سیستمی (Windows System Restore) در

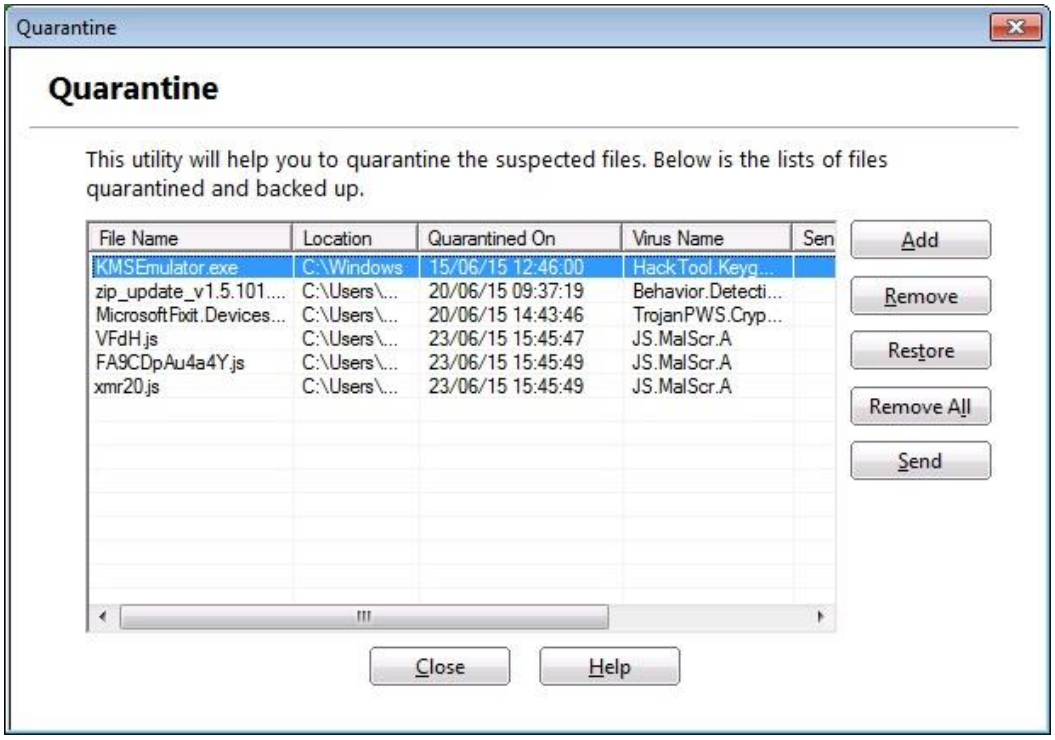
ویندوز ایجاد گردد. با کمک این ویژگی ویندوز می‌توانید در صورت نیاز، سیستم را به پیش از پاکسازی برگردانید.

Error Report Submission: شما را به سایت کوییک هیل رهنمون می‌سازد.

از طریق منوی Settings می‌توانید، فایل یا پوشه‌هایی را از اسکن استثناء کنید. همچنین می‌توانید اسکن آیتم‌های مشکوک را فعال/غیرفعال نمایید.

توجه۱: این ویژگی، با برنامه اصلی آنتی‌ویروس متفاوت است. برای رفع مشکلات ویروسی، از آنتی‌ویروس استفاده کنید.

ز) View Quarantine Files (نمایش فایل‌های قرنطینه)



یکی از ویژگی‌های مفید کوییک‌هیل، عدم حذف فایل‌های آلوده می‌باشد. با توجه به اینکه برخی فایل‌های آلوده (مثل کرک‌ها) ممکن است با وجود آلوده بودن موردنیاز کاربران باشد، کلیه فایل‌های آلوده یا مشکوک هنگام پاکسازی به صورت قرنطینه و ایزوله (رمز شده و غیرقابل اجرا) نگهداری می‌گردد. بنابراین کاربر می‌تواند در صورت نیاز آنها را بازیابی نماید.

زمانی که یک فایل قرنطینه می‌شود، کوییک‌هیل آن فایل را رمز کرده و در پوشه Quarantine کوییک‌هیل نگهداری می‌کند. نگهداری فایل‌ها با فرمت رمز شده موجب می‌شود آنها نتوانند اجرا شوند و در نتیجه امن باقی خواهند ماند. قرنطینه همچنین پیش از تعمیر فایل، یک کپی از آنها تهیه می‌کند. اگرچه شما نیز می‌توانید پیش از انجام هرگونه اقدام، یک کپی از فایل‌ها تهیه نمایید.

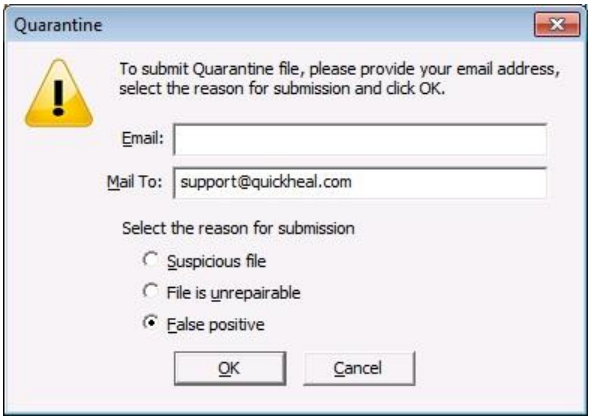
Add: می‌توانید یک فایل را به صورت دستی قرنطینه (رمز) نمایید.

Remove: می‌توانید یک فایل قرنطینه شده را حذف نمایید. (فایل‌های حذف شده غیرقابل بازگشت می‌باشند)

Restore: یک فایل قرنطینه شده را به مکان اولیه آن بازگردانید. (فایل رمزگشایی می‌شود)

Remove All: می‌توانید همه فایل‌های قرنطینه شده را حذف نمایید. (فایل‌های حذف شده غیرقابل بازگشت می‌باشند)

Send: می‌توانید فایل قرنطینه شده را جهت آنالیز بیشتر به آزمایشگاه ویروس‌شناسی کوییک‌هیل ارسال نمایید. فایلی را که می‌خواهید ارسال کنید، انتخاب کرده و ***Send*** را کلیک کنید.



پس از کلیک بر روی Send فرمی نمایش داده می‌شود که ایمیل خود را در فیلد Email و دلیل ارسال را مشخص می‌کنید:

Suspicious File: در صورتی که احساس می‌کنید که این فایل فعالیت‌های مشکوک در سیستم شما انجام می‌دهد.

File is un-repairable: در صورتی که Quick Heal در طی اسکن سیستم می‌تواند فایل آلوده را شناسایی کند اما قادر به پاکسازی آن نیست.

False positive: اگر فایل حاوی داده‌های غیرمخرب بوده و شما از کارکرد و عملکرد آن آگاهی کامل دارید، اما کوییک‌هیل آن را به عنوان فایل مشکوک شناسایی می‌کند.

