راهنمای سریع استفاده از کوییک هیل اندپوینت سکیوریتی

QuickHeal Endpoint Security 5.3

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 نسخه سازمانی 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 می توانید با شرکت فناوری ارتباطات و اطلاعات قانوس 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.

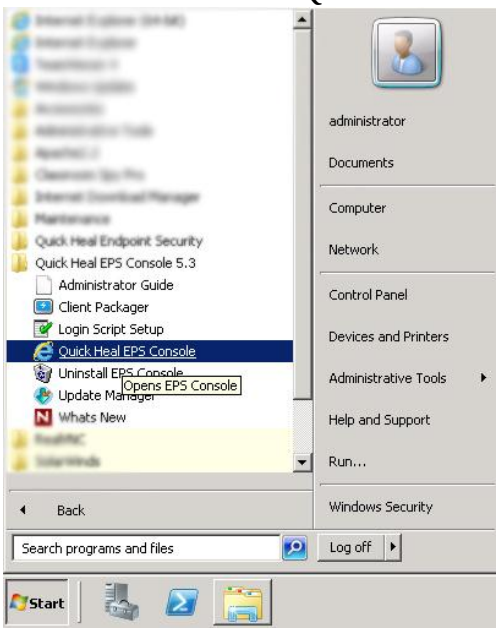
بدیهی است استفاده از این جزوه تنها ویژه شبکه توزیع، مشتریان شرکت فناوری فانوس مجاز می‌باشد و حق نسخه‌برداری برای این شرکت محفوظ است.

فهرست مطالب

آغاز به کار کنسول مدیریتی متمرکز اندپوینت‌سکیوریتی کوییک‌هیل

۱. اجرای کنسول کوییک‌هیل اندپوینت‌سکیوریتی از روی سرور:

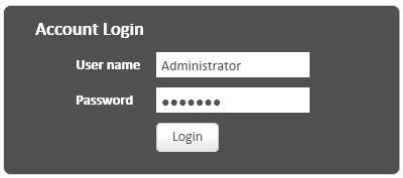
Start > Quick Heal EPS Console 5.3 > Quick Heal EPS Console



همچنین می توانید کنسول مدیریتی تحت وب اندپیونت را از روی سرور و یا هر یک از کلاینت های موجود در شبکه اجرا نمایید. برای اجرا باید آدرس و یا نام سرور را به صورت زیر از طریق مرورگر اینترنت اکسپلورر IE اجرا نمایید:

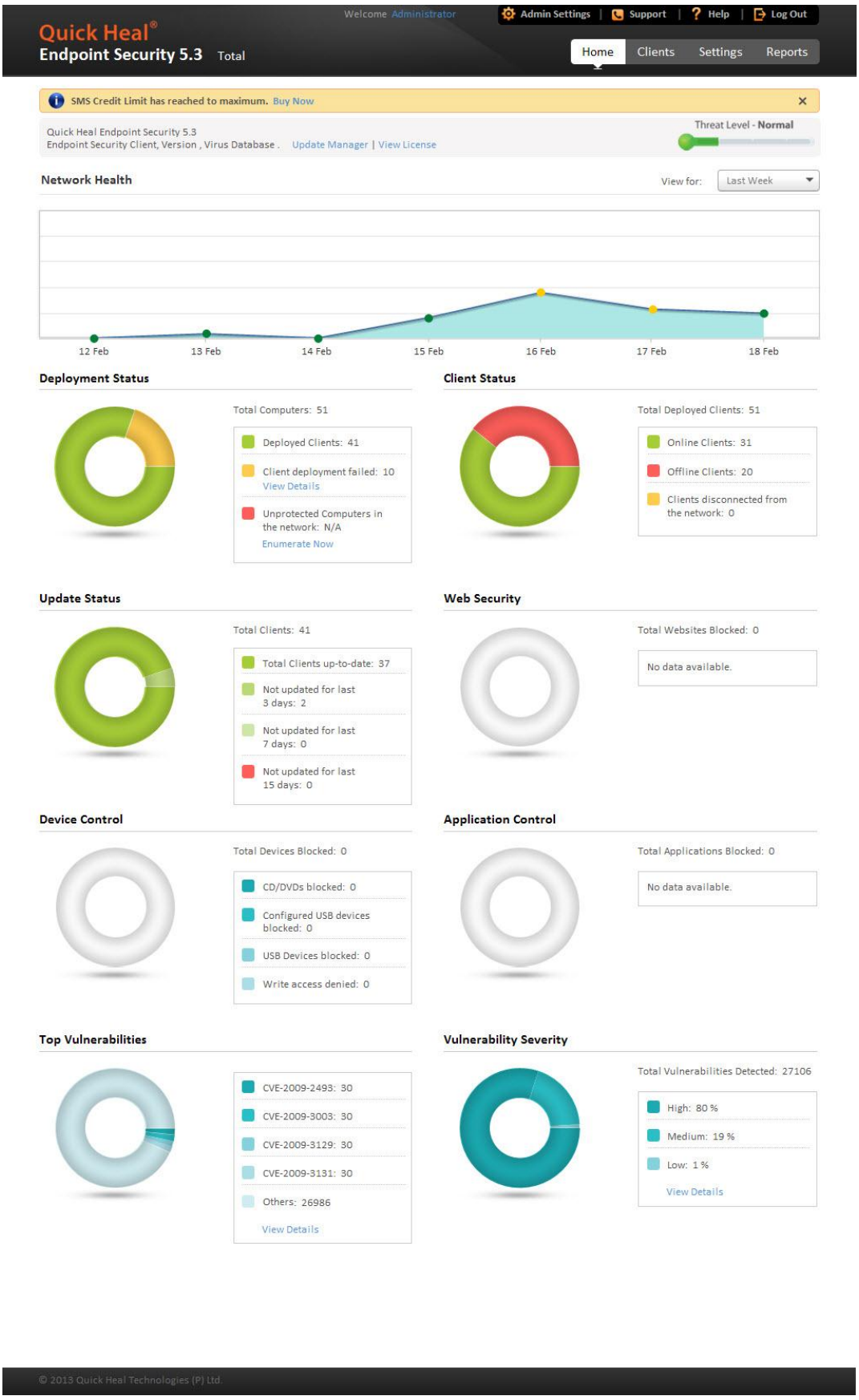
https://IP-Server:9098/qhscan503

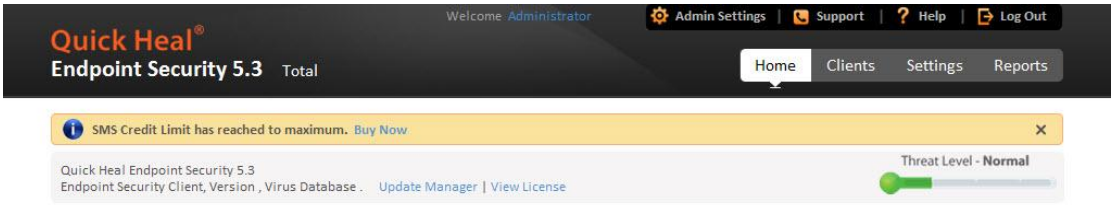
۲. نام کاربری پیش فرض Administrator و رمز عبور، همان رمزی مدیریتی است که در زمان نصب تعریف نمودید.



داشبورد مدیریتی

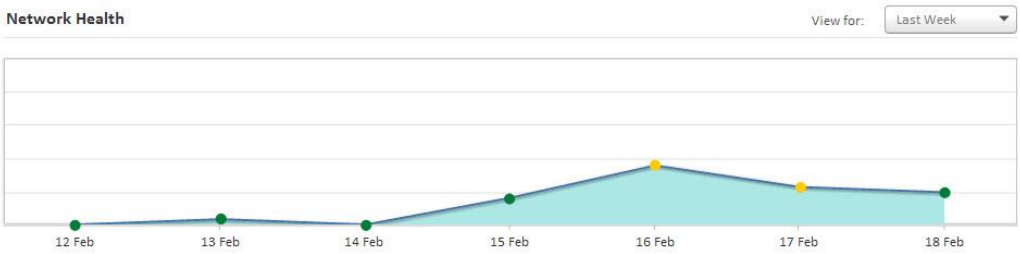
صفحه نخست (داشبورد) خلاصه اطلاعاتی راجع به مسائل امنیتی شبکه ارائه می دهد.





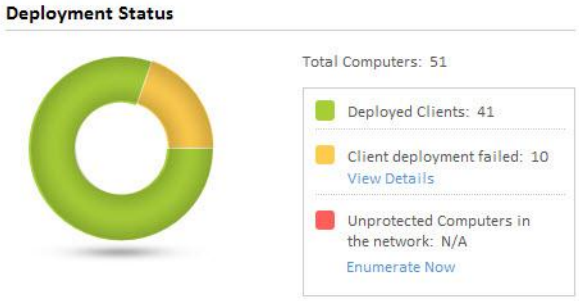
اعلان ها و اخطارهای ضروری راجع به کنسول مدیریتی در صورت وجود، در نوار نارنجی رنگ بالای صفحه به نمایش در می آید. (مثلا تعداد پیامک های اطلاع رسانی مجاز به اتمام رسیده است، لایسنس در حال انقضا می‌باشد، سرویس پک جدید برای اندپوینت ارائه شده است و نیاز به اجرا دارد، مدت زمان طولانی است که سیستم بروزرسانی نشده است، تعداد کاربران نصب شده از تعداد لایسنس مجاز فراتر رفته است و...)

در نوار طوسی رنگ، نام و نسخه محصول به همراه تاریخ بروزرسانی نمایش داده می‌شود. با کلیک بر روی Update Manager می توانید وضعیت بروزرسانی اندپوینت را مشاهده و یا تنظیمات دلخواه را اعمال نمایید. اطلاعات مربوط به لایسنس از طریق لینک View License در دسترس می‌باشد. سطح تهدید در شبکه با نمودار رنگی (سبز=عادی، زرد=درحال افزایش، نارنجی=زیاد، قرمز=بحرانی) قابل مشاهده می‌باشد.



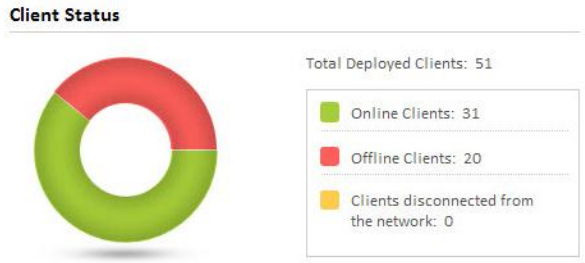
باکس Network Health به صورت گرافیکی وضعیت امنیتی شبکه را نمایش می دهد. از طریق فرم بازشو View for می توانید نمایش را از هفته اخیر (Last Week) به حالت ۲٤ ساعت گذشته، ۱۵ روز اخیر و ۳۰ روز اخیر تغییر دهید. با کلیک بر روی هر یک از گره می توانید اطلاعات ویروس و کلاینت آلوده مربوطه را دریافت نمایید.

در ادامه صفحه، اطلاعات کوییک‌هیل اندپوینت‌سکیوریتی به صورت نمودارهای حلقه ای نمایش داده می‌شود.



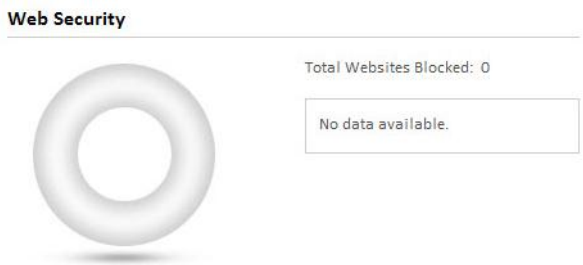
الف) Deployment Status: در این بخش وضعیت نصب کلاینتها نمایش داده می‌شود. تعداد کل کلاینت ها (Total Computers)، تعداد کلاینت های نصب شده

(Deployed Clients) و تعداد کلاینتهایی که هنوز کوییک‌هیل ایجنت برروی آنها نصب نشده و غیرمحافظت شده می‌باشند (Unprotected Computers in the network) نشان داده می‌شود. با کلیک بر روی Enumerate Now اندپوینت به دنبال تعداد کلاینتهای جدید در شبکه می‌گردد.

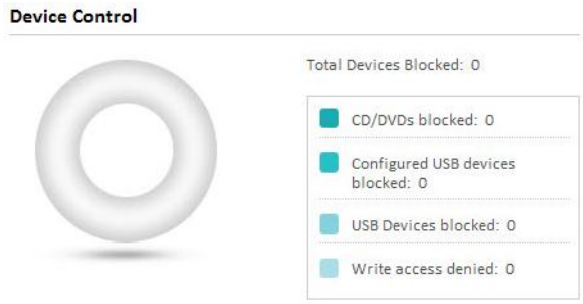


ب) *Client Status:* در این بخش وضعیت کلاینت نشان داده می‌شود. تعداد کل کلاینتهایی که کوییک‌هیل بر روی آنها نصب شده است (Total Deployed Clients)، تعداد کلاینتهایی که هم اکنون روشن و آنلاین بوده و ارتباط با سرور دارند (Online Clients)، تعداد کلاینت هایی که هم اکنون آفلاین، خاموش و یا ارتباط شبکه ای با سرور ندارند (Offline Clients)، تعداد کلاینت هایی –که به علت آلودگی و تیک بودن گزینه مربوط به قطع اتصال شبکه ای در صورت آلوده بودن در بخشی سیاست گذاری– ارتباط آن با شبکه قطع شده است (Clients disconnected from the network) نمایش داده می‌شود.

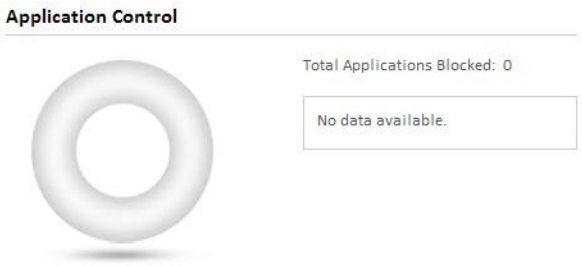
ج) *Update Status:* وضعیت بروزرسانی در این بخش نشان داده می‌شود. تعداد کلاینت ها (Total Clients)، تعداد کلاینت های بروز شده (Total Clients up-to-date)، تعداد کلاینتهایی که از ۳ روز گذشته آپدیت نشده اند (Not updated for last 3 days)، تعداد کلاینتهایی که از ۷ روز گذشته آپدیت نشده اند (Not updated for last 7 days)، تعداد کلاینتهایی که از ۱۵ روز گذشته آپدیت نشده اند (Not updated for last 15 days) در این بخش نمایش داده می‌شود.



د) *Web Security:* در این بخش اطلاعات مربوط به امنیت وب نشان داده می‌شود. در این بخش می توانید اطلاعات مربوط به تعداد سایت های آلوده و نیز مسدود شده توسط مدیر که کاربران قصد مشاهده آنها را داشتند را ملاحظه نمایید.

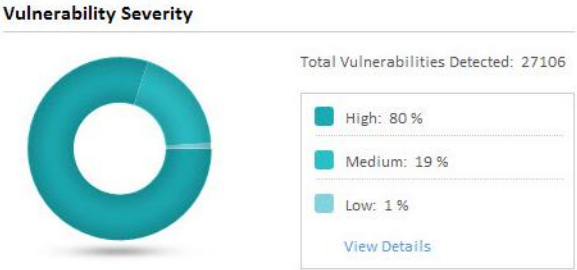


هـ) *Device Control:* در صورتی که از گزینه مسدود کردن دستگاههای حافظه های جانبی USB (فلش، هارد اکسترنال) و CD/DVD Rom استفاده نمایید، اطلاعات مربوط به مسدود سازی آنها در این بخش قابل مشاهده می‌باشد. می‌توانید اطلاعاتی نظیر مجموع دستگاههای مسدود شده (Total Devices Blocked)، تعداد سی دی رام / دی وی دی رام مسدود شده (CD/DVDs blocked)، دستگاههای USB پیکربندی شده مسدودی (Configured USB devices blocked)، ابزارهای USB مسدود شده (USB Devices blocked)، تعداد ابزارهای فقط خواندنی (Write access denied) را مشاهده نمایید.



و) *Application Control:* در این بخش اطلاعات مربوط به کنترل برنامه و مسدودسازی برنامه ها ارائه می‌گردد.

ز) *Top Vulnerabilities:* در این بخش بیشترین آسیب پذیری ها و حفره های نرم افزاری موجود در شبکه لیست می‌شود. با کلیک بر روی View details می توانید اطلاعات بیشتری راجع به آسیب پذیری مربوطه دریافت نمایید.

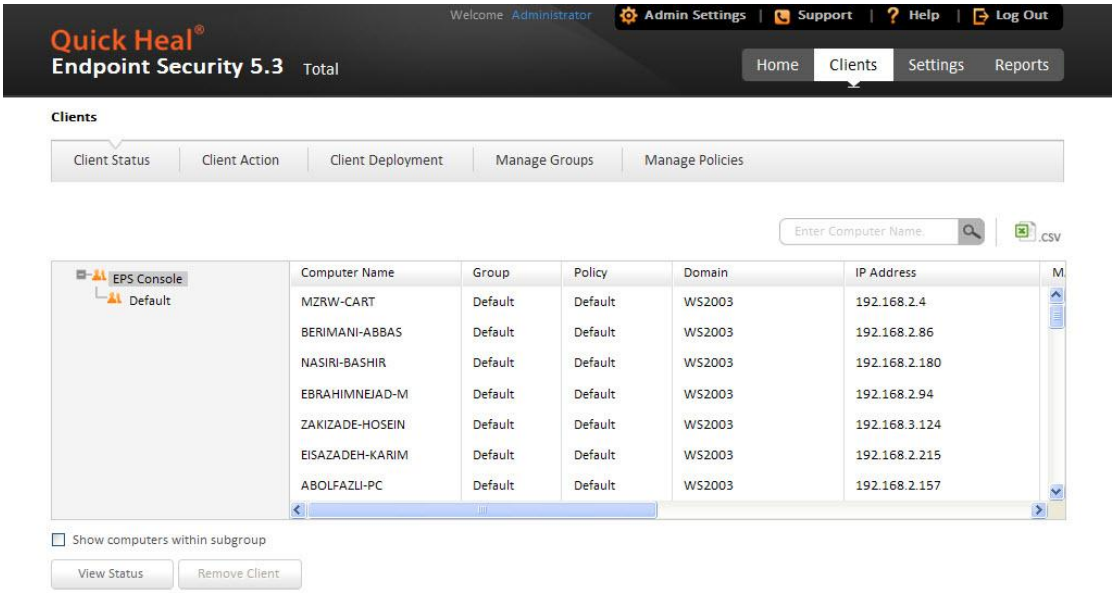


ح) *Vulnerability Severity:* در این بخش میزان خطرپذیری حفره های کلاینت های شبکه، بسته به میزان تهدید آسیب پذیری لیست می‌شوند.

کلاینت ها Clients

دومین سربرگ اصلی، Clients می‌باشد. در بخش کلاینت پیکربندی های آنتی ویروس کلاینت ها قابل اعمال می‌باشد.

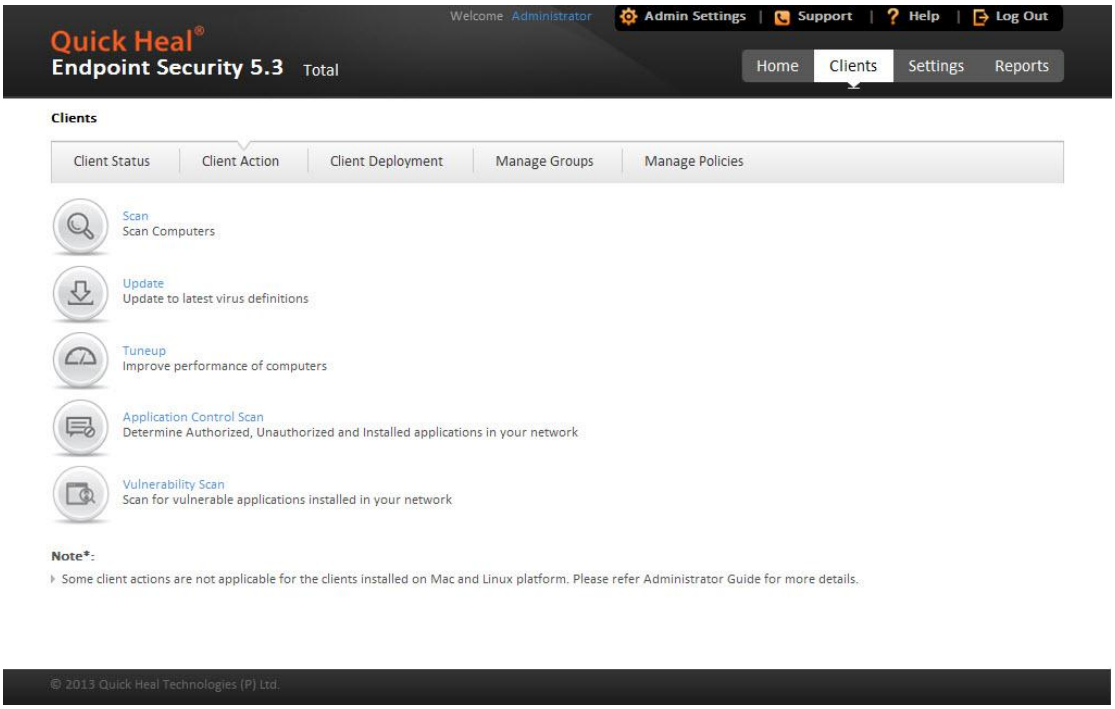
الف) Client Status



این سربرگ وضعیت کلاینت ها را نشان می دهد. در این صفحه می توانید کلاینت همه گروه ها و گروههای خاص را مشاهده نمایید. با کلیک بر روی نام گروه در درختواره سمت چپ می توانید اطلاعات کامپیوترهای موجود در آن گروه را ببینید. گروه پیش فرض Default می‌باشد. اطلاعاتی نظیر نام کامپیوتر (Computer Name)، گروهی که کلاینت عضو آن است (Group)، سیاست گذاری اعمال شده بر روی آن کلاینت یا گروه (Policy)، دامنه (Domain)، آدرس آی پی (IP Address)، آدرس فیزیکی کارت شبکه (MAC Address)، وضعیت آنلاین و یا آفلاین بودن (Status)، وضعیت نصب (Installation Status)، نسخه محصول ایجنت (Product Version)، تاریخ بروزرسانی (Virus Database Date) و تاریخ آخرین اسکن (Last Scan Date) در این بخش ارائه می‌شود. با کلیک بر روی عنوان هر گزینه براساس آن پارامتر مرتب سازی انجام می‌گیرد. با انتخاب یک کلاینت و کلیک بر روی دکمه View Status، اطلاعات کاملی از کلاینت مربوطه ارائه می‌گردد. با تیک کردن گزینه Show computers within subgroup همه کلاینتهای عضو زیرگروه انتخابی لیست می‌گردند.