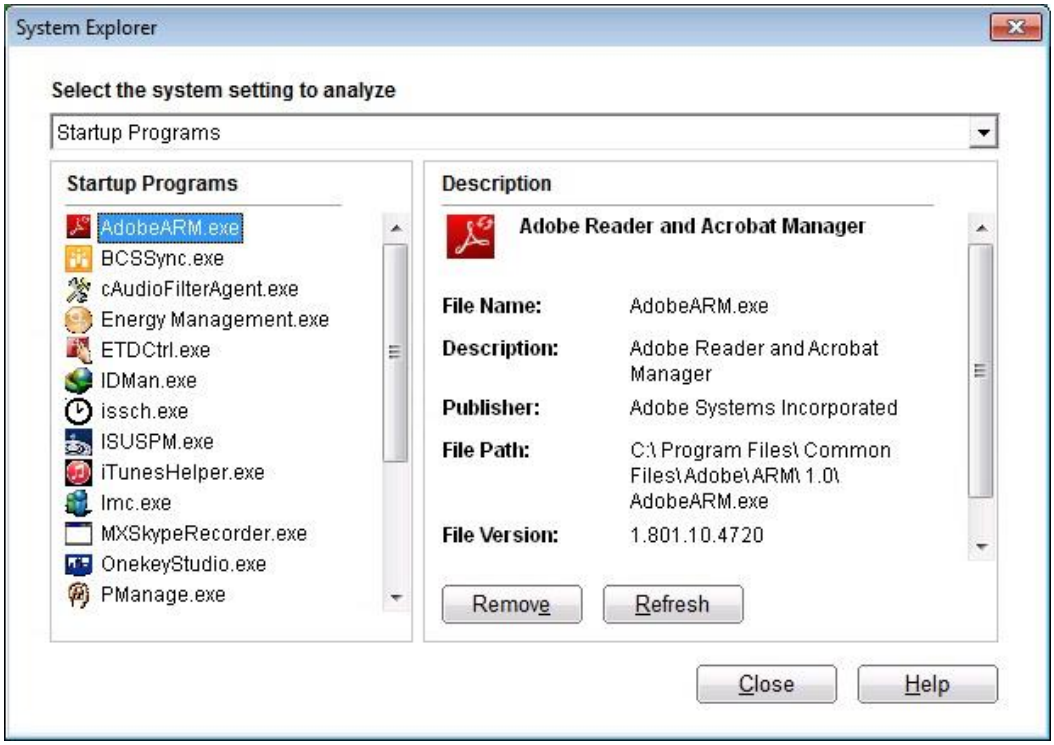
ح) USB Drive Protection (محافظت از درایوهای USB)

هنگامی که درایوهای خارجی (مانند فلش، Ram Reader، حافظه‌های خارجی، هارد دیسک اکسترنال و...) را به سیستم خود متصل می‌کنید، ویژگی آتوران یا اجرای خوکار (autorun) به صورت اتوماتیک اجرا شده و ممکن است تمامی برنامه‌های موجود در درایو خارجی اجرا شوند. همچنین ممکن است بدافزار autorun در داخل درایو USB قرار داشته باشد و به محض اتصال درایو به رایانه، اجرا شده و آلودگی را به سیستم شما گسترش دهد. این ویژگی به شما کمک می‌کند تا از ابزارهای USB خود در برابر بدافزار آتوران محافظت کنید.

برای امن سازی درایوهای USB، ابتدا آن را به سیستم متصل کرده، سپس از منوی بازشونده نام درایو خارجی را انتخاب و بر روی دکمه *Secure Removable Drive* کلیک کنید. پس از امن کردن درایو، این درایو USB (مثلاً فلش) حتی در سیستم های دیگر نیز در برابر ویروس آتوران محافظت شده باقی می‌ماند.

توجه: کوییک‌هیل توصیه می‌کند که درایو فلش را امن شده حفظ کنید، اما اگر می‌خواهید این ویژگی را غیرفعال کنید می‌توانید از همین منو استفاده کنید.

ط) System Explorer(مرورگر سیستمی)



با استفاده از این ابزار می‌توانید اطلاعات مهمی از رایانه خود دریافت نموده تا در مواقع ضروری (نفوذ یک بدافزار یا ریسک‌افزار جدید) برای عیب‌یابی سیستم استفاده نمایید.

این اطلاعات شامل موارد زیر می‌باشد:

اطلاعات کاملی از پروسس‌های در حال اجرا، BHOهای نصب شده (پلاگین‌های IE)، نوار ابزارهای نصب شده در Internet Explorer، ActiveXهای نصب شده، Hostها، LSPها، برنامه‌های Startup، تنظیمات IE و اتصال‌های فعال شبکه.

ی) Windows Spy (جاسوس پنجره‌ها)

با استفاده از این ویژگی می‌توانید اطلاعات بیشتری درباره یک برنامه یا پروسس دریافت نمایید. گاهی اوقات دائماً یک پنجره (فرم) یا پیام نمایش داده می‌شود که در واقع توسط جاسوس‌افزار یا بدافزاری نمایش داده می‌شود، اما ما قادر نیستیم مکان آن را پیدا کنیم. در چنین مواردی این ابزار می‌تواند مفید باشد، با کلیک بر روی آیکن (بالا سمت راست) و نگه داشتن کلیک ماوس و کشیدن آیکن نشانه و رها کردن بر روی پنجره مشکوک می‌توانید اطلاعات کاملی در رابطه با برنامه دریافت کنید. (Drag & Drop کردن آیکن نشانه بر روی پنجره مشکوک)

اطلاعات شامل موارد زیر می‌باشد:

Application Name: نام برنامه

Original File Name: نام اصلی فایل

Company Name: نام شرکت سازنده نرم‌افزار

File Description: توضیحات فایل

File Version: نسخه فایل

Internal Name: نام داخلی

Product Name: نام محصول

Product Version: نسخه محصول

Copyrights Information: اطلاعات کپی‌رایت

Comments: توضیحات

اگر می‌خواهید برنامه یا پنجره را ببندید، می توانید بر روی Kill Process کلیک کنید.

ی) Exclude File Extensions(مستثنی کردن پسوند فایل)

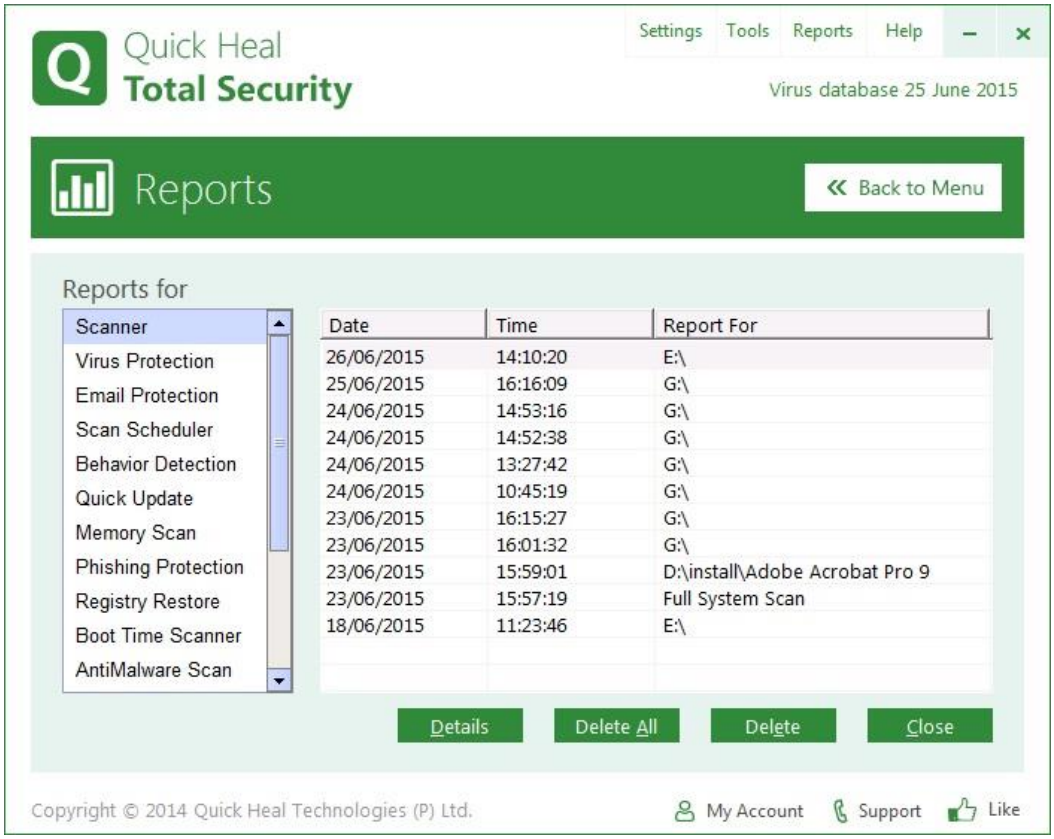
شما می‌توانید لیستی از نوع یا پسوندهای فایل تهیه نمایید تا محافظت ویروس (Virus Protection)، آن نوع از فایل‌ها را اسکن نکند. این ویژگی کمک می‌کند تا محافظت ویروس، بر روی آن دسته از فایل‌هایی که گرایش به رفتارهای مشکوک دارند تمرکز کند.