ب) سربرگ Client Action:

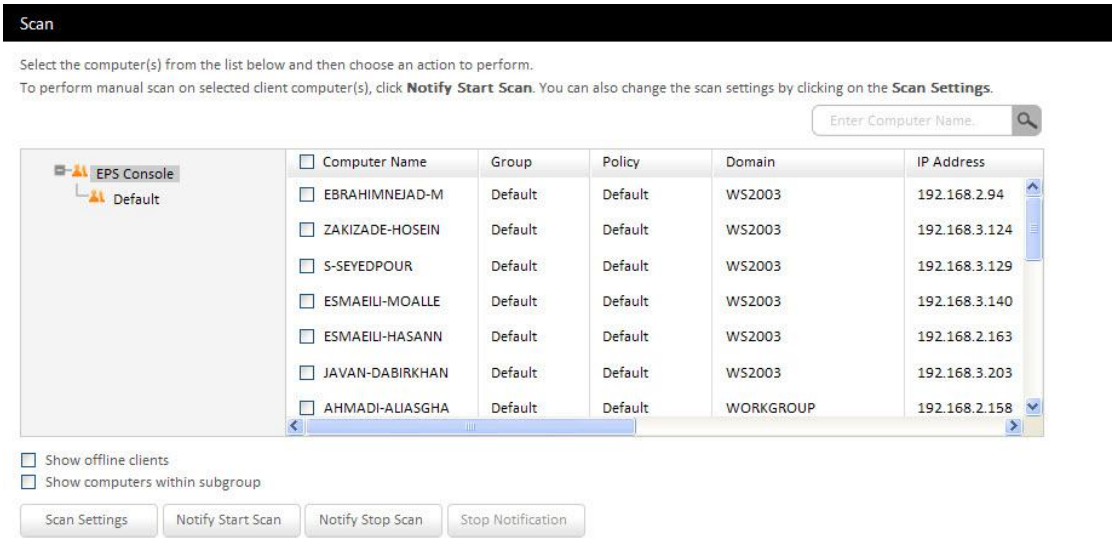
عملیات قابل اجرا بر روی کلاینت ها در این صفحه لیست می‌شود:



.

Scan:

برای اسکن و ویروسیابی کلاینت ها از راه دور از این گزینه استفاده می‌شود. با کلیک بر روی این گزینه پنجره جدیدی باز می‌شود که می توانید کلاینت های مورد نظر را از گروه مربوطه انتخاب و اسکن نمایید.



از طریق جعبه متنی بالایی می توانید نام کامپیوتر موردنظر را جستجو نمایید.

برای نمایش کلاینت های آفلاین گزینه Show offline clients را تیک کنید.

برای نمایش کامپیوترهای موجود در زیرگروه گزینه Show computers within subgroup را تیک نمایید.

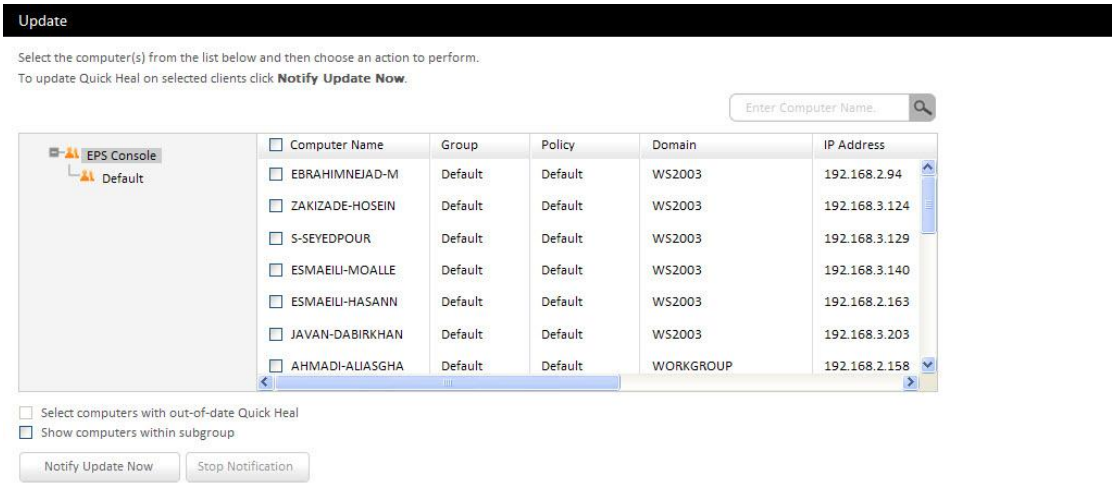
تنظیمات اسکن از طریق دکمه Scan Settings قابل تغییر می‌باشد.

برای ارسال دستور اسکن پس از انتخاب کامپیوتر مربوطه دکمه Notify Start Scan را کلیک نمایید.

در صورتی که می خواهید عملیات اسکن بر روی کلاینت مربوطه متوقف گردد، بر روی دکمه Notify Stop Scan کلیک کنید تا دستور توقف به کلاینت ارسال گردد.

در صورتی که از ارسال دستور شروع و یا توقف اسکن پشیمان شده اید می توانید بر روی Stop Notification کلیک کنید تا ارسال دستور، متوقف گردد.

Update:



بروزرسانی کلاینت ها به صورت خودکار می‌باشد و نیاز به هیچ عملیات اضافی برای این کار نمی‌باشد. اما اگر به هر علتی مایلید فرآیند بروزرسانی کلاینتی خاص را فوری انجام دهید، می توانید از این گزینه استفاده نمایید.

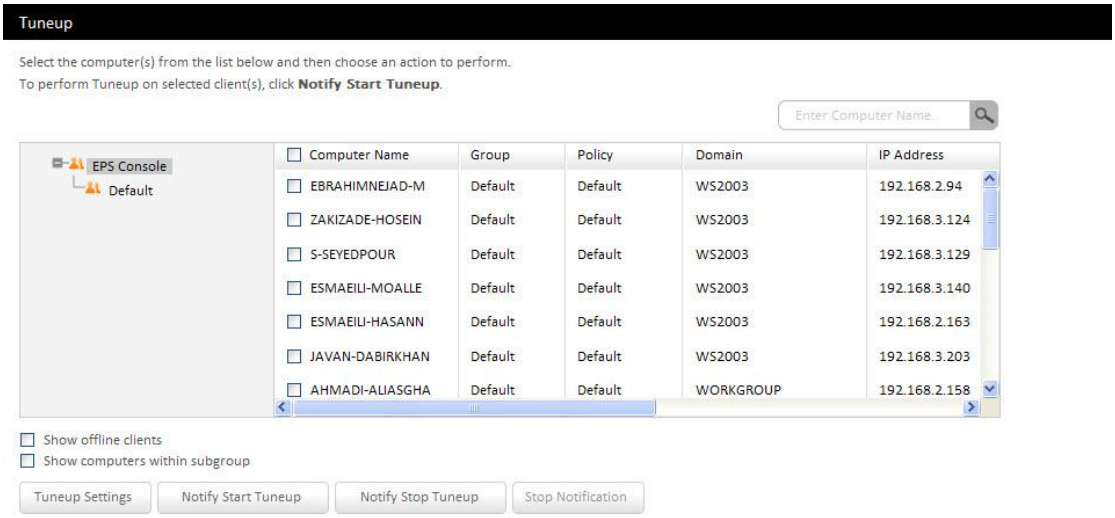
Select computers with out-of-date Quick Heal: این گزینه کامپیوترهای بروز نشده را انتخاب می کند.

Notify Update Now: با انتخاب کلاینتهایی که مایلید بروز گردند، و کلیک بر روی این دکمه، ارسال دستور آپدیت به کلاینت ها صورت می‌پذیرد.

Stop Notification: ارسال دستور بروزرسانی را متوقف می کند.

Tuneup:

بهینه سازی و بهبود عملکرد ویندوز از طریق این برنامه سودمند قابل انجام است.



Tuneup Settings: تنظیمات بهینه سازی با کلیک برروی این دکمه قابل انجام است. فرایند بهینه سازی از طریق پاکسازی اطلاعات زائد (Disk Cleanup)، پاکسازی اطلاعات زائد رجیستری ویندوز (Registry Cleanup) و دیفرگمنت فایل های مهم سیستم عامل در راه‌اندازی بعدی (Defragment at next boot) قابل انجام است.

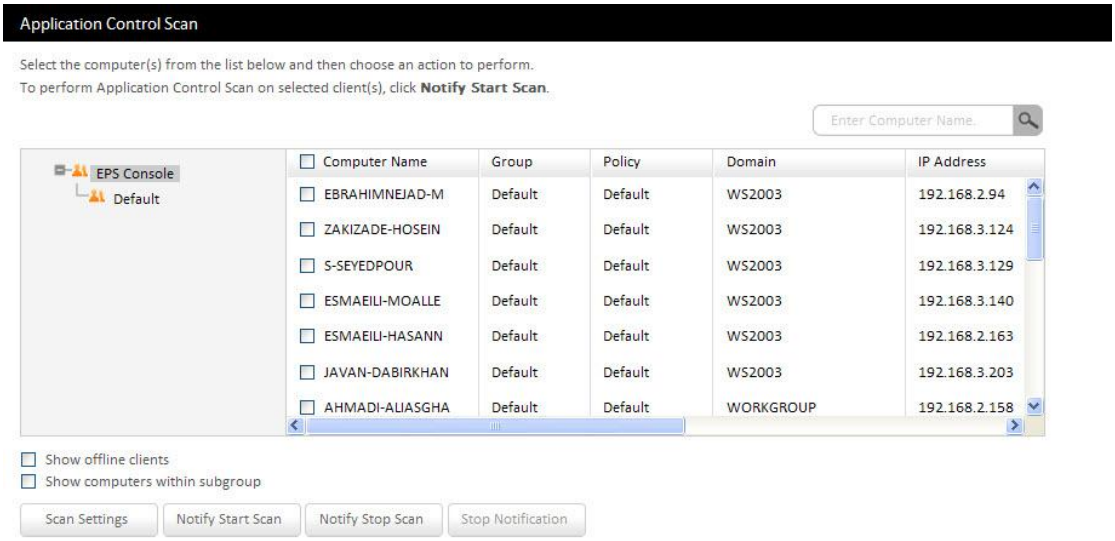
Notify Start Tuneup: ارسال دستور شروع بهینه سازی به کلاینت/کلاینت های انتخابی.

Notify Stop Tuneup: ارسال دستور توقف بهینه سازی به کلاینت/کلاینت های انتخابی.

Stop Notification: انصراف از ارسال دستور به کلاینت.

Application Control Scan:

در این بخش می توانید اقدام به اسکن اپلیکیشن و برنامه های نصب شده بر روی کلاینت یا کلاینت های مورد نظر نموده و گزارش آن را در بخش Report ملاحظه فرمایید.



Scan Settings: با کلیک بر روی این دکمه می توانید تنظیمات اسکن برنامه ها را تغییر دهید. می توانید تنها برنامه‌های کاربردی که در پالیسی تعریف شده شما غیرمجاز شده اند (Unauthorized applications)، یا همه برنامه های مجاز و غیر مجاز (Unauthorized and authorized applications)، و یا همه برنامه های نصب شده بر روی کلاینت (All installed applications) را اسکن و گزارش کاملی از آن دریافت نمایید.

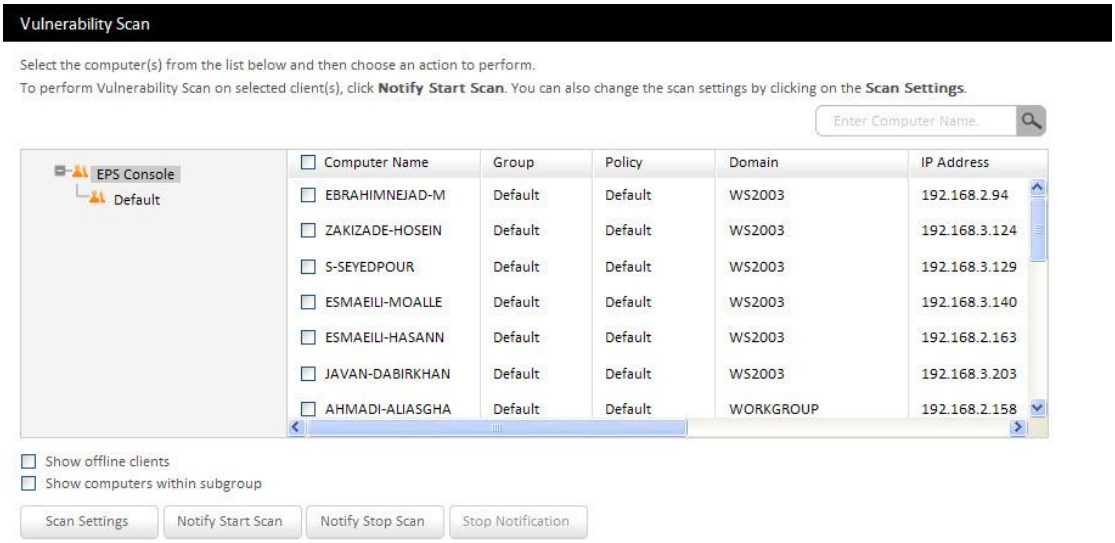
Notify Start Scan: ارسال دستور شروع به کار اسکن برنامه ها به کلاینت/کلاینت های انتخابی.

Notify Stop Scan: ارسال دستور توقف اسکن برنامه ها به کلاینت/کلاینت های انتخابی.

Stop Notification: توقف فرایند ارسال دستور به کلاینت.

Vulnerability Scan:

گزارش کاملی از آسیب پذیری های سیستم عامل مایکروسافت ویندوز و برنامه های نصب شده بر روی کلاینت از شرکت های مختلف نرم افزاری جهان مانند Adobe، Apple، Mozilla، Oracle ارائه می دهد. با این ویژگی می توانید به راحتی وضعیت امنیتی رایانه های شبکه خود را بررسی و وصله های مورد نیاز را دریافت نمایید.

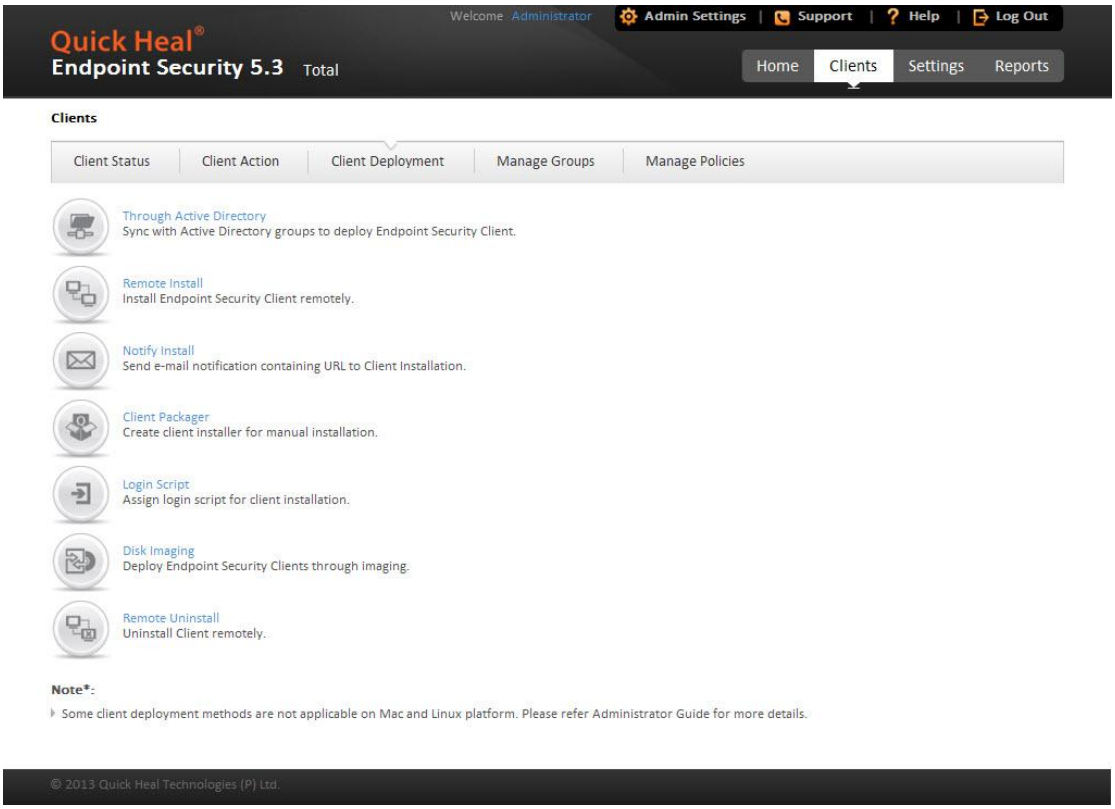


با کلیک بر روی Scan Settings می توانید تعیین کنید که آسیب پذیری های مایکروسافت و شرکت های دیگر یا فقط آسیب پذیری های مایکروسافت و یا تنها آسیب پذیری های شرکت های دیگر مورد بررسی و کاوش قرار گیرند.

- ✓ با انتخاب کلاینت مورد نظر و کلیک بر روی دکمه Notify Start Scan دستور اجرای اسکن آسیب پذیری و تهیه گزارش ارسال می‌گردد.
- ✓ برای ارسال دستور توقف فرایند اسکن آسیب پذیری بر روی Notify Stop Scan کلیک کنید.
- ✓ جهت انصراف از ارسال دستور بر روی Stop Notification کلیک کنید.

ج) سربرگ Client Deployment

مدیریت نصب و حذف کلاینت ها در این بخش انجام می‌پذیرد.



اندپوینت‌سکیوریتی کوییک‌هیل از ٦ روش نصب و یک روش حذف پشتیبانی می کند. متناسب با پیکربندی شبکه و مطابق سلیقه خود می توانید یکی از این ٦ روش نصب را استفاده می کنیم.

١. Through Active Directory: با استفاده از این ویژگی می توانید نصب Client Agent کوییک‌هیل را از طریق کنترلر دامنه Active Directory انجام دهید. توضیحات بیشتر در صفحه ٣٤ راهنمای اندپوینت‌سکیوریتی ٥.٣ موجود است.

٢. Remote Install: امکان نصب کلاینت ایجنت کوییک‌هیل از راه دور در این قسمت پیش بینی شده است. راهنمای کامل تر در صفحه ٣٧ نمای اندپوینت‌سکیوریتی ٥.٣ موجود است.

٣. Notify Install: در صورت تمایل می توانید با استفاده از این روش یک ایمیل اطلاع رسانی جهت نصب کوییک‌هیل به کاربران شبکه ارسال نمایید. این ایمیل شامل لینک نصب کوییک‌هیل می‌باشد. در ضمن می توانید این لینک (https://SERVER-IP:9098/install.htm) را از طریق IE بر روی هرکلاینت بدون ارسال ایمیل اجرا و کوییک‌هیل شروع به دانلود و نصب می نماید.

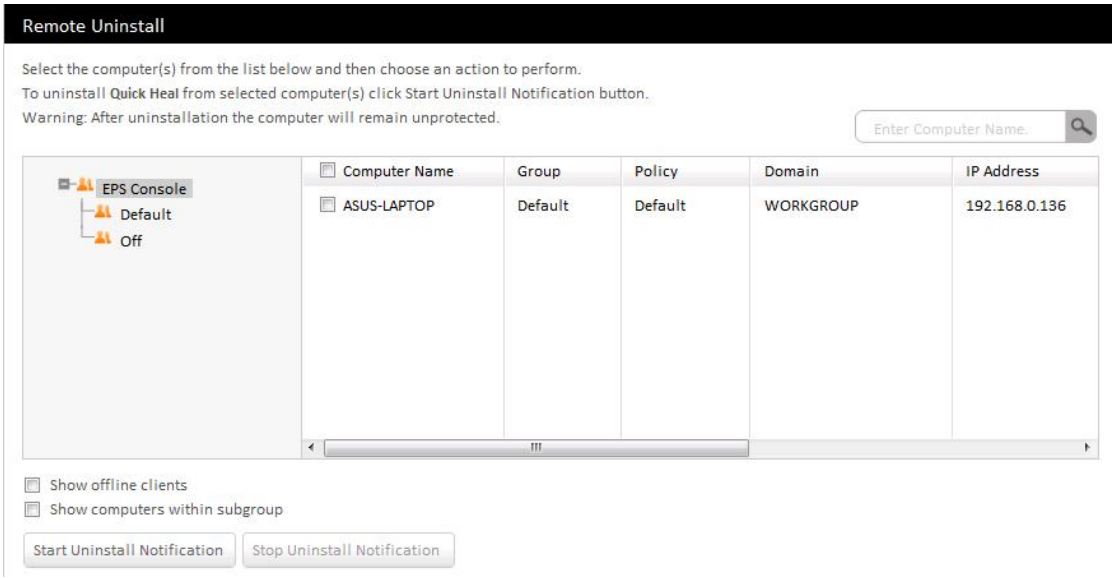
٤. Client Packager: ساده ترین و کارمدترین روش نصب می‌باشد. در این روش با استفاده از برنامه سازنده کلاینت پکیجر یک فایل نصب کننده ایجاد کرده و آن را در شبکه به اشتراک گذاشته و یا از طریق حافظه فلش به کلاینت‌های دیگر منتقل می کنید. فرایند نصب در سمت کلاینت تنها نیاز به دوبار کلیک دارد.

نیاز به هیچ گونه ویزارد، سوال، تنظیمات و... ندارد. راهکار ساده پیشنهادی استفاده از Client Packager می‌باشد.

۵. Login Script: این روش تنها در شبکه های مبتنی بر دامنه قابل اجرا است. در این روش یک فایل QHEPS.BAT ساخته می‌شود. کوییک‌هیل به محض لاگین شدن کلاینتها به سرور دامنه نصب می‌گردد. توضیحات بیشتر در صفحه ٤١ راهنما.

٦. Disk Imaging: در صورتی که نصب ویندوز و نرم افزارها را با استفاده از image انجام می دهید، این گزینه بسیار سودمند می‌باشد. پس از نصب ویندوز و برنامه های کاربردی مورد نیاز، ارتباط شبکه ای کلاینت را قطع کرده و بعد Agent ساخته شده توسط Client Packager را نصب نمایید. سپس اقدام به ساختن ایمیج نمایید. از این پس به محض نصب ایمیج، کوییک‌هیل هم به صورت خودکار نصب و اکتیو می‌گردد.

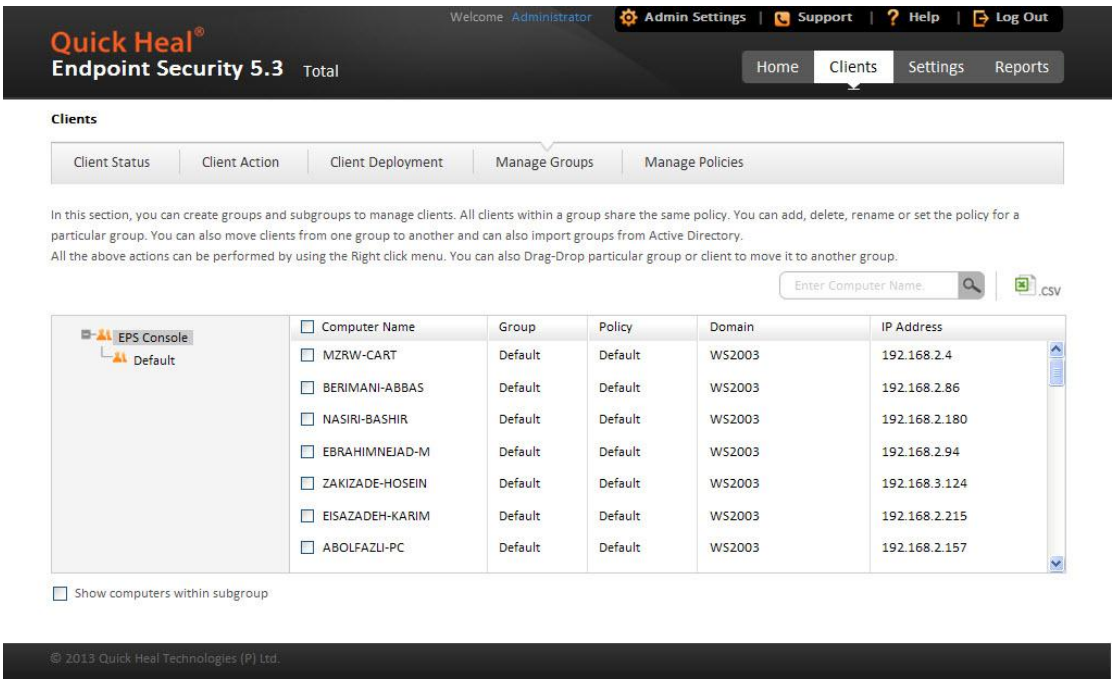
Remote Uninstall: اگر کاربر به هر شکلی کوییک‌هیل را از روی کلاینت حذف نماید، پس از راه‌اندازی مجدد، کوییک‌هیل به صورت خودکار بر روی آن نصب می‌گردد. برای حذف از روی کلاینت ها تنها مدیر می تواند از این گزینه استفاده نماید.



برای حذف، کافی است کلاینت مورد نظر را انتخاب و بر روی دکمه Start Uninstall Notification کلیک کنید، برای انصراف از ارسال دستور حذف، بر روی Stop Uninstall Notification کلیک کنید.

د) سربرگ Manage Groups

این سربرگ مدیریت گروه بندی کلاینت ها را برعهده دارد.



برای گروه بندی و اعمال سیاست گزاری مورد نظر بر روی هر گروه از این سربرگ استفاده می‌شود. درختواره سمت چپ گروه ها و زیرگروه ها را لیست می کند. به صورت پیش فرض همه کلاینت ها عضو گروه Default می‌باشند. با کلیک بر روی هر گروه، کلاینت های عضو آن گروه نمایش داده می‌شوند. برای ایجاد گروه اصلی بر روی EPS Console کلیک راست کرده و Add Group را انتخاب نمایید. در پنجره ی ظاهر شده اسم گروه را وارد نمایید (مثلا Finance). با انتخاب کلاینتها و Drag & Drop آنها به گروه دیگر (آیکن انتقال باید سبز رنگ شود) می توانید گروه کلاینت ها را تغییر دهید. راه دیگر تغییر گروه، کلیک راست برروی کلاینت یا کلاینت ها و انتخاب گزینه Move to Group می‌باشد.

پس از ایجاد و قراردادن کلاینت ها در گروه موردنظر پالیسی باید بر روی این گروه اعمال گردد تا سیاست های خاص بر روی کلاینت های این گروه اجرا شود. برای اعمال سیاستگذاری بر روی گروه کلیک راست کرده و گزینه Set Policy را انتخاب و از منوی بازشونده سیاستی که از قبل ساخته شده را انتخاب می کنیم. اعمال سیاست گذاری پس از ایجاد آن، که در ادامه به آن اشاره خواهد شد، باید صورت پذیرد.

با کلیک راست برروی نام گروه گزینه های زیر نمایش داده می‌شود.

Add Group: می توانید یک زیرگروه به گروه موجود اضافه نمایید.

Delete Group: گروه مورد نظر حذف می‌گردد.

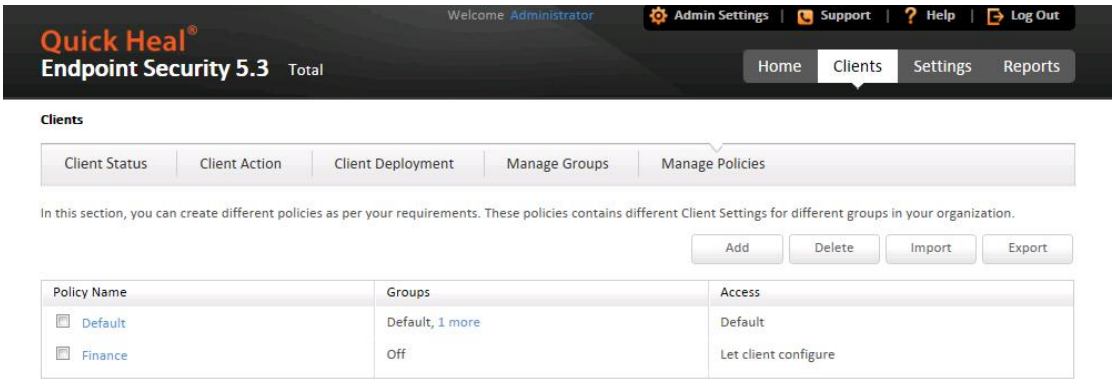
Rename Group: تغییر نام گروه از بخش صورت می‌پذیرد.

Import from Active Directory: در صورتی که می خواهید لیست کلاینت ها را از اکتیو دایرکتوری وارد نمایید، از این گزینه استفاده می کنید.

Set Policy: برای اختصاص پالیسی خاص به این گروه از این گزینه استفاده می‌شود.

هـ) سربرگ Manage Policy

این بخش مدیریت سیاست گذاری کلاینت ها را برعهده دارد.



در این بخش تعاریف مربوط سیاست گذاری آنتی ویروس کلاینت ها صورت می‌پذیرد. همه تنظیمات آنتی ویروس کوییک‌هیل کلاینت ها در این بخش قابل تعریف می‌باشد. با کلیک بر روی اسم هر پالیسی می توانید آنرا ویرایش نمایید.

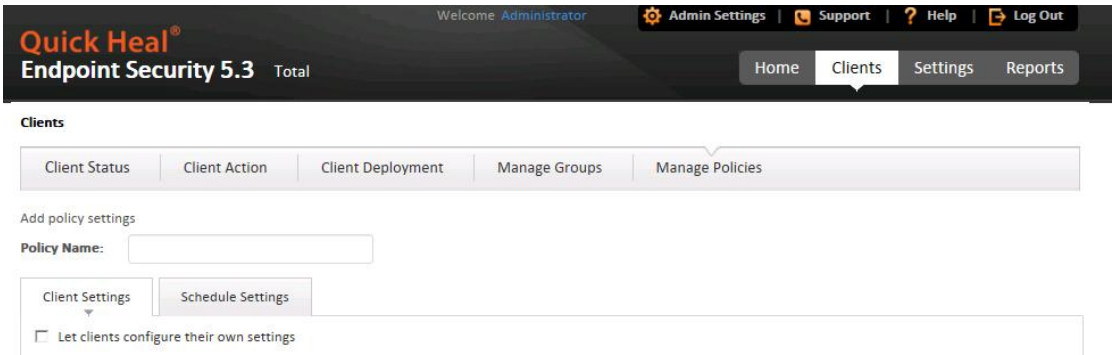
Add: افزودن سیاست گذاری.

Delete: حذف سیاست گذاری.

Import: وارد کردن تنظیمات سیاست گذاری که قبلاً از آن پشتیبان گرفته بودید.

Export: صادر کردن تنظیمات سیاست گذاری برای پشتیبان و یا انتقال به سرور دیگر.

برای افزودن پالیسی جدید بر روی Add کلیک نمایید تا صفحه جدید نمایش داده شود.



در بخش Policy Name، نام پالیسی که می خواهید ایجاد نمایید را وارد نمایید.

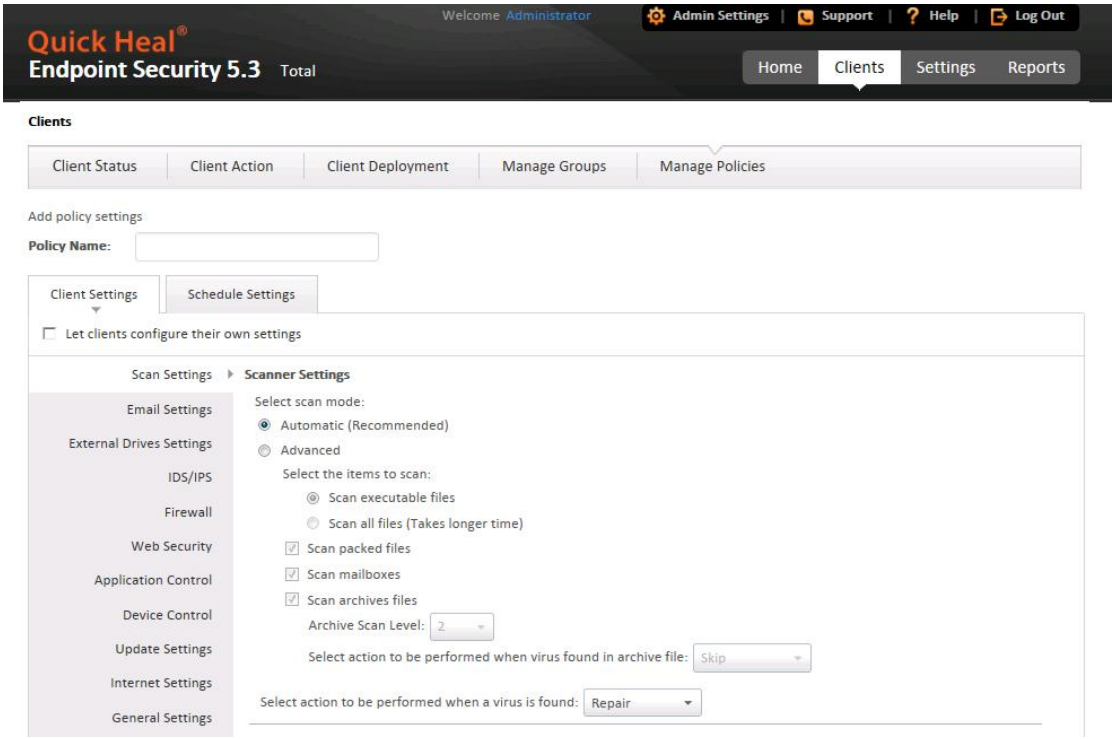
این صفحه دارای دو سربرگ Client Settings (تنظیمات کلاینت) و Schedule Settings (تنظیمات زمانبندی) می‌باشد.

سربرگ Client Settings

این سربرگ شامل تنظیمات اصلی پالیسی کلاینت ها می‌باشد.

Let clients configure their own settings: در صورتی که این گزینه تیک باشد، پیکربندی کلاینت های عضو این سیاستگذاری، از حالت متمرکز خارج شده و به آنها اجازه می دهیم پیکربندی خاص خود را از پای کلاینت داشته باشند. در صورتی که این گزینه تیک نباشد، پیکربندی تنها از سمت سرور صورت می‌پذیرد و اگر کاربر تنظیماتی را روی کلاینت اعمال کند، دوباره به تنظیمات پیش فرض سرور بر می‌گردد.

Scanner Settings



در سمت چپ بخش های مختلف پیکربندی کلاینت قابل مشاهده می‌باشد. بخش اول Scan Settings تنظیمات اسکن آنتی ویروس را شامل می‌شود.

در ابتدای صفحه حالت اسکن تعیین می‌گردد. که به صورت پیش فرض بر روی Automatic (Recommended) می‌باشد. در صورت تمایل می توانید پیکربندی بیشتری را در حالت Advanced انجام دهید.

در انتها گزینه Select action to be performed when a virus is found به صورت پیش فرض بر روی Repair می‌باشد که بیانگر این مطلب می‌باشد که هنگام یافته شدن یک ویروس، آن را تعمیر کند. گزینه های دیگر می تواند حذف (Delete)، صرف نظر (Skip) باشد.

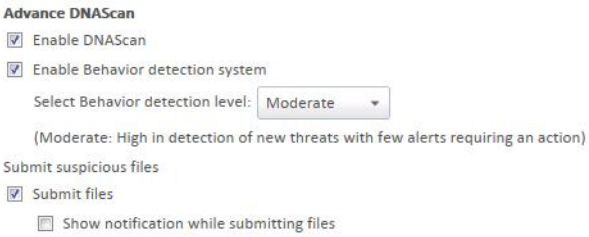
Virus Protection Settings

Load Virus Protection at Startup: اگر این گزینه تیک باشد، در هنگام راه‌اندازی به صورت خودکار آنتی ویروس در سیستم کلاینت بارگذاری و اجرا می‌گردد.

Display alert messages: در صورت فعال بودن پیام های اخطار به کاربر نشان داده می‌شود.

Select action to be performed when a virus is found: در صورت پیدا شدن ویروس توسط محافظت بلادرنگ کوییک‌هیل، آنرا تعمیر (Repair)، حذف (Delete)، صرف نظر (Skip) کند.

Advance DNAScan:



در این بخش تنظیمات مربوط به اسکن پیشرفته مبتنی بر نقشه ژنوم انسانی (DNAScan) که وظیفه اسکن ویروس‌های ناشناخته را دارد، قابل پیکربندی می‌باشد. در واقع کوییک‌هیل مجهز به لابراتوار مجازی بر روی همه کلاینت‌های خود بوده که مانند یک سرور سنسور عمل می کند.

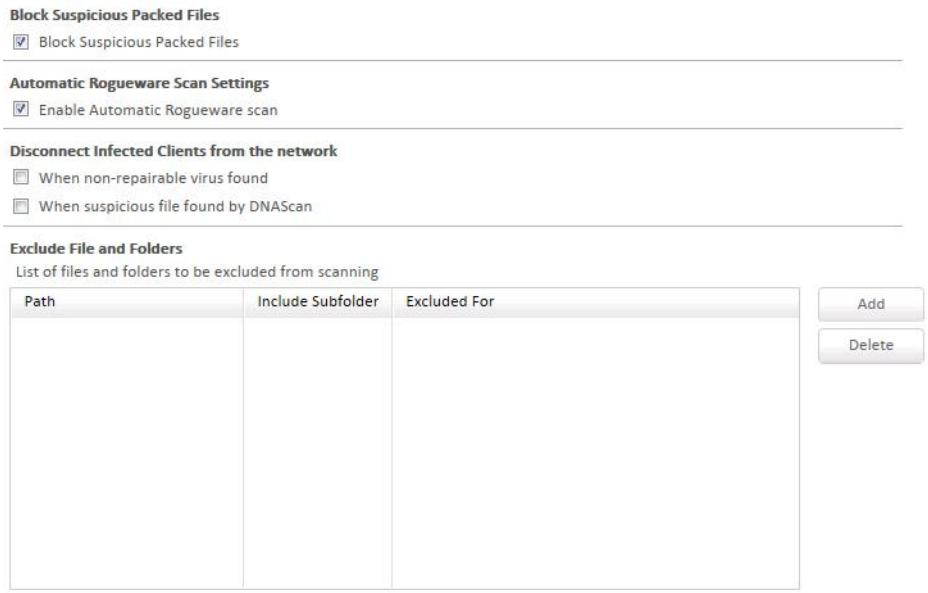
Enable DNAScan: با تیک بودن این گزینه دی.ان.ای اسکن کوییک‌هیل فعال می‌گردد.

Enable Behavior detection system: علاوه بر DNAScan کوییک‌هیل مجهز به هوش مصنوعی سیستم شناسایی بدافزار بر اساس رفتار (رفتارشناسی) می‌باشد که مانع حمله ویروسهای جدید به سیستم می‌گردد. با تیک بودن این گزینه این سیستم فعال می‌گردد.

Select Behavior detection level: در این بخش می توانید سطح تشخیص انجین رفتارشناسی را تعیین نمایید.

Submit suspicious files: در صورتی که انجین های هوشمند کوییک‌هیل به فایلی مشکوک شده باشد و این گزینه تیک باشد، فایل به لابراتوار کوییک‌هیل جهت آنالیز ارسال می‌گردد.

Show notification while submitting files: اگر این گزینه تیک باشد، در هنگام ارسال فایلهای مشکوک، پیغام به کاربر نشان داده می‌شود.



Block Suspicious Packed Files: تیک بودن این گزینه موجب می‌شود که فایل های بسته بندی شده (Packed) مشکوک مسدود گردند.

Enable Automatic Rogueware scan: در صورت تیک بودن این گزینه، آنتی ویروس های جعلی به صورت خودکار اسکن می‌گردند.

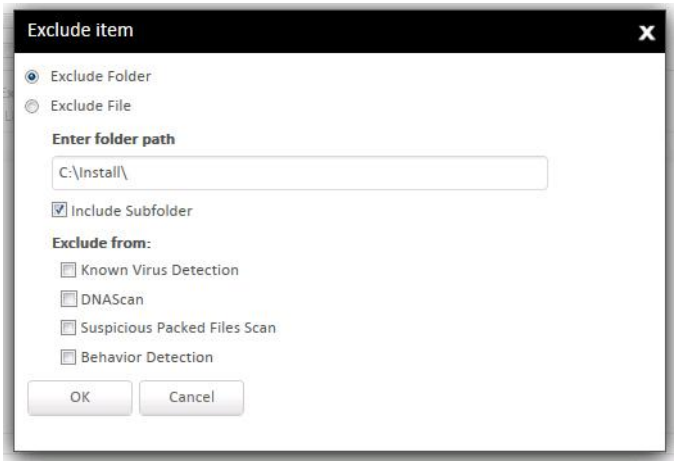
When non-repairable virus found: اگر این گزینه فعال بوده و ویروسی پیدا شود که قابل تعمیر نباشد، کلاینت آلوده از شبکه قطع ارتباط می‌گردد.

When suspicious file found by DNAScan: اگر این گزینه فعال بوده و فایل مشکوکی توسط DNAScan کوییک‌هیل پیدا شود، کلاینت مشکوک از شبکه قطع ارتباط می‌گردد.

Exclude File and Folders

اگر فایل ها یا پوشه هایی دارید که دارای ویروس بوده (مانند بسیاری از فایل های کرک شده) و یا پوشه ی خاصی از برنامه های که تمایل ندارید مورد اسکن قرار گیرند، می توانید فایل یا پوشه را از ویروسیابی شدن استثناء نمایید. پس از افزودن (Add کردن) آن فولدر یا فایل و افزوده شدن در لیست مربوطه، کلاینتهای عضو آن پالیسی فایل یا فولدر موردنظر را اسکن نمی کنند.

پس از کلیک بر روی دکمه Add پنجره ای نمایش داده می‌شود که می توانید تنظیمات مربوط به استثنا شدن را در آن درج نمایید.



اگر می خواهید پوشه ای را از اسکن استثناء کنید گزینه Exclude Folder و اگر می خواهید فایل خاصی را استثناء کنید گزینه Exclude File را انتخاب کنید.