برای استثناء کردن یک نوع فایل از اسکن، پسوند را وارد کرده و بر روی *Add* کلیک کنید. (مثلا dat)

اگر یک پسوند را به اشتباه وارد کردید، جهت حذف از لیست استثناها پسوند مربوطه را انتخاب و بر روی *Remove* کلیک کنید.

در انتها بر روی *OK* کلیک کنید تا تغییرات ذخیره شود.

منوی Reports



آنتی‌ویروس کوییک‌هیل گزارش کاملی از همه فعالیت‌های مهم مانند اسکن ویروس، جزئیات بروزرسانی، تغییر در تنظیمات ویژگی‌ها و غیره ایجاد و نگهداری می‌کند.

گزارش‌ها بر اساس ویژگی‌های زیر کوییک‌هیل توتال سکیوریتی قابل مشاهده می‌باشند:

Scanner: در صورت اسکن و ویروسیابی گزارشی از آن در این بخش قابل مشاهده است.

Virus Protection: گزارشی از محافظت از ویروس که به صورت خودکار محافظت از سیستم را برعهده دارد. به محض دسترسی به فایل یا پوشه به صورت پیشگیرانه محافظت صورت می‌پذیرد.

Email Protection: گزارش محافظت ایمیل

Scan Scheduler: گزارش اسکن‌های زمانبندی (برنامه‌ریزی) شده

Behavior Detection: گزارش انجین مبتنی بر رفتارشناسایی و هوشمند کوییک‌هیل برای ویروس‌های ناشناخته و جدید.

Quick Update: گزارشی از جزئیات زمان، و تاریخ بروزرسانی‌های خودکار آنتی‌ویروس

Memory Scan: گزارشی از اسکن های حافظه (RAM) سیستم

Phishing Protection: گزارشی از مسدود شدن سایت‌های فیشینگ و کلاهبردارانه که محافظت پیشگیرانه از آن به عمل آمده است.

Registry Restore: گزارشی از بازیابی رجیستری ویندوز که توسط بدافزارها آلوده شده بود.

Boot Time Scanner: گزارشی از اسکن زمان بوت (راه‌اندازی)، که پیش از بارگذاری ویندوز، اقدام به اسکن و ویروسیابی آلودگی‌های شدید می‌کند.

AntiMalware Scanner: گزارشی از اسکن موتور ضد بدافزار کوییک هیل

Firewall Protection: گزارشی از تغییرات در تنظیمات و محافظت‌های صورت پذیرفته توسط فایروال

Parental Control: گزارش کاملی از ویژگی کنترل خانواده کوییک‌هیل (که دسترسی به اینترنت را برای کودکان محدود می‌سازد)

IDS & IPS: گزارشی از حفاظت های صورت پذیرفته توسط ماژول IDS&IPS کوییک‌هیل که به صورت هوشمند و آنالیز پکت‌های شبکه نفوذ غیرمجاز به سیستم را شناسایی و از آن جلوگیری می‌کند.

Browsing Protection: گزارشی از محافظت مرورگر که از ورود به سایت‌های آلوده جلوگیری می‌کند.

PC2Mobile Scan: گزارشی از اسکن گوشی‌های موبایل توسط رایانه.

Vulnerability Scan: گزارشی از اسکن آسیب‌پذیری و حفره‌های نرم‌افزاری موجود در سیستم.

در پنل سمت راست پنجره ی Reports، اطلاعات مربوط به گزارش نشان داده می شود. با کلیک بر روی هر یک از ردیف‌های گزارش و کلیک بر روی دکمه های انتهای صفحه، می‌توانید اقدامات زیر را بر روی آنها انجام دهید:

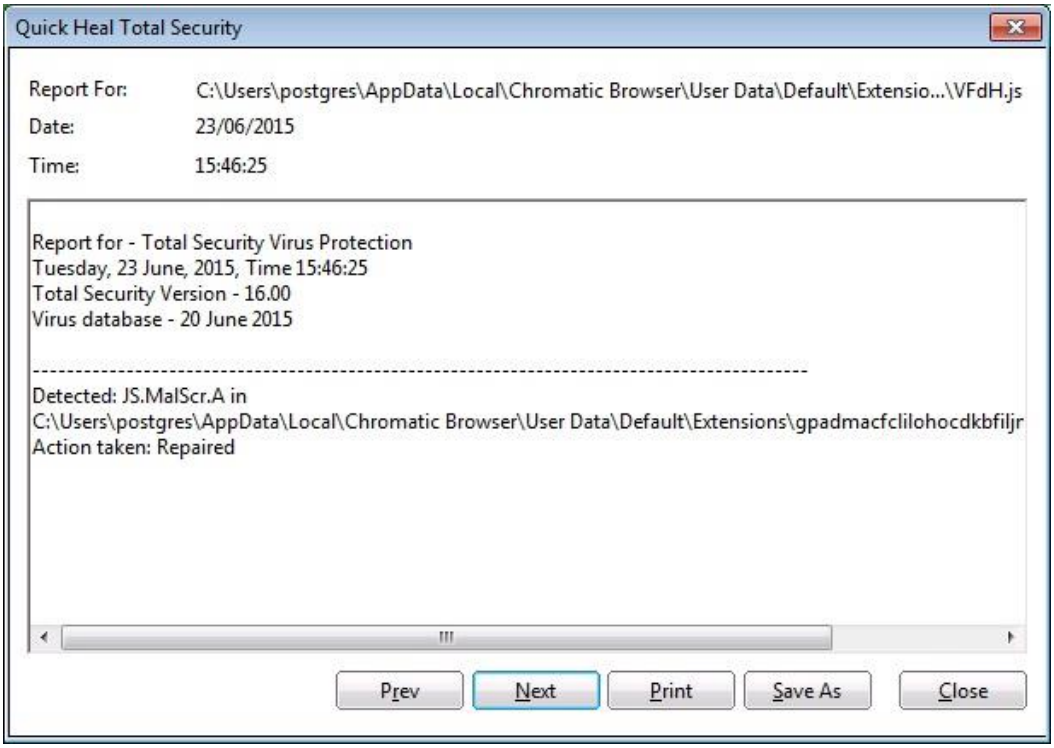
Details: جزئیات بیشتری از رکورد گزارش انتخاب شده در لیست ارائه می‌دهد.

Delete All: همه رکوردهای (ردیف‌های) گزارش را حذف می‌کند.

Delete: رکورد انتخاب شده گزارش را حذف می‌کند.

Close: صفحه گزارش را می‌بندد.

با کلیک بر روی *Details* یا دوبار کلیک بر روی هر ردیف از گزارش می‌توانید اطلاعات کامل‌تری از آن گزارش دریافت نمایید.



اقدامات قابل اجرا در صفحه جزئیات با دکمه‌هایی در انتهای صفحه قابل اجراست:

Prev: جزئیات گزارش رکورد (ردیف) قبلی را نمایش می‌دهد. (اگر رکورد انتخابی، اولین رکورد باشد، غیرفعال می‌گردد.)

Next: جزئیات گزارش رکورد بعدی را نمایش می‌دهد. (اگر رکورد انتخابی، آخرین رکورد باشد، غیرفعال می‌گردد.)

Print: می‌توانید جزئیات گزارش انتخابی را چاپ کنید.

Save As : جزئیات گزارش را به فرمت **.txt** بر روی رایانه شما ذخیره می‌کند.

Close: صفحه جزئیات گزارش را می‌بندد.

منوی Help

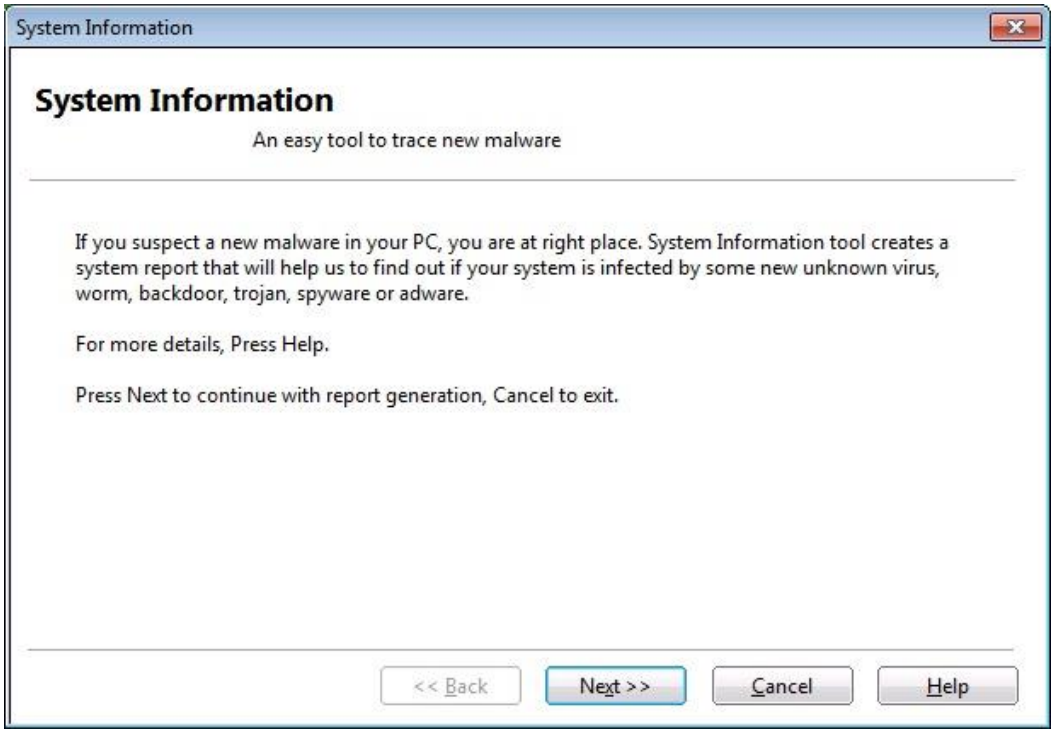
با استفاده از راهنمای کوییک‌هیل می‌توانید با نحوه استفاده و پیکربندی ویژگی‌های کوییک‌هیل توتال سکیوریتی، نحوه ارتباط با تیم پشتیبانی فنی کوییک‌هیل (شرکت فناوری ارتباطات و اطلاعات فانوس نماینده رسمی این شرکت در ایران)، نحوه بروزرسانی و جزئیات لایسنس محصول آشنا شوید.

الف) Help (راهنما)

آنتی‌ویروس کوییک‌هیل به شکلی طراحی شده است که نصب و استفاده از آن ساده باشد، اما اگر برای استفاده از امکانات پیشرفته‌تر کوییک‌هیل نیاز به راهنمایی بیشتری دارید، می‌توانید از منوی ***Help*** و زیرمنوی ***Help*** استفاده نمایید.

همچنین می‌توانید با فشردن کلید F1 صفحه کلید بر روی ماژول‌های مختلف برنامه، راهنما را فراخوانی کنید.

ب) Submit System Information (ارسال اطلاعات سیستمی)



ویژگی اطلاعات سیستمی کوییک‌هیل توتال سکیوریتی، یک ابزار ضروری برای جمع آوری اطلاعات مهم سیستمی مبتنی بر ویندوز می‌باشد. این ابزار تنها اطلاعات سیستمی را جمع‌آوری می‌کند. از این ابزار در مواقع زیر استفاده می‌شود:

شناسایی بدافزارهای جدید

این ابزار اطلاعات سیستمی مانند پروسس‌های درحال اجرا، رجیستری، فایل‌های سیستمی مانند Config.Sys، Autoexec.bat و غیره را برای شناسایی بدافزار جدید جمع آوری می‌کند.

برای دریافت اطلاعات کوییک‌هیل توتال سکیوریتی

اطلاعات مربوط به نسخه‌ی آنتی‌ویروس کوییک‌هیل نصب شده بر روی سیستم، تنظیمات، پیکربندی را جمع آوری و در صورت وجود فایل(های) قرنطینه آنها را نیز دربر می‌گیرد.

این ابزار از اطلاعات سیستمی، یک فایل با نام INFO.QHC در درایو C:\ ایجاد کرده و همچنین آن را به صورت خودکار به ایمیل sysinfo@quickheal.com ارسال می‌کند.

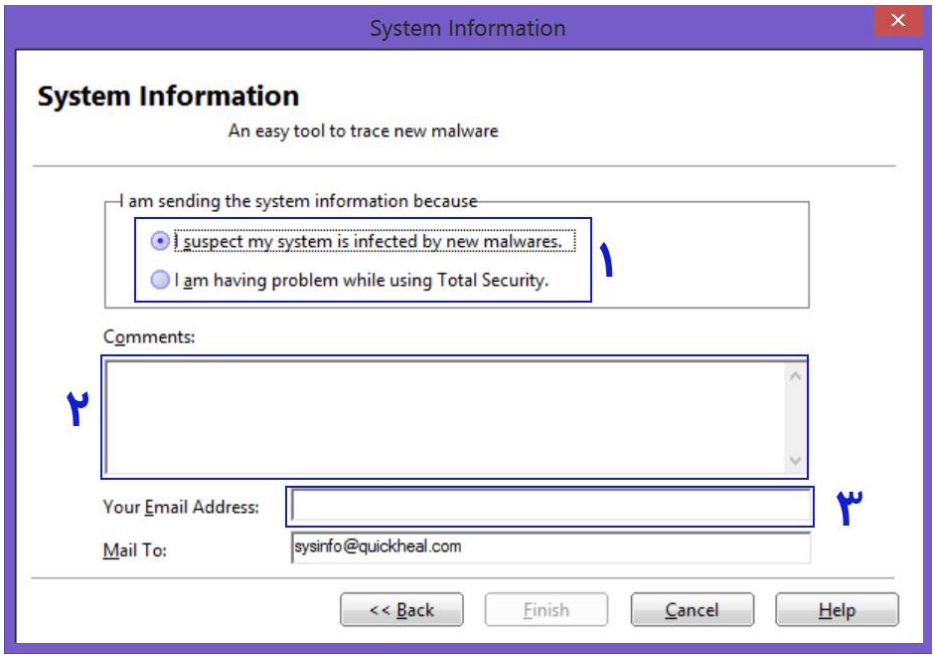
فایل INFO.QHC حاوی اطلاعات به فرمت‌های متنی و باینری می‌باشد. این فایل شامل اطلاعات حیاتی سیستمی و اطلاعات نسخه توتال سکیوریتی کوییک‌هیل نصب شده می‌باشد. اطلاعات حاوی فایل‌های اجرا شونده خودکار (از طریق Registry، Autoexec.bat، System.ini، Win.ini) و