Enter folder path: مسیر فولدر مورد نظر را در این بخش وارد می کنید.

Include Subfolder: در صورتی که پوشه دارای زیرپوشه هایی باشد، تیک بودن این گزینه، آن زیرپوشه ها را نیز از اسکن مستثنی می کند.

Exclude from: در این بخش موارد استثنا مشخص می‌گردد.

Known Virus Detection: با تیک بودن این گزینه همه ویروس های شناخته شده از اسکن استثنا می‌گردند.

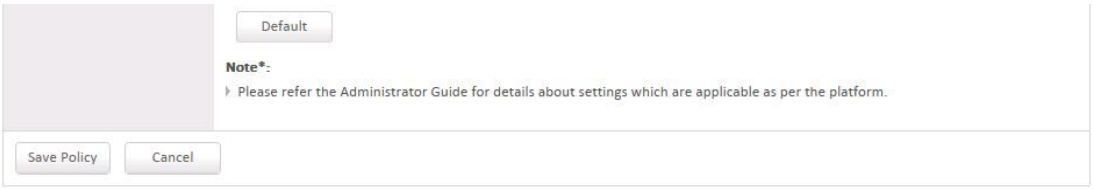
DNAScan: عدم پویش DNAScan از پوشه یا فایل مورد نظر در این بخش تعیین می‌گردد.

Suspicious Packed Files Scan: استثنا شدن از اسکن فایل های بسته ای مشکوک.

Behavior Detection: استثنا شدن از انجین رفتارشناسی کوییک‌هیل.

Exclude Extensions:

در این بخش می توانید پسوندهای فایل خاصی را از اسکن استثنا کنید. مثلا می توانید jpg یا هر پسوند خاصی (مثلا پسوند ویژه برنامه سفارشی خود) را از اسکن شدن استثنا نمایید. با درج نام و زدن دکمه Add می توانید پسوند جدید را وارد نمایید.

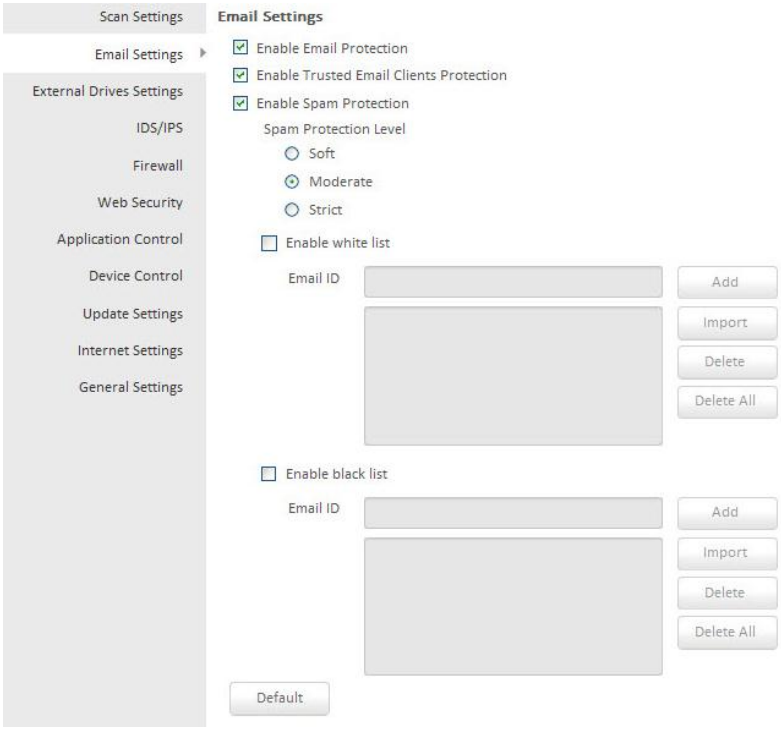


Default: تغییرات تنظیمات صورت گرفته را می توانید به حالت پیش فرض بر گردانید.

Save Policy: برای ذخیره کردن پالیسی جاری باید بر روی این دکمه کلیک کرده و منتظر باشید تا پیغام موفقیت در ذخیره سازی پالیسی نمایش داده شود.

Email Settings

در این بخش می توانید تنظیمات مربوط به محافظت ایمیل کاربران را انجام دهید.



Enable Email Protection: فعال بودن این گزینه سبب فعال شدن محافظت ایمیل می‌گردد.

Enable Trusted Email Clients Protection: با تیک بودن این گزینه محافظت از کلاینت های ایمیل مطمئن (مانند Outlook) فعال می‌گردد.

Enable Spam Protection: با فعال بودن این گزینه محافظت هرزنامه و اسپم صورت می‌گیرد.

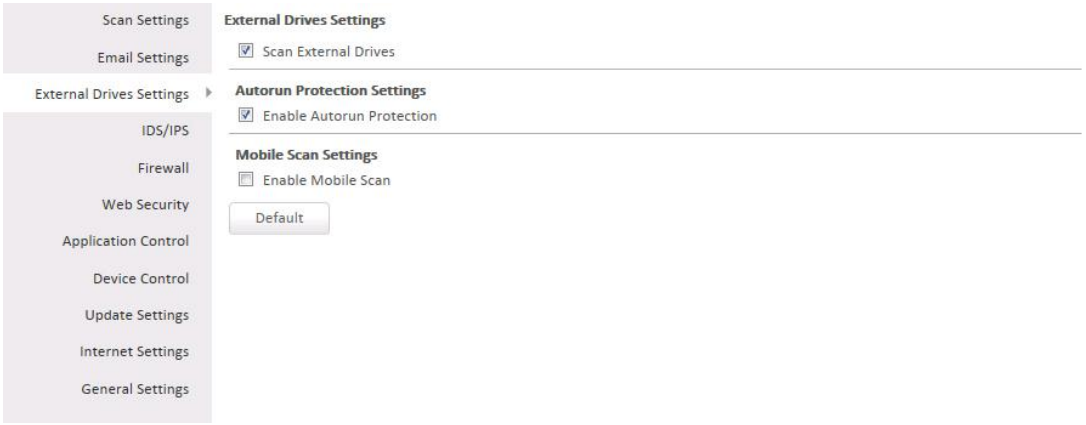
Spam Protection Level: این گزینه سطح حفاظت و دقت آنتی اسپم که می توان نرم (Soft)، متوسط (Moderate) و یا سخت (Strict) باشد را تعیین می کند.

Enable white list: با تیک کردن این گزینه لیست سفیدی از ایمیل ها را می توانید تعیین نمایید که از آنتی اسپم مستثنی شده و همواره به عنوان ایمیل سالم وارد کلاینت کاربر گردد.

Enable black list: با تیک کردن این گزینه لیست سیاهی از ایمیل ها را می توانید تعیین نمایید که آنتی اسپم همواره آنها را به عنوان ایمیل مخرب و هرزنامه در نظر می‌گیرد.

External Drives Settings

این بخش شامل تنظیمات مربوط به اسکن دستگاههای خارجی می‌باشد.



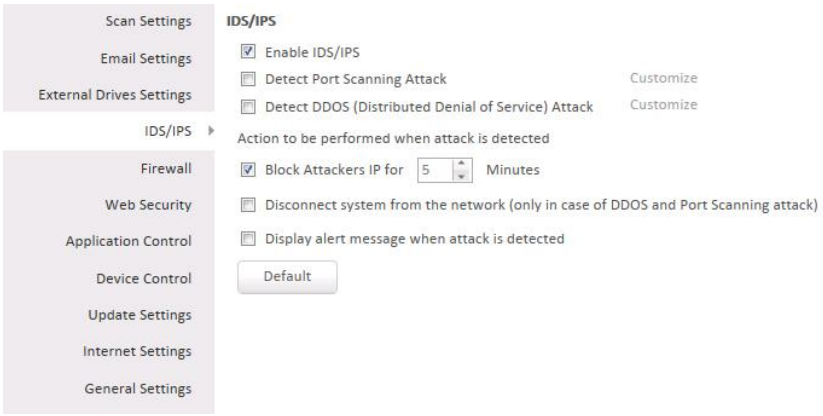
Scan External Drives: در صورتی که این گزینه تیک باشد، به محض اتصال فلش یا حافظه های USB، کوییک‌هیل به صورت خودکار اقدام به اسکن آنها می کند.

Enable Autorun Protection: اگر این گزینه تیک باشد، مخافظت آتوران فعال شده و اجازه اجرای تروجان‌های آتوران از حافظه های جانبی را نمی دهد.

Enable Mobile Scan: در صورت تیک بودن این گزینه، ویژگی اسکن موبایل PC2Mobile به کلاینتهای عضو گروه مرتبط با این پالیسی فعال می‌گردد. این ویژگی انحصاری کمک می کند تا کوییک‌هیل بدون نصب بر روی گوشی موبایل، اقدام به ویروسیابی سیستم عامل و حافظه های اصلی و جانبی کرده و کلیه ویروس های موبایلی و کامپیوتری را از روی آن پاکسازی نماید.

IDS/IPS

نسل جدید IDS/IPS کوییک‌هیل کمک می کند تا پکت های شبکه ورودی و خروجی کلاینت، مورد تحلیل قرار گرفته و مانع اجرای حملات و نفوذ به سیستم های رایانه ای گردد. نسل اول فایروال که کنترل حملات را تنها بر روی پورت انجام می داد، برای برقراری ارتباط باید همواره پورت هایی بر روی کلاینت باز می‌بود. از اینرو IDS/IPS رفتار پکت ها را بررسی و در صورت مشاهده رفتارهای مشکوک و مخرب مانع اجرای حملات و نفوذ می‌گردد.



Enable IDS/IPS: با فعال بودن این گزینه ویژگی IDS/IPS فعال می‌گردد.

Detect Port Scanning Attack: حملات اسکن و پویش پورت را شناسایی و از آن جلوگیری می کند. با کلیک بر روی Customize، می توانید سطح محافظت و آدرس های IP و پورت های مجاز – استثنا کردن– را سفارشی نمایید.

Detect DDOS (Distributed Denial of Service) Attack: شناسایی و محافظت در برابر حملات توزیع شده انکار سرویس با تیک بودن این گزینه فعال می‌گردد.

Action to be performed when attack is detected: عکس العملی که در هنگام شناسایی حملات صورت می‌گیرد در این بخش تعیین می‌گردد.

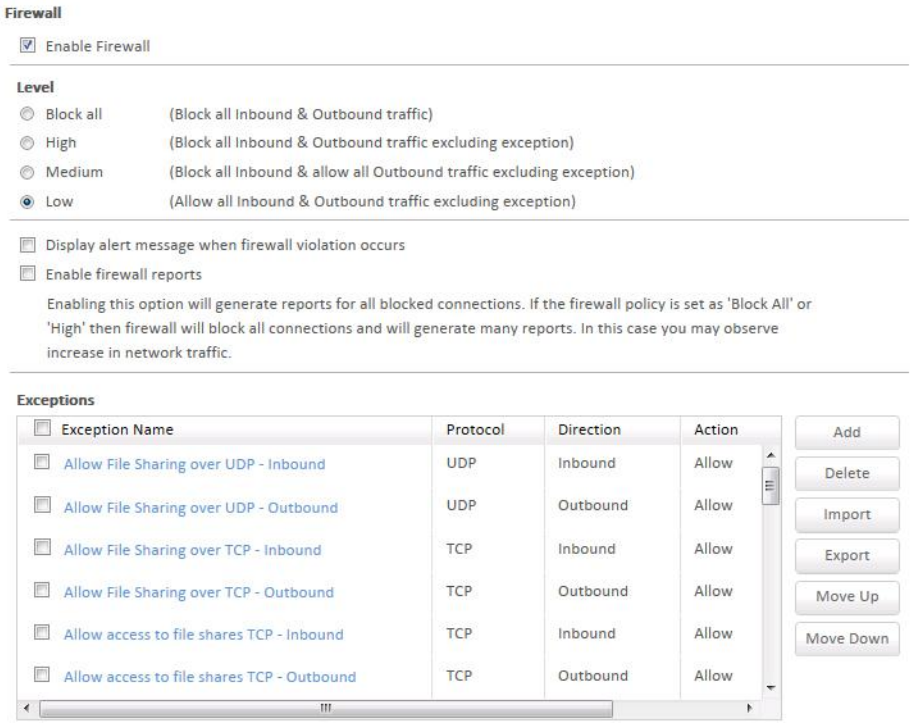
Block Attackers IP for: در این بخش می توانید آدرس های IP مهاجم را برای مدت زمانی به دقیقه مسدود نمایید.

Disconnect system from the network (only in case of DDOS and Port Scanning attack): اگر این گزینه تیک باشد در هنگام حملات اسکن پورت و DDOS، سیستم از شبکه قطع ارتباط می‌گردد.

Display alert message when attack is detected: در صورت بروزحملات پیغام مناسب به کاربر نشان داده شود.

Firewall

تنظیمات مربوط به فایروال کوییک‌هیل بر روی کلاینت ها در این بخش تعیین می‌گردند. ادمین می تواند با استفاده از رول های پیش فرض و یا تعریف رول جدید پورت هایی را برای کلاینت موردنظر بسته یا باز نماید.



Enable Firewall: تیک کردن این گزینه موجب فعال شدن فایروال بر روی کلاینت می‌گردد.

Level: در این بخش سطح امنیت فایروال تعیین می‌گردد.

Block all (Block all Inbound & Outbound traffic): کل ترافیک های ورودی و خروجی به همه پورت‌ها را مسدود می کند.

High (Block all Inbound & Outbound traffic excluding exception): همه ترافیک های ورودی و خروجی را مسدود می کند بجز ترافیک هایی که در حالت استثنا قرار گرفته اند.

Medium (Block all Inbound & allow all Outbound traffic excluding exception): همه ترافیک‌های ورودی را مسدود کرده و همه ترافیک های خروجی و ترافیک هایی که در حالت استثنا قرار گرفته اند را مجاز می کند.

Low (Allow all Inbound & Outbound traffic excluding exception): همه ترافیک های ورودی و وخروجی و همچنین استثناها را مجاز می کند.

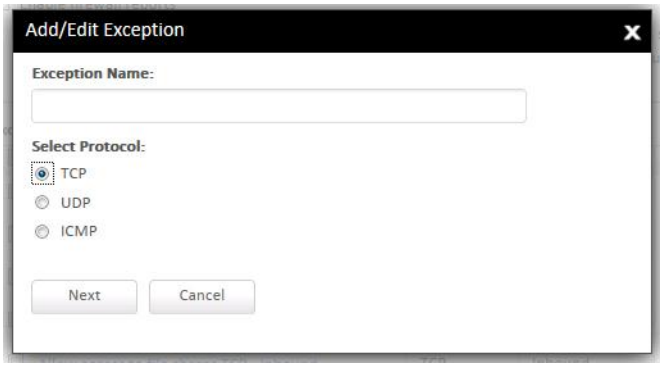
Display alert message when firewall violation occurs: اگر این گزینه فعال باشد، در هنگام حملات، فایروال پیغام اخطار مناسب به کاربران نشان می دهد.

Enable firewall reports: در صورت فعال بودن، گزارشات فایروال به صورت مجتمع در کنسول مدیریتی ثبت می‌گردد.

Exceptions: استثناهای فایروال در این بخش مدیریت می‌گردند. به صورت پیش فرض چندین رول و قانون پرکاربرد برای استثنا شدن در نظر گرفته شده است مانند ICMP برای فعال نمودن Ping یا DHCP و...

در جدول استثناها نام استثنا (Exception Name)، پروتکل (Protocol) که می تواند TCP/UDP/ICMP باشد، جهت (Direction) که می تواند ورودی (Inbound) یا خروجی (Outbound) باشد، اقدام مربوطه (Action) که می‌تواند مجاز (Allow) یا غیرمجاز(Deny) و وضعیت (Status) که می تواند فعال (On) یا خاموش (Off) باشد قابل مشاهده است. با کلیک بر روی وضعیت جاری می توانید آنرا فعال ON و یا غیر فعال OFF کنید.

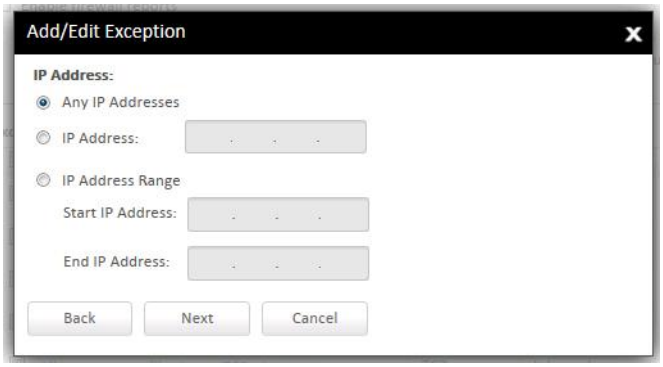
Add: برای افزودن رول استثنای جدید از این دکمه استفاده می‌شود. پس از فشردن این دکمه، صفحه ای باز می‌گردد که می توانید پورت خاصی را مجاز یا غیر مجاز نمایید. به عنوان مثال شما از برنامه یک اتوماسیون اداری استفاده می کنید که از پورت خاصی استفاده می کند، برای استفاده از آن باید پورتهای مربوطه به صورت مجاز تعریف گردند. با کلیک بر روی Add پنجره زیر ظاهر می‌گردد:



Exception Name: نام یا شرحی برای استثنا وارد نمایید.

Select Protocol: در این بخش نوع پروتکل را انتخاب می کنید. نوع پروتکل می تواند TCP یا UDN یا ICMP باشد. اگر می خواهید دو یا سه پروتکل را فعال کنید باید برای هر پروتکل یک رول مجزا تعریف کنید. سپس دکمه Next را کلیک کنید.

Select Direction: در این بخش جهت ترافیک را تعیین می کنید. جهت ترافیک می تواند ورودی (Inbound)، خروجی (Outbound) یا هر دو جهت باشد. سپس دکمه Next را کلیک کنید.

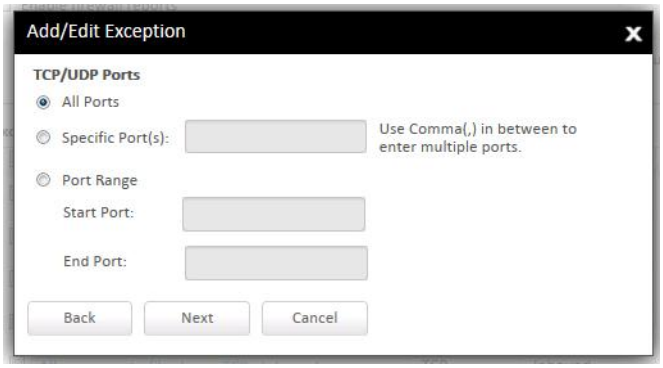


IP Address: در این بخش آدرس های IP که قانون فایروال باید بر روی آنها اعمال شود را مشخص می کنید.

Any IP Addresses: اگر این گزینه تیک باشد این قانون بر روی همه آدرس های IP که کلاینت با آنها مرتبط است، اعمال می‌گردد.

IP Address: می توانید فقط یک IP خاص را تعیین کنید تا تنها این رول بر روی آن اعمال گردد.

IP Address Range: اگر این گزینه تیک باشد، یک محدوده IP را برای اعمال قانون تعیین می کنید. آدرس IP شروع (Start IP Address) و آدرس IP پایان (End IP Address) را در فیلدهای مربوطه وارد نمایید. سپس دکمه Next را کلیک کنید.

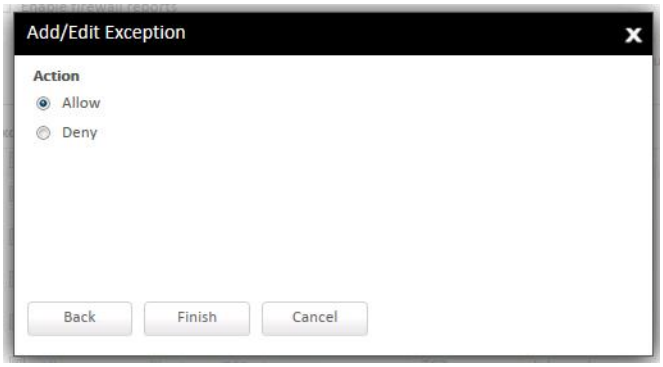


TCP/UDP Ports: در این بخش پورتهایی را که قانون فایروال باید بر روی آنها اعمال شود، مشخص نمایید.

All Ports: اگر این گزینه تیک باشد این قانون بر روی همه پورتها که کلاینت با آنها مرتبط است، اعمال می‌گردد.

Specific Port(s): می توانید یک یا چند پورت خاص را تعیین کنید تا تنها این رول بر روی آن اعمال گردد. از کاما (,) برای جداسازی چند پورت استفاده کنید . (مثلا اگر می خواهید رول را بر روی پورت های ۸۰ و ٤٤٣ اعمال کنید می‌نویسید 80,443)

Port Range: اگر این گزینه تیک باشد، یک محدوده | پورت را برای اعمال قانون تعیین می کنید. پورت شروع (Start Port) و پورت پایان (End Port) را در فیلدهای مربوطه وارد نمایید. سپس دکمه Next را کلیک کنید.



Action: در انتها تعیین می کنید که نوع اقدام چگونه باشد. Allow به معنای مجاز کردن رول و Deny به معنای غیرمجاز کردن رول باشد. اگر می خواهید دسترسی به پورت و یا IP خاصی را باز کنید باید Allow انتخاب گردد.

در انتها بر روی دکمه Finish کلیک کنید تا رول ساخته و اعمال گردد.

Delete: با انتخاب رول دلخواه از جدول استثناها و کلیک بر روی این دکمه، رول مربوطه حذف می‌گردد.

Import: با کلیک بر روی این دکمه می توانید از رول هایی که قبلا صادر شده در این کنسول استفاده نمایید.