پروسس‌های درحال اجرا به همراه اطلاعات کتابخانه‌های پشتیبان شده آنها می‌باشد. این اطلاعات برای آنالیز سیستم، شناسایی بدافزارها و عملکرد مناسب کوییک‌هیل توتال سکیوریتی استفاده می‌شود. این ابزار هیچ گونه اطلاعات شخصی، اطلاعات قابل شناسایی و هویتی، رمزهای عبور و غیره نمی‌باشد. کوییک‌هیل به حفظ حریم خصوصی کاربران خود احترام می‌گذارد؛ مطمئن باشید که این اطلاعات (سیستمی) نیز نه به اشتراک گذاشته و نه فاش خواهد شد.

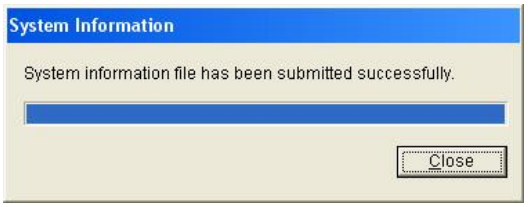
برای ارسال اطلاعات سیستمی گام‌های زیر را بردارید:

۱- در این بخش اطلاعات مشکل را به شرح زیر وارد می‌کنیم:

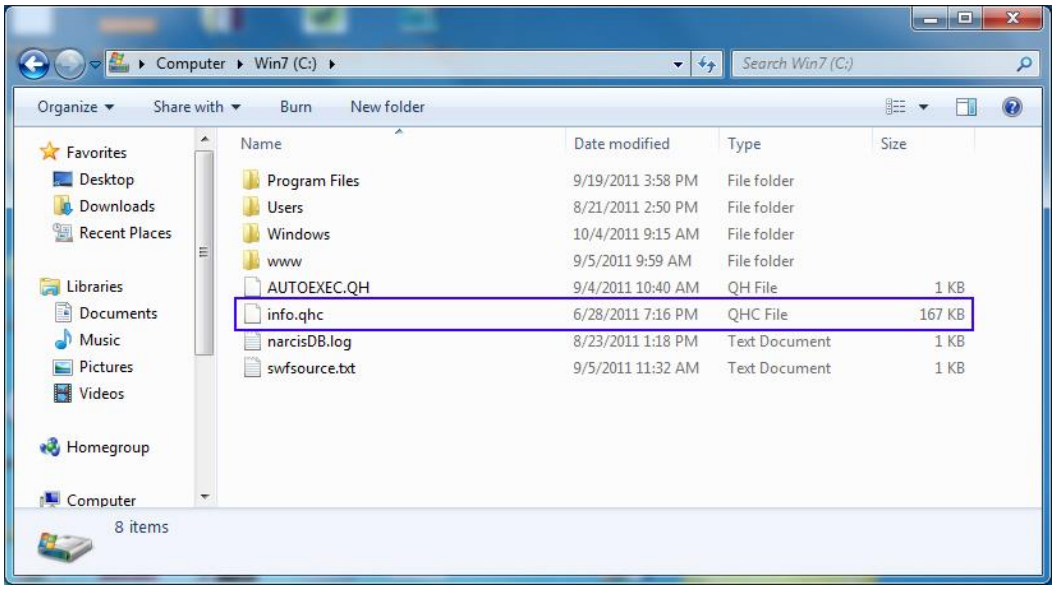
در قسمت (۱) در صورتی که احتمال می‌دهید سیستم به بدافزار جدید آلوده شده است گزینه اول را انتخاب می‌کنیم. اگر در کار کردن با مشکل برخورد کردیم گزینه دوم را انتخاب می‌نماییم.
در قسمت (۲) توضیحاتی راجع به مشکل به همراه مشخصات خود ارسال می‌نماییم.
در قسمت (۳) ایمیل خود را وارد و دکمه *Finish* را کلیک می‌کنیم.



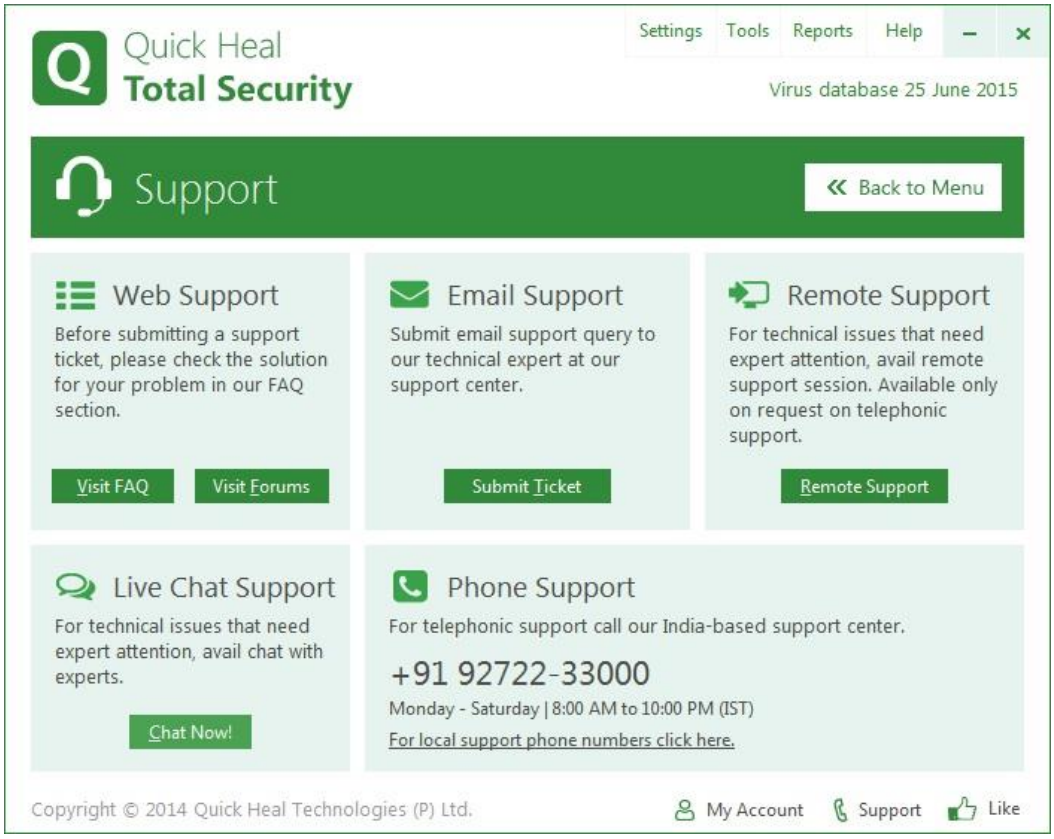
۲- پس از جمع‌آوری اطلاعات ضروری سیستمی پنجره زیر نمایش داده می‌شود:



۳- در انتها فایل info.qhc را که در درایو ریشه ویندوز (معمولاً C) ساخته می‌شود را به همراه فایل مشکوک به صورت فشرده Zip با پسورد ۱۲۳ قرار داده و به ایمیل support@quickheal.co.ir یا support @42722.ir ارسال نمایید.



ج) Support (پشتیبانی)

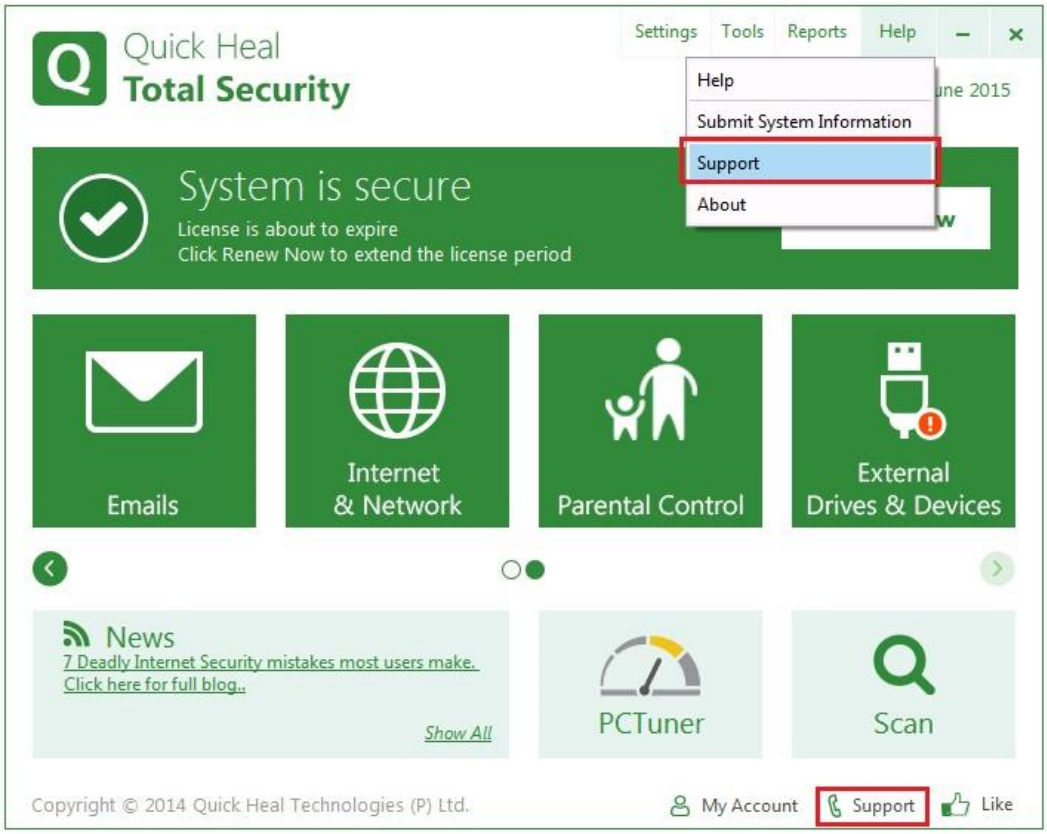


کوییک‌هیل، پشتیبانی فنی گسترده‌ای به کاربران ثبت (رجیستر) شده خود ارائه می‌دهد. برای دریافت پشتیبانی کارآمدتر، هنگام ارسال ایمیل یا تماس با تیم پشتیبانی کوییک‌هیل توصیه می‌شود که همه اطلاعات ضروری را اعلام فرمایید.

یکی از ویژگی‌های کلیدی و نقطه تمایز کوییک‌هیل نسبت به رقبا پشتیبانی این شرکت می‌باشد. علاوه بر پشتیبانی شرکت فناوری ارتباطات و اطلاعات فانوس –نماینده انحصاری محصولات کوییک‌هیل در ایران– که همه ی کانال‌های پشتیبانی کوییک‌هیل را توسط مهندسین دوره دیده خود ارائه می‌دهد، شرکت جهانی تکنولوژی‌های کوییک‌هیل نیز به صورت مستقیم به همه مشتریان ایرانی خود خدمات پشتیبانی ارائه می‌دهد. این پشتیبانی چند لایه‌ای، بهترین خدمات را به کاربران ارائه می‌دهد.

دسترسی به صفحه پشتیبانی (Support) از دو راه ممکن است:

۱. از منوی *Help > Support*
۲. از طریق دکمه *Support* انتهای پنجره



کارهایی که هنگام گم کردن کلید محصول (لایسنس) باید انجام دهید

کلید محصول به عنوان شناسه هویتی شما برای آنتی‌ویروس کوییک‌هیل می‌باشد.

در صورتی که رمز عبور خود را گم کرده‌اید با پشتیبانی فنی کوییک‌هیل تماس بگیرید.

در صورتی که مشتری طرح جزیره امن کوییک‌هیل هستید به سایت 42722.ir مراجعه فرمایید.

پشتیبانی

این گزینه یک پشتیبانی جامع آنلاین به شما ارائه می‌دهد تا بتوانید پاسخ سوالات خود را از روش‌های گوناگون بیابید. در صفحه پشتیبانی می‌توانید دسترسی به انواع کانال‌های پشتیبانی کوییک‌هیل را مشاهده نمایید. صفحه پشتیبانی کوییک‌هیل حاوی گزینه‌های FAQ (سوالات متداول) که می‌توانید پاسخ به سوالات پرتکرار را مطالعه نمایید، ارسال سوال، ارسال ایمیل درباره سوالات یا اطلاعات تماس مستقیم با ما می‌باشد.

این پشتیبانی شامل گزینه‌های زیر می‌باشد:

Web Support (پشتیبانی وب)

با استفاده از این گزینه می‌توانید سوالات خود را ارسال و یا سوالات متداول (FAQ) را مشاهده نمایید. پیش از استفاده از ابزارهای دیگر پشتیبانی، توصیه می‌شود صفحه ی سوالات متداول را مطالعه نمایید. ممکن است سوال شما قبلاً در این بخش پاسخ داده شده باشد.

برای مشاهده سوالات متداول بر روی دکمه *Visit FAQ* کلیک نمایید.

در صورتی که سوال خود را در این بخش نیافته‌اید می‌توانید سوال خود را از طریق انجمن کوییک‌هیل با کلیک بر روی دکمه *Visit Forums* مطرح نمایید.

Email Support (پشتیبانی ایمیل)

این ویژگی به شما کمک می‌کند تا با ایجاد تیکت، سوالات خود را با متخصصین کوییک‌هیل درمیان گذاشته و پاسخ مناسب دریافت نمایید.

برای ارسال ایمیل (ایجاد تیکت) بر روی دکمه *Submit Ticket* کلیک کنید.

Phone Support (پشتیبانی تلفنی)

برای دریافت پشتیبانی فنی کوییک‌هیل به صورت تلفنی، با شماره تلفن درج شده در این بخش (۷۷۱۴۲۵۲۶-۰۲۱) تماس بگیرید.