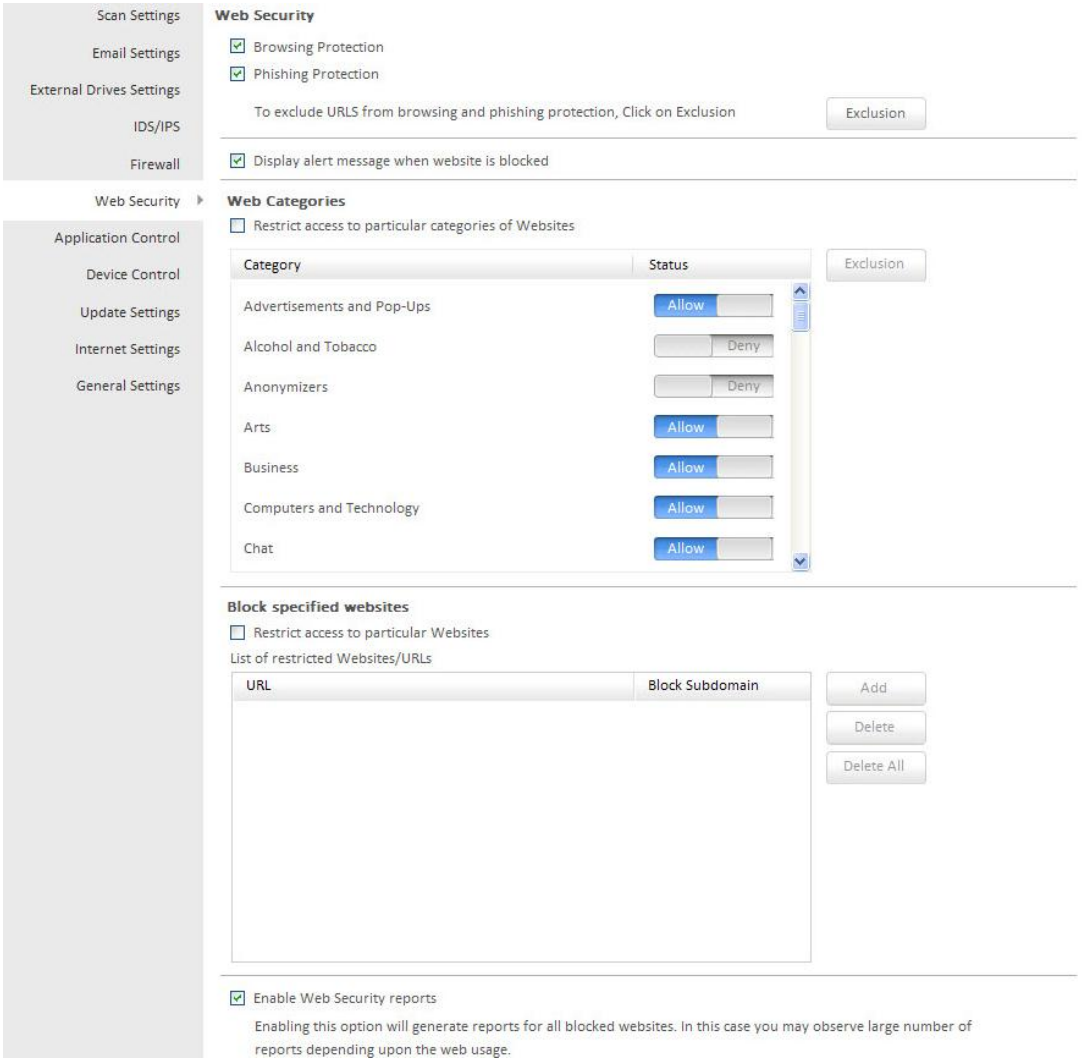
Export: با انتخاب یک یا چند رول و کلیک بر روی این گزینه می توانید یک پشتیبان از رول ها گرفته و آنها را بر روی کنسول های دیگر یا در زمان نصب مجدد استفاده نمود.

Move Up: با انتخاب رول دلخواه و کلیک بر روی این دکمه می توانید اولویت اجرای رول را بالاتر ببرید.

Move Down: با انتخاب رول دلخواه و کلیک بر روی این دکمه می توانید اولویت اجرای رول را کاهش دهید.

Web Security

در این بخش امنیت وب تعیین می‌گردد. فعال سازی محافظت های امنیتی و نیز دسته بندی سایتها و مسدود یا مجاز کردن سایتهای خاص در این بخش قرار دارند.



Browsing Protection: با فعال بودن این گزینه محافظت مرورگر شروع به کار کرده و از کاربران در برابر سایت‌های آلوده محافظت می کند.

Phishing Protection: تیک بودن این گزینه موجب می‌گردد تا سایت های کلاهبردارانه و فیشینگ مسدود شوند.

Exclusion: با کلیک بر روی این دکمه، می توانید سایت خاصی را از اسکنر فیشینگ مستثنی کنید.

Display alert message when website is blocked: هنگامی که کاربر قصد مشاهده یک سایت مسدود شده را دارد، پیام اخطار مناسب نمایش داده شود.

Web Categories

در این بخش دسته بندی سایت ها قابل مدیریت می‌باشد. می توانید دسته خاصی از وب سایت ها (مثلا بازی) را برای کاربران مسدود نمایید. همچین امکان مسدود کردن و باز کردن یک سایت خاص نیز مهیا می‌باشد.

Restrict access to particular categories of Websites: با تیک بودن این گزینه می توانید دسترسی به دسته بندی خاصی از وب سایت ها را محدود نمایید. نشان Allow در ستون Status نشان دهنده مجاز بودن و Deny نمایانگر غیرمجاز بودن آن دسته بندی است. با کلیک بر روی این دکمه می توانید وضعیت را به مجاز و غیرمجاز تغییر دهید.

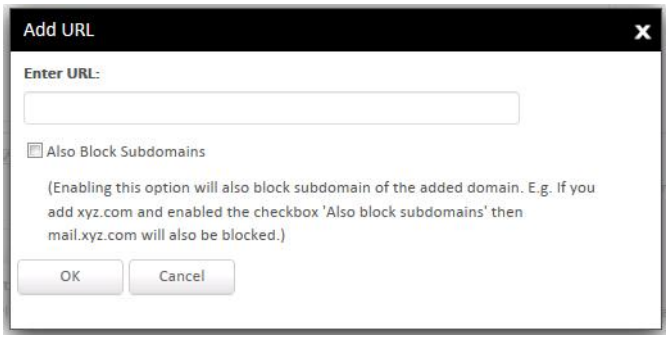
Exclusion: با کلیک بر روی این دکمه، می توانید سایت خاصی که عضو گروه بوده، را از عمل پیش بینی شده برای آن گروه مستثنی کنید. مثلا همه سایت های بازی بسته، بجز یک سایت خاص. پس از کلیک پنجره ای باز می‌شود که می‌توانید نام سایت را در آن وارد و با تیک کردن Also Exclude Subdomains همه زیردامنه های آن سایت را نیز مستثنی نمایید.

Block specified websites

در این بخش می توانید سایت های مورد نظرتان را –خارج از اینکه عضو کدام دسته قرار دارند– مسدود نمایید.

Restrict access to particular Websites: با تیک کردن این گزینه دسترسی به سایت های تعریف شده در این بخش مسدود می‌گردد.

با فشردن دکمه Add پنجره زیر برای وارد کردن آدرس سایت موردنظر جهت مسدود شدن نمایش داده می‌شود:



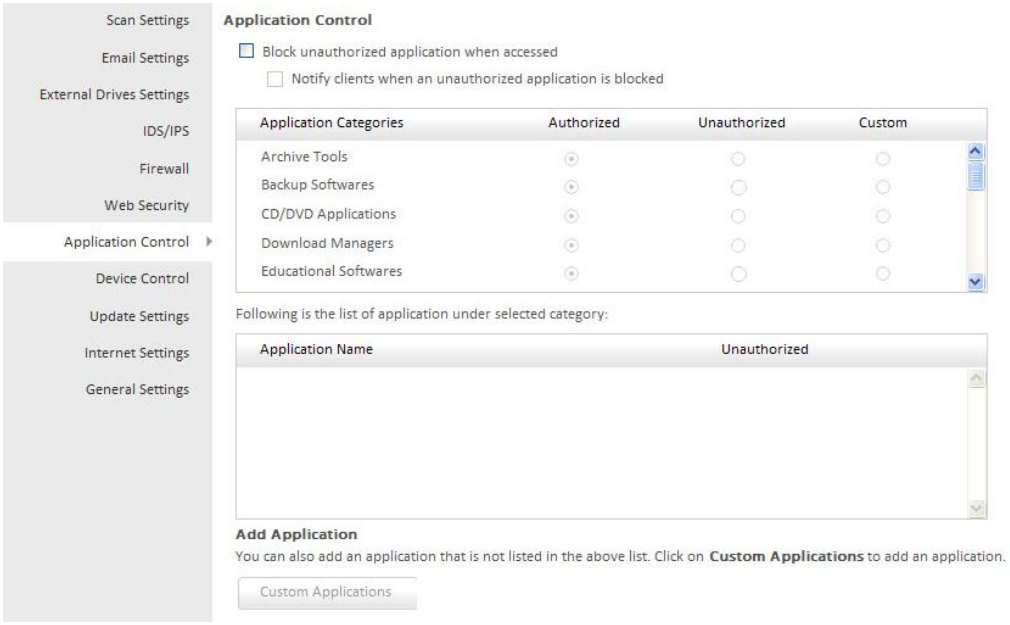
Enter URL: آدرس سایتی را که می خواهید از دسترس کاربران خارج شود را در این بخش وارد می نمایید. (مثلا yahoo.com)

Also Block Subdomains: در صورتی که می خواهید همه زیردامنه های یک سایت هم از دسترس خارج شوند، این گزینه را تیک نمایید. (مثلا mail.yahoo.com)

Enable Web Security reports: در صورتی که تمایل دارید گزارشی از درخواست های کاربران برای مشاهده سایت های مسدود شده دریافت نمایید، این گزینه را فعال کنید.

Application Control

یکی از ویژگی های کوییک‌هیل اندپوینت‌سکیوریتی، کنترل برنامه ها (Application Control) می‌باشد. این ویژگی امکان مسدود کردن برنامه های کاربران را به صورت کامل فراهم می آورد. به عنوان مثال مدیر سیستم می تواند دسترسی به برنامه های دانلود اینترنتی (مانند IDM) یا بازی یا Babylon و یا برخی نرم افزارهای خاص سفارشی را مسدود نماید. یکی از ویژگی های این قابلیت، امکان تعریف فایل خاص می‌باشد. بدین معنی که اگر کاربران از نسخه های غیرقانونی نرم افزار (مانند IDM کرک شده) استفاده نمایند، چون امضای فایل اجرایی مربوطه دچار تغییراتی شده است، کنترل برنامه امکان شناسایی آن را از دست می دهد، اما کوییک‌هیل ویژگی معرفی برنامه سفارشی (Custom Applications) را ارائه داده است که می توانید فایل exe. خود را به کوییک‌هیل معرفی نمایید تا آن را از دسترس خارج نماید.

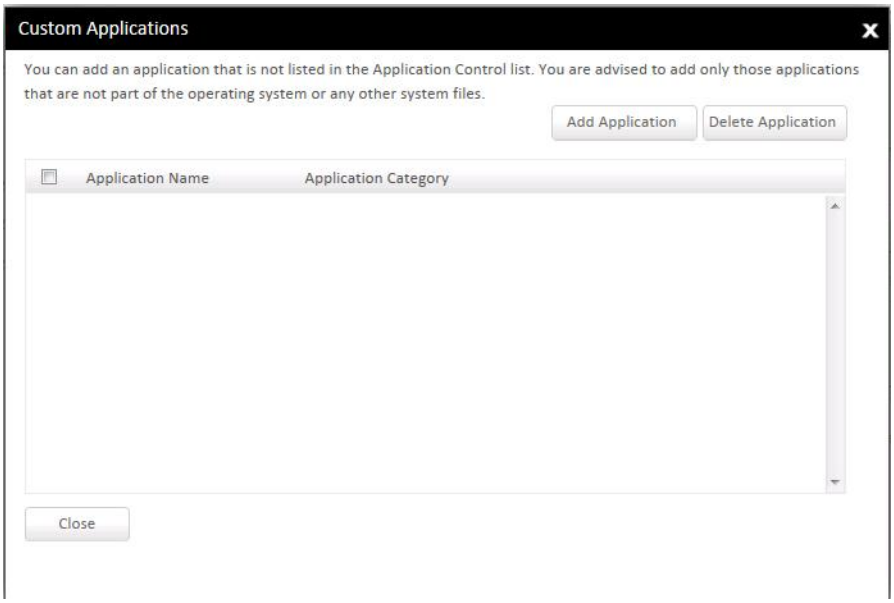


Block unauthorized application when accessed: برای فعال کردن قابلیت کنترل برنامه ها این گزینه باید تیک باشد. با فعال بودن این قابلیت، اجرای برنامه های غیر مجاز (unauthorized) برای کاربران ناممکن می‌گردد.

Notify clients when an unauthorized application is blocked: در صورتی که این گزینه تیک باشد، و کاربر بخواهد برنامه غیرمجازی را اجرا کند، پیغام مناسب مسدودی برنامه توسط مدیریت به او نشان داده خواهد شد.

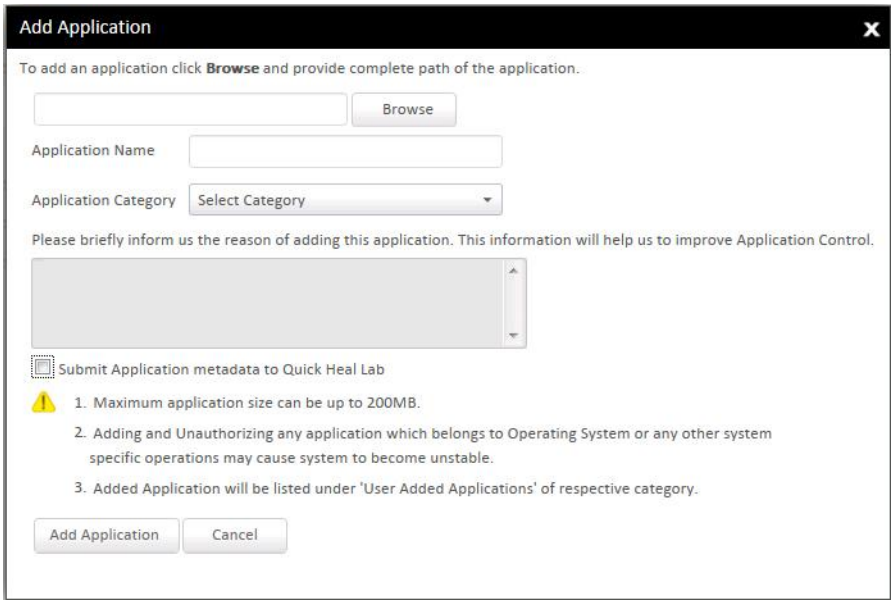
Application Categories: در این جدول دسته بندی برنامه های مختلف وجود دارد. با انتخاب گزینه Authorized، Unauthorized یا Custom در باکس بالایی می توانید کل نرم افزارهای آن گروه را مجاز، غیرمجاز و یا سفارشی نمایید. در صورتی که مایلید یک یا چند برنامه عضو آن گروه را غیرمجاز کنید باید گزینه Custom آن گروه را انتخاب و برنامه موردنظر را از باکس پایینی غیرمجاز یا مجاز نمایید.

Custom Applications: در صورتی که برنامه مورد نظر شما در لیست پیش فرض وجود ندارد و یا فایل اجرایی برنامه تان به هر دلیلی (مثلا کرک شدن) با فایل اجرایی استاندارد تفاوت دارد، می توانید آن برنامه را خودتان به کوییک‌هیل معرفی نمایید تا فیلتر صورت پذیرد. پس از زدن این دکمه، پنجره زیر باز می‌شود.



Delete Application: با انتخاب برنامه و کلیک بر روی این دکمه، برنامه جاری از لیست حذف می‌گردد.

Add Application: برای افزودن برنامه جدید از این دکمه استفاده می‌شود. پس از فشردن آن پنجره دیگری برای انتخاب و افزودن برنامه باز می‌گردد.



برای افزودن و معرفی فایل اجرایی دکمه Browse را فشرده و فایل مورد نظر را از کامپیوتر خود انتخاب کنید.

Application Name: نام برنامه را به صورت دلخواه وارد نمایید.

Application Category: دسته بندی و گروه برنامه مورد نظر را می توانید از لیست پیش فرض انتخاب کنید تا این برنامه در آن گروه قرار گرفته و امکان کنترل آن فراهم گردد. می توانید این برنامه را در گروه دیگر Other قرار دهید و کنترل را بر روی این گروه انجام دهید.

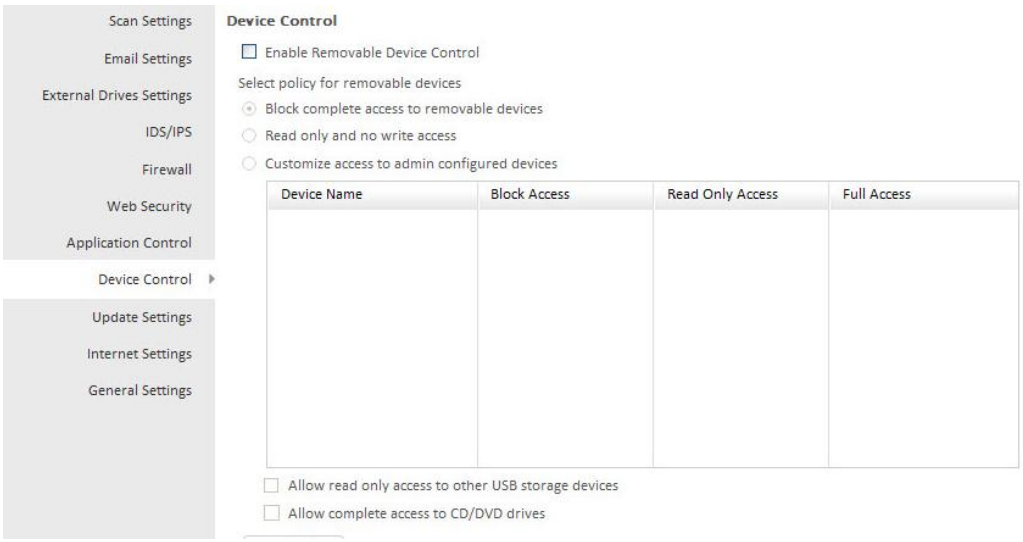
Submit Application metadata to Quick Heal Lab: در صورت تمایل می توانید فایل را به لابراتوار کوییک‌هیل ارسال نمایید. در فرم بالای این گزینه علت افزودن برنامه را به کوییک‌هیل توضیح می دهید. (این بخش قابل صرف نظر می‌باشد)

Add Application: برنامه را به لیست گروه با زدن این دکمه اضافه کنید.

پس از تایید و خروج از افزودن برنامه کاربردی سفارشی، می توانید گروهی را که برنامه به آن اضافه شده (مثلا Others)، غیرمجاز نمایید. همچنین می توانید آن گروه را در حالت Custom قرار داده و در باکس دومی فقط برنامه موردنظرتان را غیرمجاز کنید.

Device Control

در این بخش می توانید حافظه های USB (مانند فلش ها، هاردهای اکسترنال و...) و نیز CD/DVD-Romها را مدیریت نمایید. امکان مسدود کردن کامل، فقط خواندنی کردن، مسدود کردن همه فلش ها بجز فلش های معرفی شده در این بخش درنظر گرفته شده است. لازم به ذکر است این مسدود سازی مانع استفاده از چاپگرها اسکنرهای USB نمی‌گردد.



Enable Removable Device Control: برای فعال شدن بخش مدیریت کنترل ابزار این گزینه باید تیک باشد.

Select policy for removable devices: در این بخش می توانید سیاست مورد نظر برای دستگاههای جداشدنی (حافظه های USB و درایوهای نوری) را تعیین نمایید.

Block complete access to removable devices: با انتخاب این گزینه، دسترسی به حافظه های USB به صورت کامل قطع می‌گردد. از این پس کاربر نمی تواند از فلش های USB استفاده نماید.

Read only and no write access: در صورت انتخاب این گزینه، تنها امکان خواندن از درایو فلش ممکن بوده ولی نمی توان اطلاعاتی از روی کلاینت را وارد فلش نمود (جلوگیری از سرقت اطلاعات).

Customize access to admin configured devices: اگر می خواهید دسترسی فلش ها را به صورت سفارشی مدیریت کنید این گزینه را انتخاب کنید. به عنوان مثال می توانید همه فلش ها را مسدود کرده اما فلش های خاص (مانند فلش مدیر) را مجاز به استفاده کنید. همچنین می توانید دسترسی به درایوهای CD/DVD را نیز محدود و یا مجاز کنید.