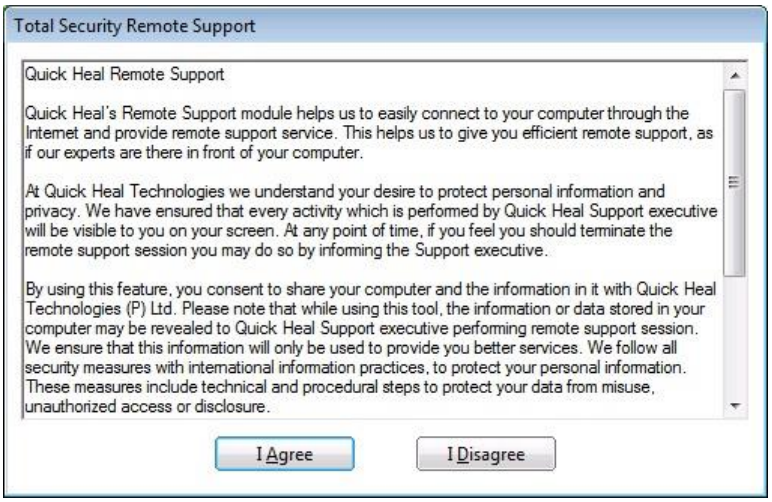
کاربران طرح جزیره امن برای دریافت پشتیبانی می‌توانند با شماره ۴۲۷۲۲-۰۱۱ تماس بگیرند.

Remote Support (پشتیبانی راه دور)

در برخی مواقع تیم پشتیبانی فنی کوییک‌هیل، خدمات پشتیبانی راه دور (Remote Support) ارائه می‌دهند. این ماژول پشتیبانی کمک می‌کند تا به سادگی از طریق اینترنت به سیستم رایانه‌ی شما متصل شده و از راه دور پشتیبانی فنی ارائه دهیم. این ویژگی به کوییک‌هیل کمک می‌کند تا پشتیبانی کارآمد به شما ارائه داده و مهندسین فنی شرکت مشکل شما را حل نمایند.

برای اجرای پشتیبانی ریموت، مراحل زیر را دنبال کنید:

۱. بر روی *Remote Support* کلیک کنید.



۲. متن توافقنامه را به دقت مطالعه کرده و بر روی *I Agree* کلیک کنید.

۳. ID (شناسه) نشان داده شده در پنجره پشتیبانی ریموت را به مهندسین پشتیبانی کوییک‌هیل اعلام نمایید.

٤. مهندسین پشتیبانی کوییک‌هیل به صورت ریموت و از راه دور به سیستم شما متصل شده و مشکل شما را رفع خواهند کرد.

توجه ۱: با استفاده از این ویژگی، مهندسین کوییک‌هیل به سیستم شما دسترسی خواهند داشت (درست همانند اینکه مهندسین کوییک‌هیل در پشت سیستم شما قرار دارند). شما می‌توانید تمام فعالیت‌هایی که مهندسین پشتیبانی بر روی رایانه شما انجام می‌دهند را مشاهده نمایید.

توجه ۲: به محض اینکه شما پنجره پشتیبانی ریموت (Quick Heal Remote Support) را ببندید، ارتباط تیم پشتیبانی به طور کامل قطع خواهد شد.

Live Chat Support (پشتیبانی گفتگوی زنده)

شما می‌توانید با استفاده از این قابلیت، با کارشناسان فنی کوییک‌هیل به صورت زنده چت و گفتگو نموده و مشکل خود را رفع نمایید.

ارتباط با پشتیبانی کوییک‌هیل در ایران:

سیستم تیکتینگ: http://support.quickheal.co.ir

اطلاعات تماس: http://quickheal.co.ir/contact

ارتباط با پشتیبانی طرح جزیره امن کوییک‌هیل:

سیستم تیکتینگ: http://support.quickheal.co.ir/

اطلاعات تماس: http://42722.ir/contact.php

اطلاعاتی که هنگام تماس با پشتیبانی نیاز دارید

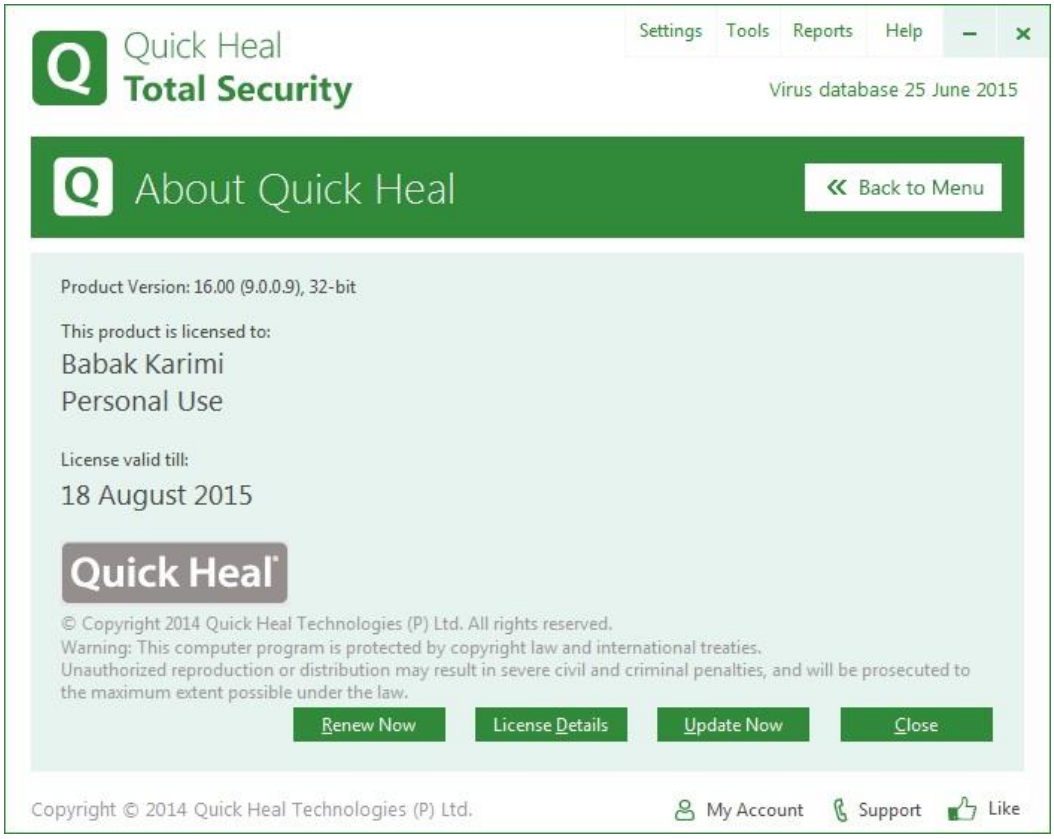
- کلید محصول (لایسنس): که در اختیار شما قرار گرفته است (بسته به نوع خرید: در صفحه اول دفترچه راهنما درج شده، یا پس از خرید آنلاین به شما نشان داده شده و به ایمیل شما ارسال شده؛ یا به شماره همراه شما پیامک شده؛ یا در رسید یا فاکتور فروش به شما ارائه شده است).
- اطلاعاتی راجع به کامپیوتر خود: برند، نوع CPU، ظرفیت RAM، سایز درایو هارد و فضای آزاد موجود در آن (درایوی که آنتی ویروس بر روی آن نصب شده) و نیز اطلاعاتی در رابطه با وسایل جانبی متصل شده به آن.
- نام سیستم عامل، شماره نسخه (version number) و زبان.
- نوع و نسخه آنتی‌ویروس نصب شده و تاریخ آپدیت آنتی‌ویروس.
- نرم افزار نصب شده بر روی کامپیوتر.
- آیا رایانه شما به شبکه متصل است؟ اگر بله – ابتدا با مدیر شبکه تماس بگیرید. اگر مدیران شبکه نتوانستند مشکل شما را حل کنند، آنها باید با پشتیبانی فنی کوییک‌هیل تماس بگیرند.
- جزئیات: چه زمانی اولین بار این مشکل ظاهر شد؟ وقتی مشکل به وجود آمد شما چه کاری انجام دادید؟

یادآوری: در اکثر موارد این اطلاعات به ما کمک می‌کند تا مشکل شما را به سرعت حل کنیم.