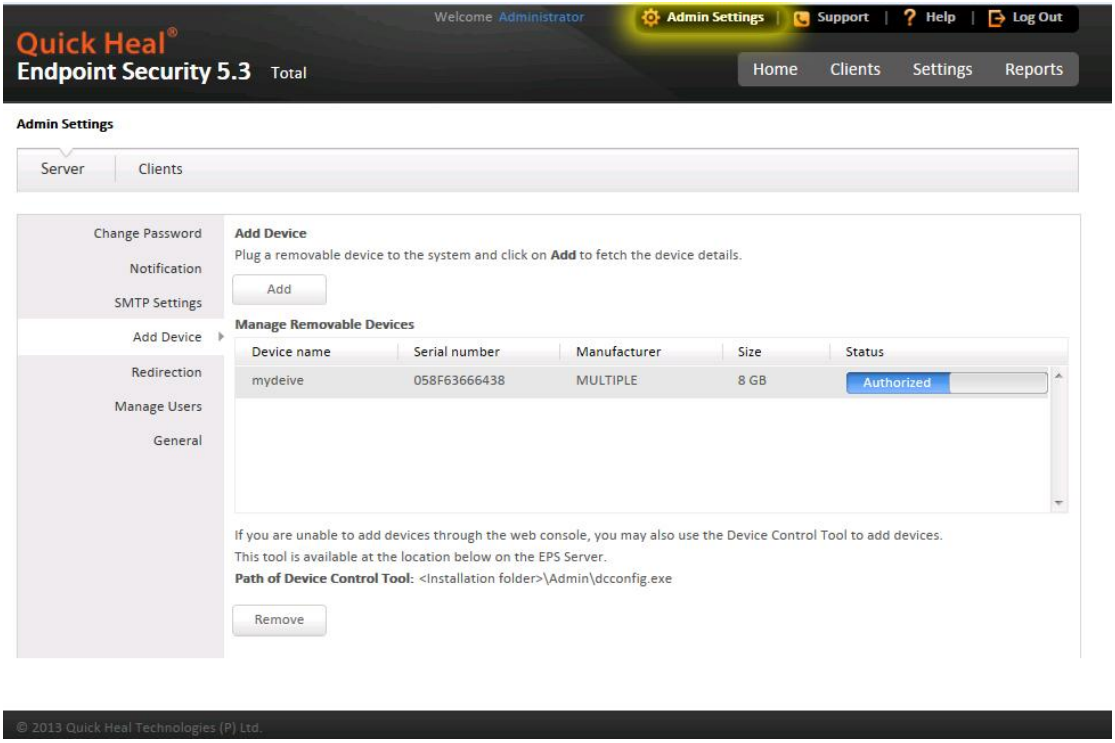
با انتخاب نام دیوایس افزوده شده در لیست، می توانید آن دیوایس خاص را مسدود (Block Access)، فقط خواندنی (Read Only Access)، و یا دسترسی کامل و بدون محدودیت (Full Access) اعطا کنید.

Allow read only access to other USB storage devices: با تیک بودن این گزینه، امکان فقط خواندنی به حافظه های USB دیگر –به غیر از آنهایی که به لیست افزوده شده اند– اعطا می‌گردد.

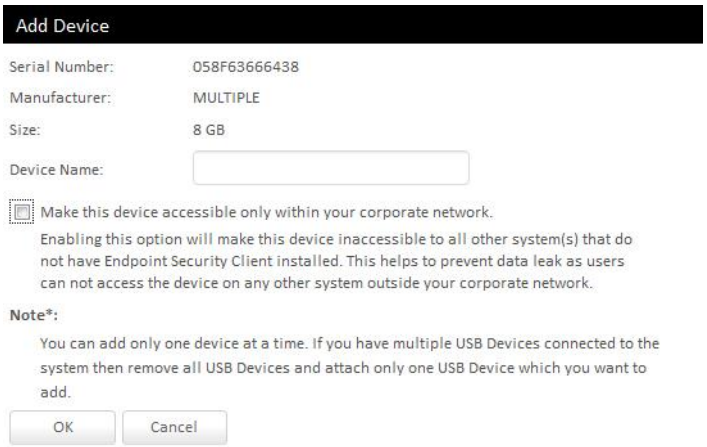
Allow complete access to CD/DVD drives: با فعال بودن این گزینه دسترسی به درایو های CD/DVD مجاز می‌گردد.

معرفی حافظه USB فلش به لیست Device Control

در این بخش می توانید دیوایس ها (حافظه USB) خود را مدیریت کنید. این بخش از طریق منوی بالای صفحه Admin Settings قابل دسترس است.



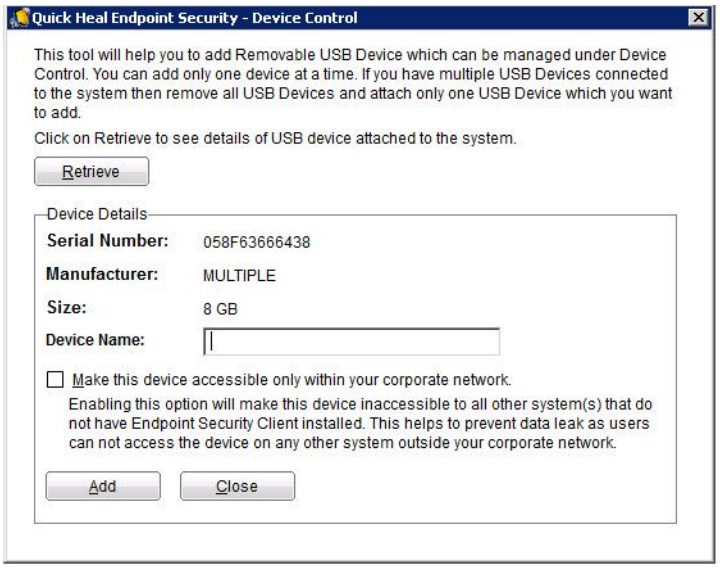
Add: با کلیک بر روی این دکمه می توانید ابزار USB خود را به اندپوینت سکیوریتی معرفی کنید.



Make this device accessible only within your corporate network: اگر این گزینه فعال باشد، این دیوایس تنها بر روی شبکه سازمان فعال خواهد بود و قابلیت استفاده در مکان های دیگر را ندارد (جلوگیری از سرقت اطلاعات).

نکته: فایل سیستم فلش دیسک باید NTFS باشد.

راه دیگر افزودن ابزار حافظه USB، استفاده از برنامه اجرایی تحت ویندوز می‌باشد که در مسیر نصب کوییک‌هیل در دسترس می‌باشد:



اجرای برنامه از مسیر:

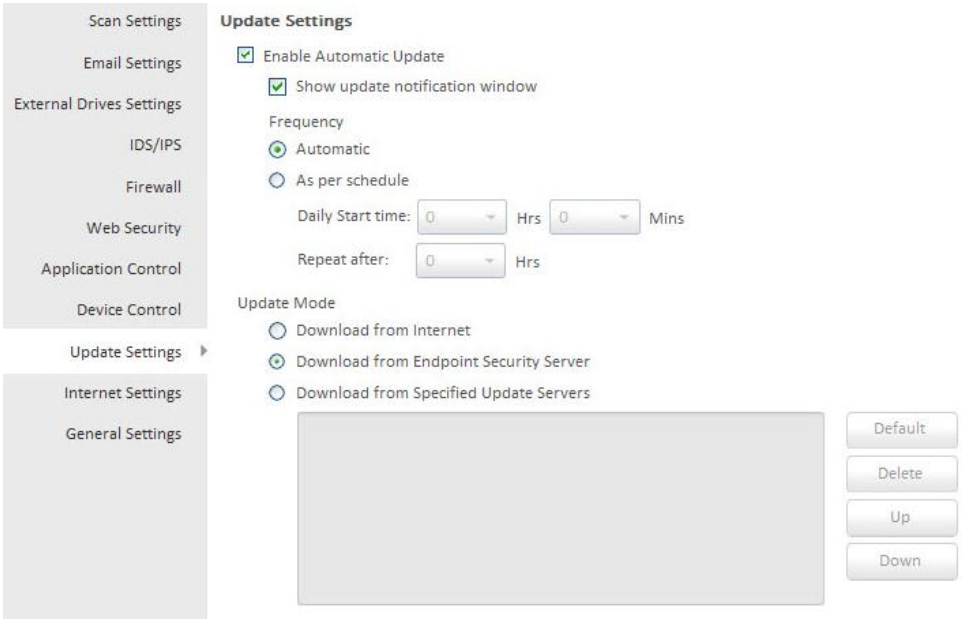
\Quick Heal Installing Path\Admin\dcconfig.exe

مانند:

C:\Program Files (x86)\Quick Heal\Endpoint Security 5.3\Admin\dcconfig.exe

Update Settings

تنظیمات بروزرسانی کلاینت ها در این بخش قابل پیکربندی می‌باشد. تنظیمات مدیریت بروزرسانی سرور اندپوینت‌سکیوریتی در اینجا پیکربندی نمی‌شود.



Enable Automatic Update: در صورت فعال بودن این گزینه بروزرسانی کلاینت ها به صورت خودکار صورت می‌گیرد.

Show update notification window: اگر این گزینه تیک باشد، پنجره اطلاع رسانی مربوط به بروزرسانی نمایش داده می‌شود.

Frequency: بازه زمانی بروزرسانی کلاینت ها را می توانید در این بخش تعیین نمایید.

Automatic: بازه زمانی بروزرسانی کلاینت ها خودکار تعیین می‌گردد.

As per schedule: اگر این گزینه فعال باشد، بروزرسانی کلاینت ها را می توانید زمانبندی و برنامه ریزی نمایید.

Daily Start time: ساعت آغاز بروزرسانی را می توانید تعیین نمایید.

Repeat after: تکرار بروزرسانی روزانه را نیز می توانید در این بخش تعیین نمایید.

Update Mode: در این قسمت حالت آپدیت تعیین می‌گردد.

Download from Internet: اگر این گزینه انتخاب باشد، بروزرسانی کلاینت ها از بستر اینترنت دانلود (انجام) می‌گردد.

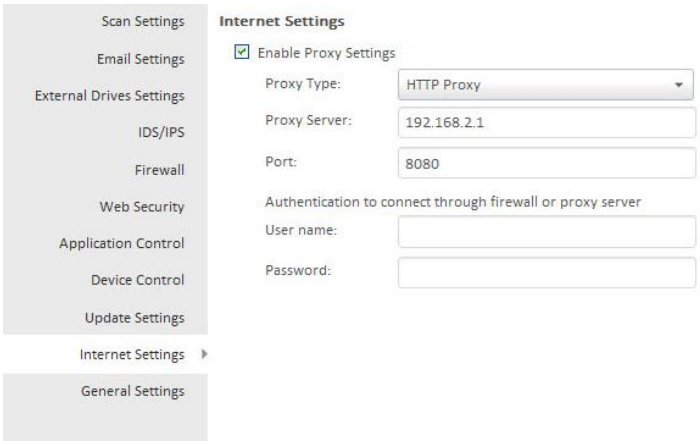
Download from Endpoint Security Server: اگر این گزینه انتخاب باشد، کلاینت ها از سرور اندپوینت بروزرسانی خود را دریافت می کنند.

Download from Specified Update Servers: اگر یک آپدیت سرور مجزا برای بروزرسانی درنظر گرفته اید (مثلا در دفتر دیگر) می توانید مشخص کنید که این کلاینت ها از آن سرور بروزرسانی آپدیت شوند.

در صورتی که چندین سرور بروزرسانی راه‌اندازی کردید، می‌توانید ترتیب سرور بروزرسانی کلاینت ها را با استفاده از دکمه های Default، Delete، Up و Down جابجا یا حذف نمایید.

Internet Settings

در صورتی که کلاینت ها برای اتصال به اینترنت نیاز به پراکسی داشته و مایلید تا کلاینت کوییک‌هیل به اینترنت متصل شود تنظیمات پراکسی را در این بخش وارد می نمایید.



Enable Proxy Settings: برای فعال کردن پراکسی، این گزینه را تیک نمایید.

Proxy Type: نوع پراکسی را در این قسمت مشخص می کنید. پراکسی می تواند HTTP Proxy، SOCKS V4 یا SOCKS V5 باشد.

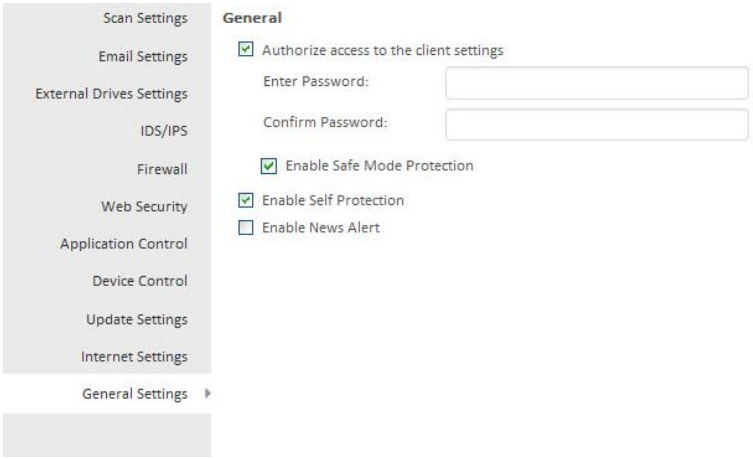
Proxy Server: آدرس IP پراکسی سرور را در این بخش وارد کنید.

Port: پورت پراکسی در این بخش وارد می‌شود.

Authentication to connect through firewall or proxy server: در صورتی که سرور پراکسی یا فایروال نیاز به احراز هویت دارد نام کاربری (User name) و رمز عبور (Password) را در این بخش وارد نمایید.

General

در این بخش تنظیمات عمومی کلاینت ها قرار دارد.



Authorize access to the client settings: اگر این گزینه فعال باشد، برای دسترسی به تنظیمات کلاینت رمز عبور پرسیده خواهد شد.

Enter Password: رمز عبور مورد نظر برای کلاینت کوییک‌هیل را وارد نمایید.

Confirm Password: مجددا رمز عبور را وارد نمایید.

Enable Safe Mode Protection: با فعال بودن این گزینه حتی در زمان راه‌اندازی سیستم در حالت Safe Mode، آنتی ویروس کوییک‌هیل به محافظت خود ادامه می دهد.

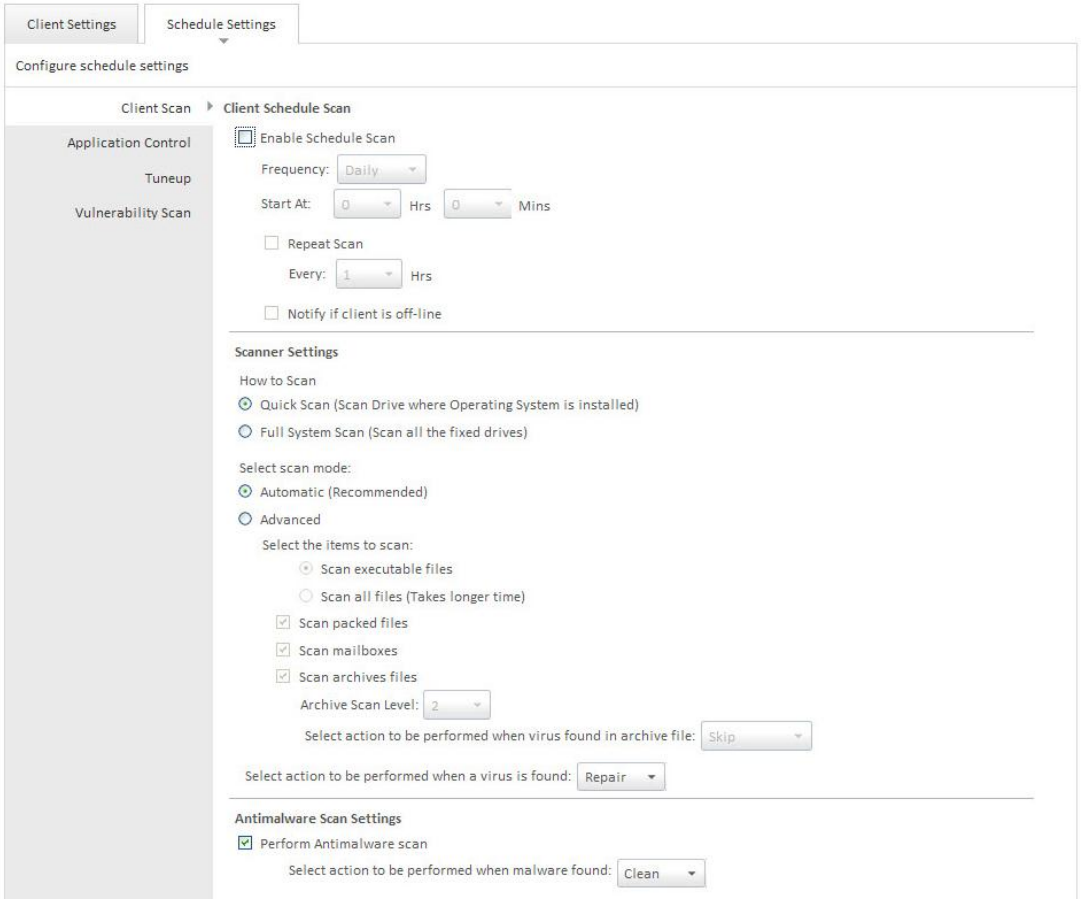
Enable Self Protection: در صورتی که این گزینه فعال باشد، کوییک‌هیل از خود در برابر هرگونه تغییر ناخواسته توسط ویروس محافظت می کند.

Enable News Alert: آخرین اخبار و اخطارها به کاربر نشان داده می‌شود.

در انتها برای ذخیره پالیسی بر روی ***Save Policy*** کلیک نمایید.

Schedule Settings

سربرگ دوم از مدیریت پالیسی، مربوط به پیکربندی تنظیمات زمانبندی است. در این بخش می توانید اسکن کلاینت ها، کنترل برنامه ها، بهینه سازی، اسکن آسیب پذیری را زمانبندی نمایید.



Client Scan

سربرگ اول این بخش مربوط به زمانبندی اسکن کلاینت می‌باشد. در این بخش می توانید تعیین کنید که در دوره های زمانی خاص کوییک‌هیل شروع به ویروسیابی کلاینتها نماید.

Enable Schedule Scan: برای فعال کردن زمانبندی اسکن این گزینه باید تیک باشد.

Frequency: فرکانس اسکن را می توانید در این بخش تعیین کنید. دوره های اسکن می تواند به صورت روزانه یا هفتگی باشد.

در صورتی که فرکانس اسکن به صورت Daily باشد، زمانی آغاز اسکن (Start At) و تکرار (Repeat Scan) را باید تعیین کنید.

اگر فرکانس اسکن هفتگی Weekly باشد، روز هفته (Weekday) نیز باید تعیین گردد.

Notify if client is off-line: اگر کلاینت آفلاین باشد، اطلاع رسانی مناسب صورت می‌پذیرد.

Scanner Settings: تنظیمات اسکنر در این بخش مشخص می‌گردد.

Antimalware Scan Settings:

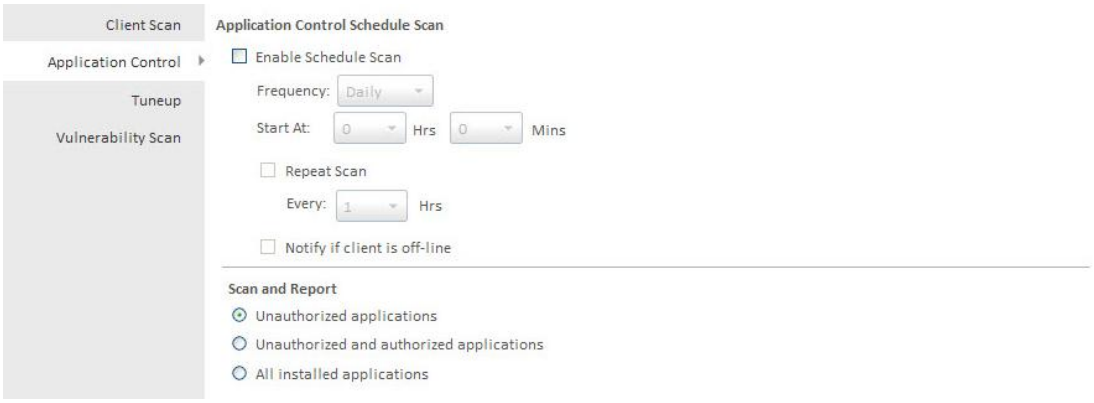
در این بخش تنظیمات اسکن ضد بدافزار تعیین می‌گردد.

Perform Antimalware scan: اگر این گزینه تیک باشد، ضد بدافزار بر روی کلاینت اجرا خواهد شد.

Select action to be performed when malware found: اقدامی که در هنگام یافتن بدافزار انجام می یابد، تعیین می‌گردد، این عمل می تواند Clean (پاکسازی) یا صرفنظر (Skip) باشد.

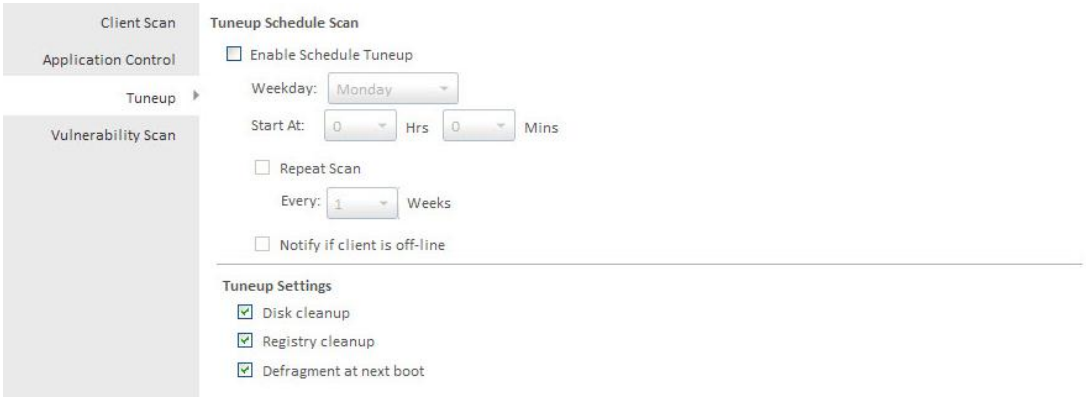
Application Control Schedule Scan

در این بخش می توانید اسکن برنامه ها را زمانبندی نمایید تا در زمان مشخص شروع به اسکن برنامه های غیرمجاز (Unauthorized applications)، برنامه های مجاز و غیرمجاز (Unauthorized and authorized applications)، همه برنامه های نصب شده (All installed applications) نماید.