چه چیزی باید به کارشناسان پشتیبانی فنی بگویم؟

باید تا حد امکان با حداکثر جزئیات اطلاعات را در اختیار کارشناسان پشتیبانی قرار دهید تا آنها بتوانند بر اساس اطلاعات شما راهکار مناسب ارائه دهند.

د) About(درباره)



صفحه About، اطلاعاتی درباره محصول شامل نسخه آنتی‌ویروس کوییک‌هیل، اطلاعات صاحب لایسنس محصول، تاریخ اعتبار لایسنس می‌باشد.

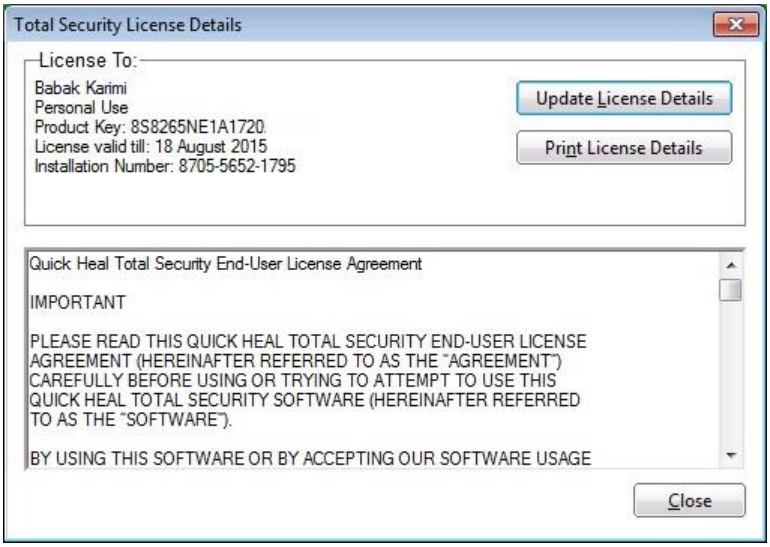
در انتهای این صفحه دکمه‌های زیر وجود دارد:

Renew Now: امکان تمدید اشتراک فعلی را فراهم می‌آورد. کاربران ایرانی می‌توانند از طریق سایت رسمی کوییک‌هیل به نشانی http://quickheal.co.ir یا مشترکان طرح جزیره امن از طریق سایت http://42722.ir اقدام نمایند.

License Details: اطلاعات کامل مربوط به لایسنس ثبت نام شده به همراه متن توافقنامه استفاده از نرم‌افزار قابل مشاهده می‌باشد.

Update Now: بروزرسانی آنتی‌ویروس به صورت خودکار و دوره‌ای انجام می‌شود. اما در صورتی که بخواهید همین الان بروزرسانی را انجام دهید، بر روی این دکمه کلیک کنید.

Close: پنجره جاری بسته شده و به صفحه داشبورد منتقل می‌شود.

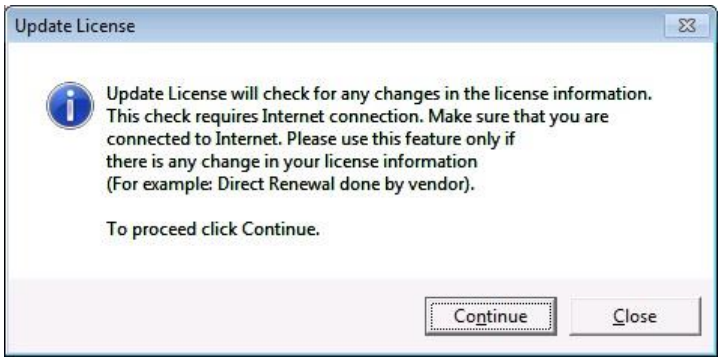


Update License Details: با استفاده از این دکمه می‌توانید اطلاعات لایسنس محصول خود را با سرور فعالسازی کوییک‌هیل همگام‌سازی نمایید. اگر می‌خواهید لایسنس خود را تمدید نمایید، اما نمی‌دانید چگونه می‌توان لایسنس را تمدید کرد، و یا در زمان تمدید با مشکل مواجه شدید، با تیم پشتیبانی کوییک‌هیل تماس گرفته و لایسنس خود را به کارشناسان پشتیبانی اعلام نمایید.

تیم پشتیبانی کوییک‌هیل، لایسنس شما را تمدید خواهند کرد. پس از خرید و اعمال لایسنس تمدیدی، نیاز است گام‌های زیر را بردارید:

۱. رایانه را به اینترنت متصل نمایید.

۲. بر روی دکمه ***Update License Details*** کلیک کنید.



۳. برای بروزرسانی اشتراک فعلی خود بر روی ***Continue*** کلیک کنید.

Print License Details: برای چاپ اطلاعات لایسنس و اشتراک فعلی خود بر روی این دکمه کلیک کنید.

Update Now: توتال سکیوریتی کوییک‌هیل (پایگاه داده ویروس) را بروزرسانی می‌کند.

Close: صفحه پشتیبانی آنتی‌ویروس را می‌بندد.

خاتمه

در کنار سه شعار اصلی هوشمندتر، سبک‌تر و سریع‌تر (smarter, lighter, faster) کوییک‌هیل، که نمایانگر استفاده حداقلی از منابع می‌باشد، رعایت اصول سادگی، کاربرپسند در نصب، راه‌اندازی و مدیریت اندپوینت سکیوریتی کوییک‌هیل یکی دیگر از مزایای کلیدی این آنتی‌ویروس نسبت به سایرین می‌باشد.

راه‌اندازی Update Server رسمی و Honeypot در ایران (ظرف عسل جهت جذب و آنالیز ویروس‌های منطقه‌ای ایران برای افزایش قدرت ویروس شناسی در ایران)، به همراه لابراتوارهای مجازی مستقر در انجین DNAScan در همه کلاینت‌ها از دیگر قابلیت‌های انحصاری این شرکت برای کاربران ایرانی جهت افزایش قدرت ویروس‌شناسی می‌باشد.

ارتباط مستقیم و مستمر و بدون واسطه تیم فنی و پشتیبانی شرکت تکنولوژی‌های کوییک‌هیل هند با کاربران نهایی و نیز شرکت فناوری ارتباطات و اطلاعات فانوس به عنوان نماینده رسمی محصولات امنیتی سازمانی در ایران موجب اطمینان خاطر کاربران از پشتیبانی بدون وقفه کوییک‌هیل می‌گردد.

برای دریافت اطلاعات بیشتر از جوایز، تاییدیه‌ها، سایر محصولات و توانمندی‌های کوییک‌هیل به وب‌سایت شرکت مراجعه و یا با شماره ۰۲۱-۷۷۱۴۲۵۲۶ تماس حاصل فرمایید.