Tuneup Schedule Scan

زمانبندی اسکن بهینه سازی در این بخش تعیین می‌گردد. در بخش اول زمانبندی مشخص می‌گردد.



تنظیمات بهینه سازی

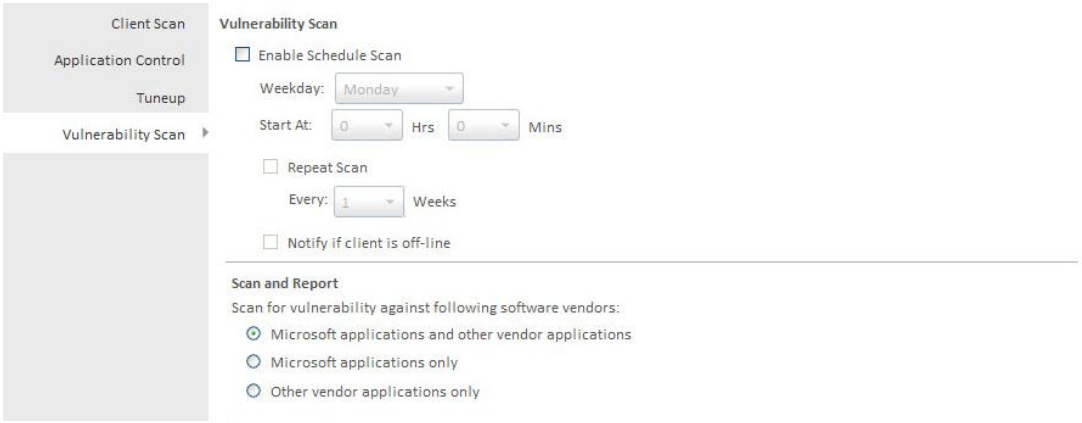
Disk cleanup: پاکسازی دیسک انجام می‌گیرد.

Registry cleanup: پاکسازی رجیستری صورت می‌پذیرد.

Defragment at next boot: در راه‌اندازی بعدی فایل های سیستمی و مهم ویندوز دفرگمنت می‌شود و موجب افزایش سرعت سیستم می‌گردد.

Vulnerability Scan

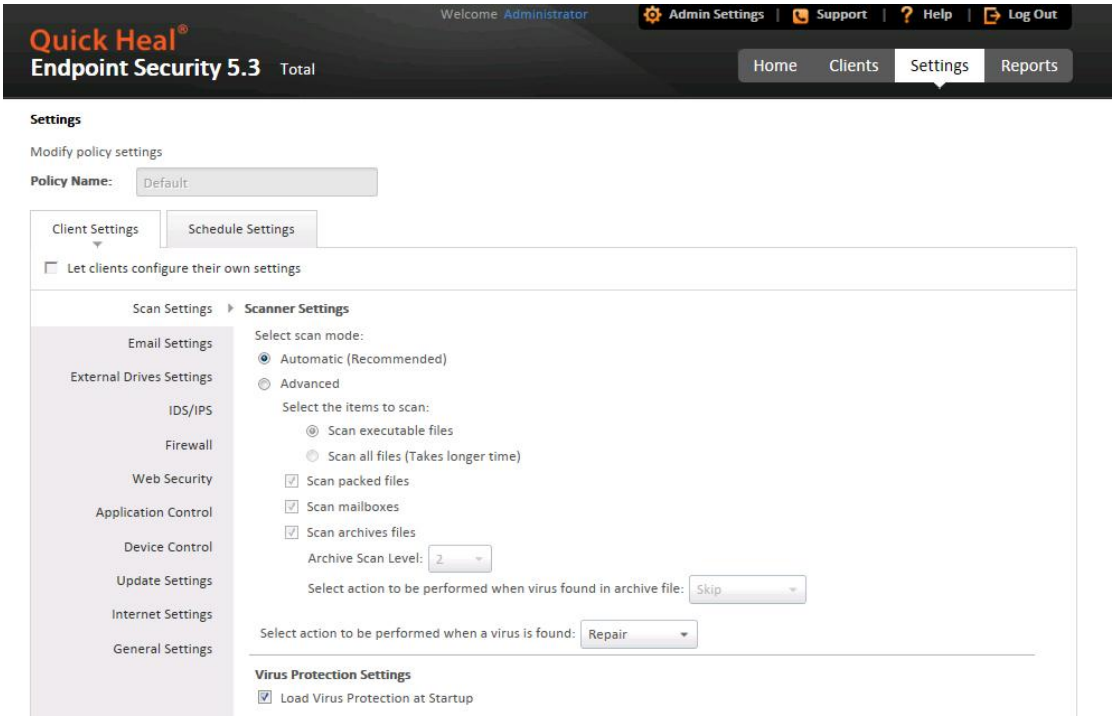
اسکن آسیب پذیری در این بخش قابل برنامه ریزی و زمانبندی است. در قسمت ابتدایی زمانبندی مشخص می‌گردد.



در بخش دوم می توانید تعیین کنید که برنامه های مایکروسافت و شرکت های دیگر(Microsoft applications and other vendor applications)، فقط برنامه های مایکروسافت (Microsoft applications only) و یا فقط برنامه های شرکتهای دیگر (Other vendor applications only) اسکن آسیب پذیری گردد.

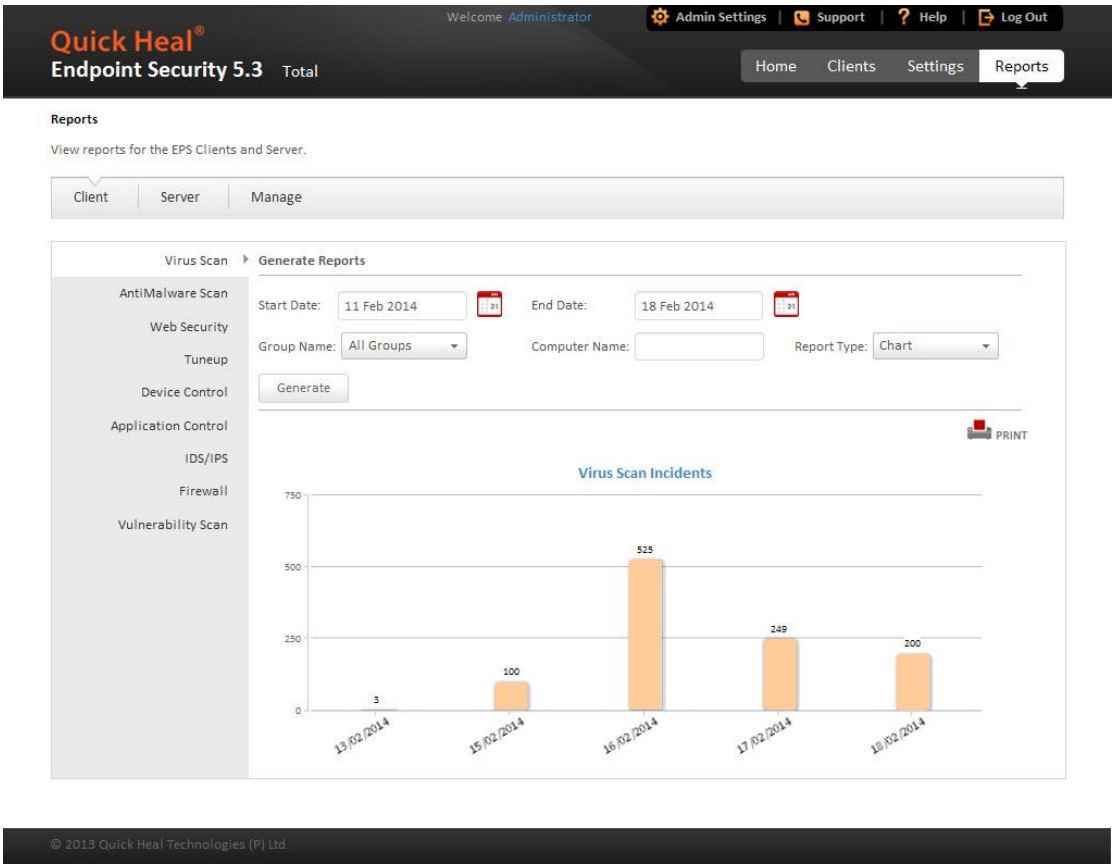
Settings

گزینه های این بخش دقیقا همانند افزودن یک پالیسی جدید می‌باشد. با این تفاوت که این تنظیمات بر روی کلاینت‌هایی که عضو هیچ گروه خاصی نبوده اعمال می‌گردد. در واقع پالیسی پیش فرض کلاینت ها می‌باشد.



Reports

گزارش ها در سربرگ اصلی Reports قرار دارد. این سربرگ دارای ۳ زیرسربرگ می‌باشد.



در بخش ***Client***، گزارش های مختلف امنیتی قابل تولید است. گزارش های مربوط به اسکن ویروس (Virus Scan)، اسکن ضدبدافزار (AntiMalware Scan)، امنیت وب (Web Security)، بهینه سازی (Tuneup)، کنترل ابزار (Device Control)، کنترل برنامه (Application Control)، سیستم شناسایی و پیشگیری از نفوذ غیرمجاز (IDS/IPS)، فایروال (Firewall)، اسکن آسیب پذیری (Vulnerability Scan) در این بخش قابل دسترس است.

Generate Reports: در بخش اول شرایط تولید گزارش تعیین می‌شود.

Start Date: تاریخ شروع

End Date: تاریخ انتها

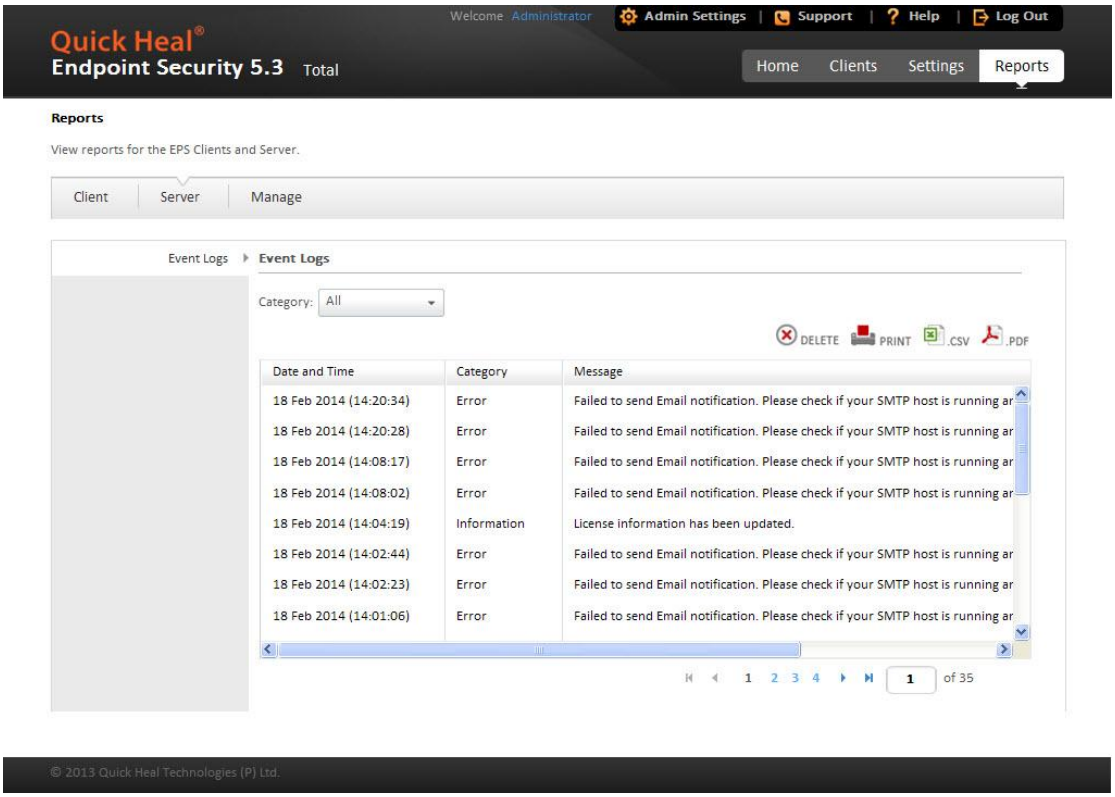
Group Name: نام گروه

Computer Name: نام کامپیوتر که می تواند خالی باشد.

Report Type: نوع گزارش که می تواند نموداری (Chart) یا به صورت اطلاعات جزئی (Tabular) باشد.

Server

بخش دوم گزارش ها Server می‌باشد. در این بخش گزارش های مربوط به سرور اندپوینت‌سکیوریتی قابل مشاهده، خروجی و چاپ است.



DELETE: با انتخاب گزارش و انتخاب این دکمه، حذف صورت می‌پذیرد.

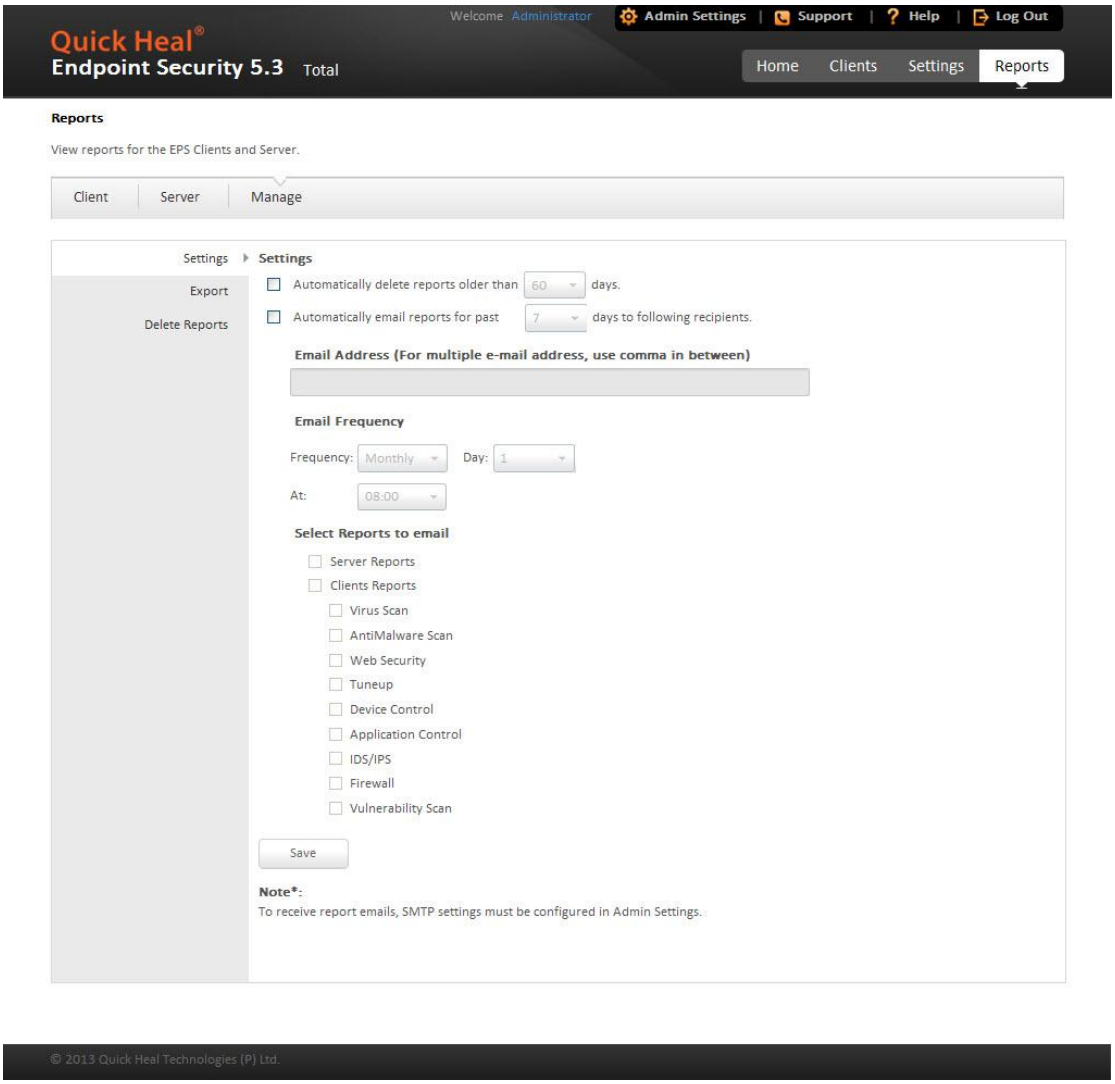
.CSV: با کلیک بر روی این دکمه، خروجی CSV می دهد.

PRINT: امکان چاپ گزارش با کلیک بر روی این دکمه وجود دارد.

.PDF: خروجی به صورت pdf صادر می‌شود

Manage

در این بخش تنظیمات مربوط به گزارش قابل اعمال است.



Settings

در بخش اول، تنظیمات اولیه مدیریت گزارش قابل انجام است.

Automatically delete reports older than … days: با تیک کردن وتعیین تعداد روز، گزارش ها پس از مدت زمان مذکور حذف می‌گردند.

Automatically email reports for past ... days to following recipients: می توانید اندپوینت‌سکیوریتی را طوری تنظیم کنید که به صورت خودکار، گزارش مربوط به تعداد روزهای مشخص را ایمیل کند.

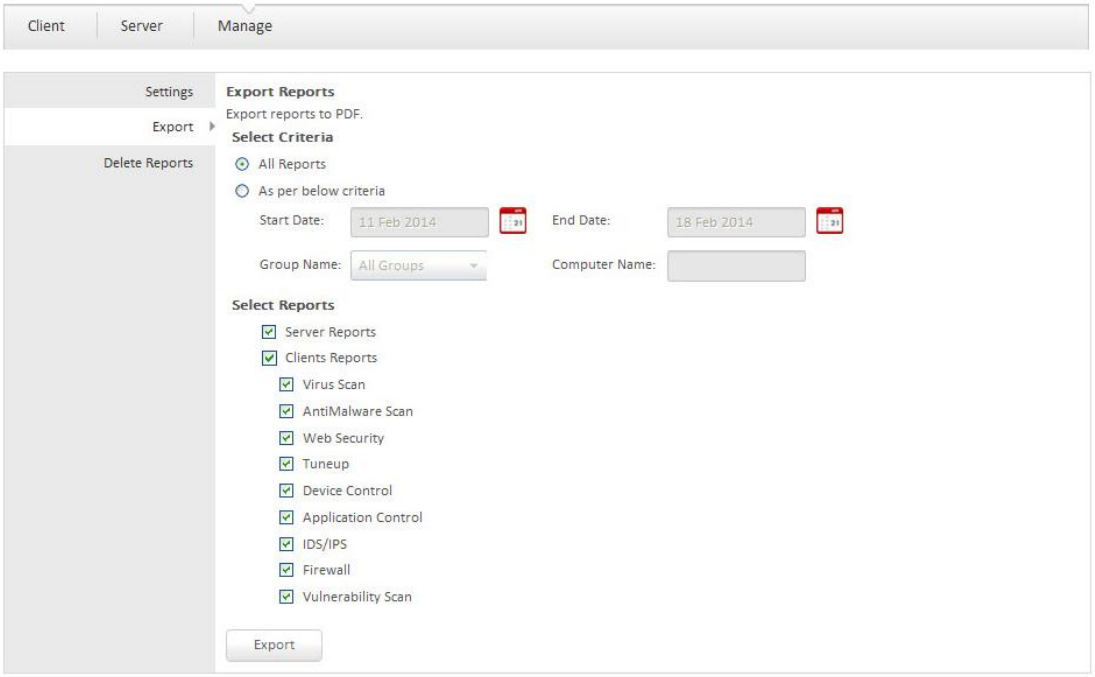
Email Address: آدرس ایمیل مقصد را در این بخش وارد می کنید. با کاما (,) می توانید چندین ایمیل را از هم جدا کنید.

با تیک کردن نوع گزارش می توانید نوع گزارشی که به ایمیل ارسال می‌شود را تعیین نمایید:

Device ،Tuneup ،Web Security ،AntiMalware Scan ،Virus Scan
Vulnerability Scan و Firewall ،IDS/IPS ،Application Control،Control

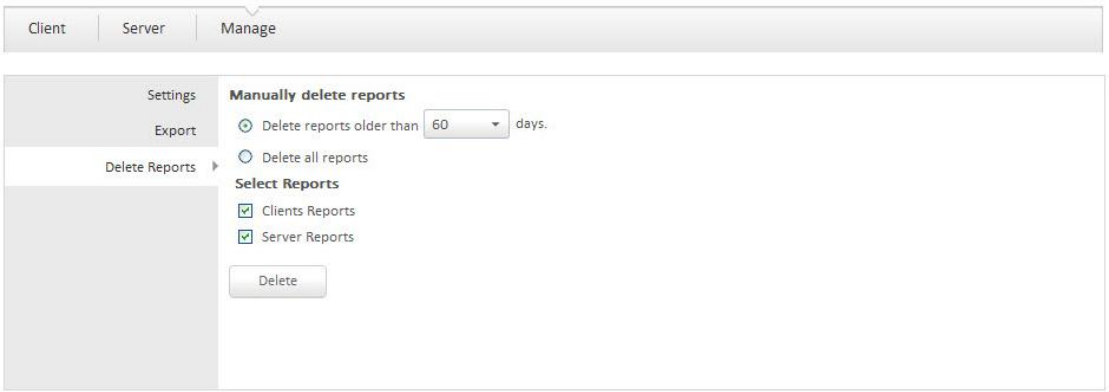
Export

در این بخش می توانید گزارشهای مورد نظر خود را در بازه زمانی مشخص و یا به صورت کلی به خروجی صادر کنید.



Delete Reports

دراین بخش می توانید تنظیمات خود را طوری قرار دهید تا پس از مدتی گزارش ها حذف گردند.



Delete reports older than ... days: پس از مدت زمانی معین، گزارش ها حذف گردند.

Delete all reports: حذف همه گزارش ها.

Select Reports: انتخاب گزارش ها جهت حذف در این بخش تعیین می‌گردد.

Clients Reports: گزارش های کلاینت ها حذف گردند.

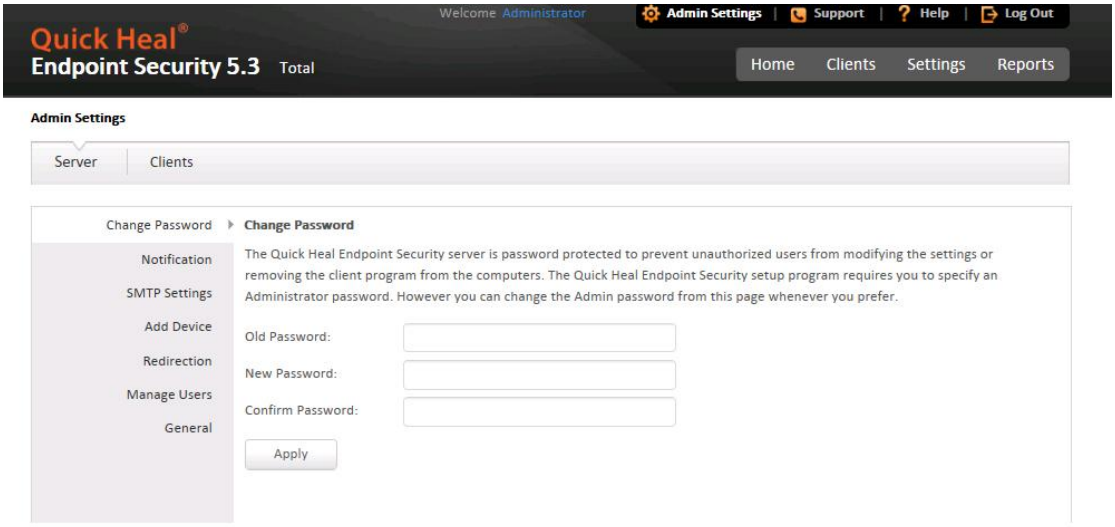
Server Reports: گزارش های سرور حذف گردند.

Delete: با انتخاب موارد فوق و کلیک بر روی این دکمه گزارش ها حذف می‌گردند.

Admin Settings

در این بخش تنظیمات مدیریتی ادمین اندپوینت‌سکیوریتی کوییک‌هیل قرار دارند.

Change Password



در این بخش می توانید رمز عبور سروری کوییک‌هیل اندپوینت‌سکیوریتی را تعویض کنید.

Old Password: رمزعبور قبلی را وارد کنید.

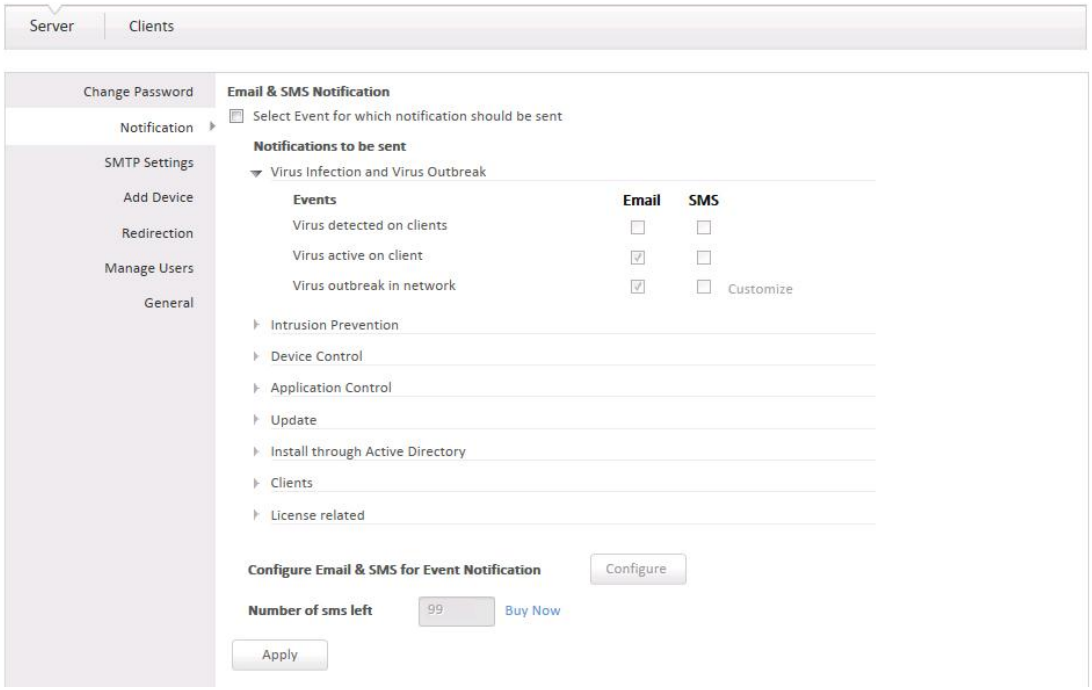
New Password: رمزعبور جدید را وارد کنید.

Confirm Password: رمزعبور جدید را مجدداً وارد کنید.

Notification:

Email & SMS Notification

در این بخش تنظیمات مربوط به اطلاع رسانی اخطارهای امنیتی از طریق ایمیل یا پیامک پیکربندی می‌شوند. انواع اخطارهای امنیتی می توانند از طریق ایمیل یا پیامک به اطلاع مدیر برسد.



Select Event for which notification should be sent: با تیک کردن این گزینه این قابلیت فعال شده و در صورت ایجاد رویدادهای امنیتی به مدیر سیستم اطلاع رسانی می‌شود.

Notifications to be sent: در این بخش انواع اطلاع رسانی و نحوه ارسال به مدیر تعیین می‌گردد. اطلاع رسانی می تواند از طریق پیامک (SMS) و یا ایمیل (Email) باشد.

Virus Infection and Virus Outbreak: اطلاع رسانی مربوط به شیوع آلودگی و ویروس در این بخش قابل پیکربندی است.

Virus detected on clients: در صورتی که ویروسی بر روی کلاینتها شناسایی شد به اطلاع مدیر برسد.

Virus active on client: در صورتی که ویروسی بر روی کلاینتها فعال باشد، به اطلاع مدیر برسد.

Virus outbreak in network: در صورتی که ویروس بر روی کلاینتها در حال شیوع و گسترش باشد، به اطلاع مدیر برسد. (با کلیک بر روی Customize می توانید نحوه شیوع رخداد را سفارشی سازید، چه تعداد ویروس بر روی چند رایانه در چه بازه زمانی شناسایی شده است)

Intrusion Prevention: اطلاع رسانی مربوط به پیشگیری از نفوذ غیرمجاز در این بخش قابل پیکربندی است.

Intrusion detected on client: در صورتی که نفوذ غیرمجاز به کلاینتی شناسایی شد به اطلاع مدیر برسد.

Port Scanning incident detected on client: در صورتی که رخداد پویش پورت بر روی کلاینت، به اطلاع مدیر برسد.

DDOS Attack detected on client: در صورتی که بروز حمله انکار سرویس توزیع شده بر روی کلاینت، به اطلاع مدیر برسد.

Device Control: اطلاع رسانی مربوط به کنترل ابزار در این بخش قابل پیکربندی می‌شود.

Attempt to access unauthorized device: در صورتی که تلاشی برای دسترسی به ابزارهای غیرمجاز صورت گیرد، به اطلاع مدیر می رسد.

Application Control: اطلاع رسانی مربوط به کنترل برنامه در این بخش قابل پیکربندی می‌شود.

Attempt to access unauthorized application: در صورتی که تلاشی برای دسترسی به برنامه های غیرمجاز صورت گیرد، به اطلاع مدیر می رسد.

Update: اطلاع رسانی مربوط به بروزرسانی در این بخش قابل پیکربندی می‌شود.

Service pack is available: در صورتی که سرویس پک جدید برای اندپوینت‌سکیوریتی کوییک‌هیل منتشر گردد، به اطلاع مدیر می رسد.

Clients are not updated to latest virus definitions: در صورتی که کلاینت ها بروزرسانی نشده باشند، به اطلاع مدیر می رسد.

*Update Manager virus definition date is older:*در صورتی که تاریخ بروزرسانی آپدیت منیجر (Update Manager) قدیمی‌باشد، به اطلاع مدیر می رسد.

Install through Active Directory: اطلاع رسانی مربوط به اکتیو دایرکتوری در این بخش قابل پیکربندی می‌شود.

Synchronization with Active Directory failed: در صورتی که همگام سازی با اکتیو دایرکتوری با شکست روبرو شد، به اطلاع مدیر می رسد.

Clients: اطلاع رسانی مربوط به کلاینت ها در این بخش قابل پیکربندی می‌شود.

Client disconnected from the network on infection: اگر کلاینت به علت آلودگی از شبکه قطع ارتباط کند، به اطلاع مدیر می رسد.

Client disconnected from the network on DDOS Attack: اگر کلاینت به علت حمله DDOS از شبکه قطع ارتباط کند، به اطلاع مدیر می رسد.

Client disconnected from the network on Port Scan: اگر کلاینت به علت پویش پورت از شبکه قطع ارتباط کند، به اطلاع مدیر می رسد.

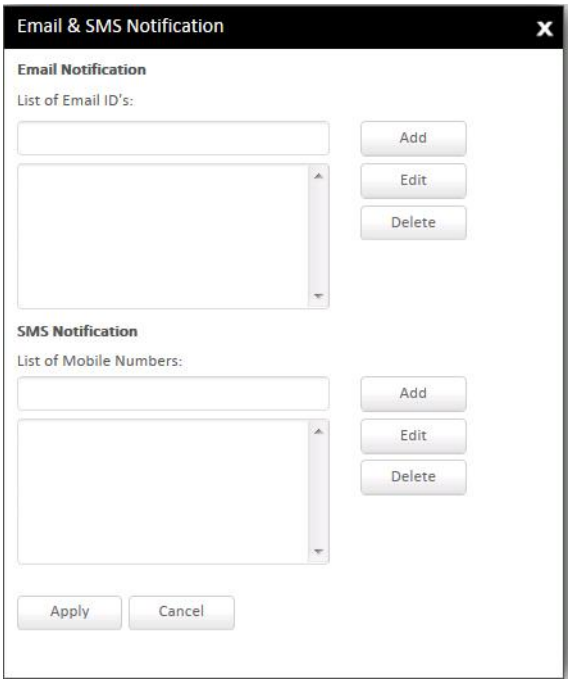
License related: اطلاع رسانی مربوط به لایسنس در این بخش قابل پیکربندی می‌شود.

License expired: در صورت انقضای لایسنس، به مدیر اطلاع داده می‌شود.

License is about to expire: در صورتی لایسنس درحال انقضا باشد، به مدیر اطلاع داده می‌شود.

License limit exceeds: در صورتی که تعداد کلاینت نصب شده از تعداد مجاز لایسنس بیشتر شود، به مدیر اطلاع داده می‌شود.

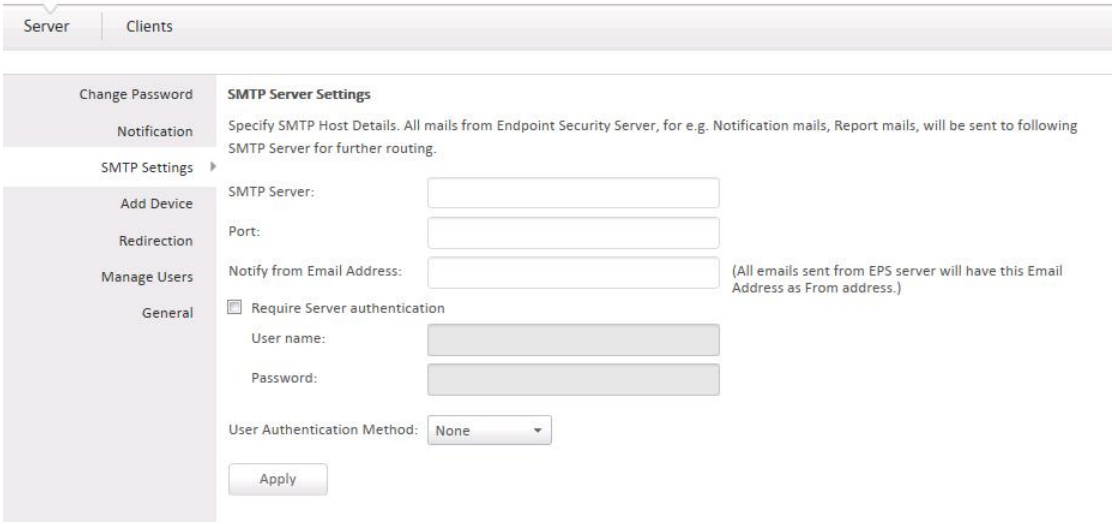
Configure Email & SMS for Event Notification: در این قسمت ایمیل و SMS خود را برای اطلاع‌رسانی پیکربندی می کنید. با کلیک بر روی دکمه Configure پنجره زیر باز می‌شود.



با وارد کردن شناسه ایمیل و شماره موبایل و زدن دکمه Add می توانید به لیست اطلاع رسانی خود بیفزایید.

SMTP Server Settings

برای ارسال ایمیل های اطلاع رسانی و گزارش توسط اندپوینت‌سکیوریتی، SMTP Server باید پیکربندی گردد.



SMTP Server: سرور SMTP در این فیلد وارد می‌شود.

Port: آدرس پورت سرور SMTP در این فیلد وارد می‌شود.

Notify from Email Address: آدرس ایمیلی که به آن آدرس ایمیل، اطلاع رسانی ارسال می‌شود.

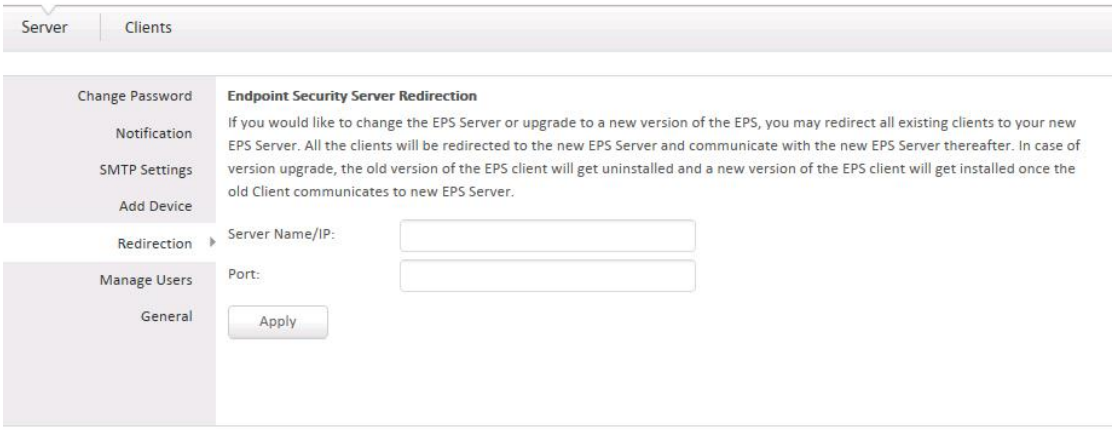
Require Server authentication: در صورتی که سرور SMTP نیاز به احراز هویت دارد، این گزینه را تیک کنید.

User name: نام کاربری در این فیلد وارد می‌شود.

Password: رمز عبور در این فیلد وارد می‌شود.

User Authentication Method: متد رمزنگاری احراز اصالت در این فیلد مشخص می‌شود. متد می تواند None، SSL یا TSL باشد.

Redirection



Endpoint Security Server Redirection:

یکی از ویژگی های مفید کوییک‌هیل اندپوینت‌سکیورتی، امکان آپگرید (Upgrade) و تغییر نسخه بدون نیاز به حذف و نصب از روی کلاینت ها می‌باشد. همچنین در صورت تمایل می توانید، بدون دردسر نصب و حذف از روی کلاینتها، به راحتی سرور اندپوینت خود را تغییر دهید.

در صورت انتشار نسخه جدید (معمولا سالانه یکبار نسخه جدید منتشر می‌گردد) نسخه جدید را بر روی سرور جدید و یا در کنار اندپوینت فعلی نصب می کنید. سپس آدرس IP و یا نام سرور –بسته به روش نصب– و آدرس پورت سرور جدید اندپوینت را در نسخه قبلی اندپوینت وارد می کنید. به صورت خودکار همه کلاینت ها از سرور اندپوینت جاری به سرور جدید اندپوینت منتقل شده و در صورت نیاز نسخه قبلی خودکار حذف و نسخه جدید کوییک‌هیل کلاینت بر روی کلاینت ها نصب می‌شود.

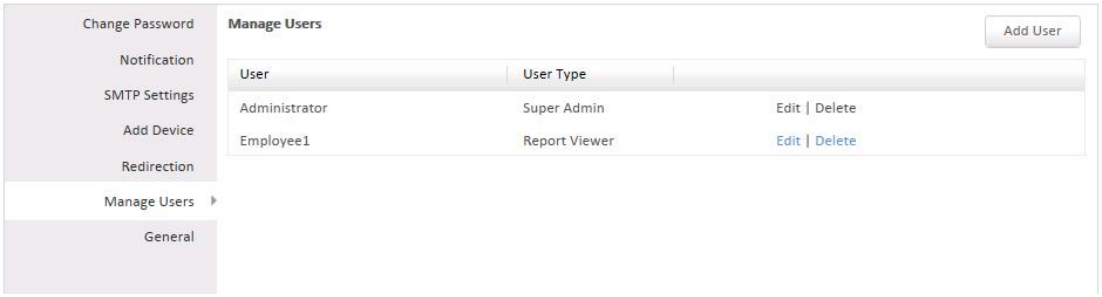
بنابراین تنها نیاز دارید آدرس IP یا نام سرور جدید را در این بخش سرور قدیمی وارد نمایید.

Server Name/IP: نام سرور یا IP اندپوینت جدید را وارد می کنید. (در صورتی که اندپوینت جدید را بر روی همان سرور قبلی نصب کردید، آدرس IP یا نام همین کامپیوتر را وارد کنید)

Port: آدرس پورت اندپوینت جدید را در این بخش وارد کنید، آدرس پورت همان آدرسی است که کلاینت ها با سرور ارتباط برقرار می کنند مثلاً پورت پیش فرض در Quick Heal Endpoint Security 5.3، آدرس ٥٠٤٤ می‌باشد.)

Manage Users

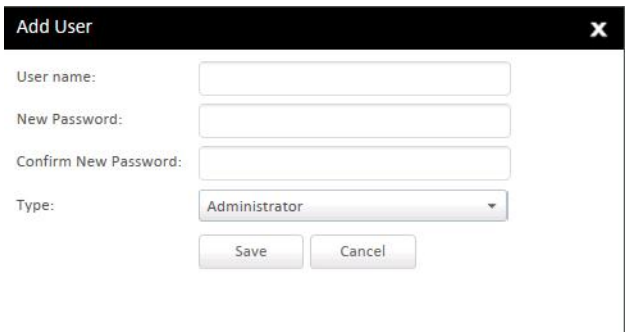
در این بخش کاربران استفاده کننده از کنسول اندپوینت‌سکیوریتی قابل مدیریت می‌باشد.



مدیر پیش فرض اندپوینت Administrator می‌باشد که رمز عبور آن در زمان نصب اندپوینت تعیین شده است.

امکان افزودن، ویرایش و حذف کاربران با سطح دسترسی مدیر و یا فقط خواندنی وجود دارد.

Add User: با کلیک بر روی این دکمه پنجره افزودن کاربر جدید اضافه می‌شود.



User name: نام کاربری جدید در این فیلد وارد می‌شود.

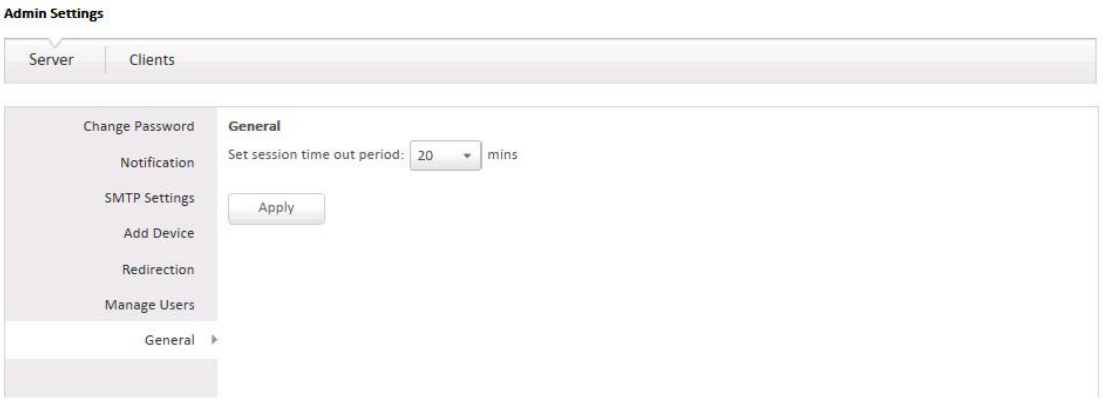
New Password: رمز عبور در این فیلد وارد می‌شود.

Confirm New Password: مجددا رمز عبور در این فیلد وارد می‌شود.

Type: در این فیلد نوع دسترسی مشخص می‌گردد که می تواند مدیر (Administrator) و یا مشاهده کننده گزارش (Report Viewer) باشد.

General

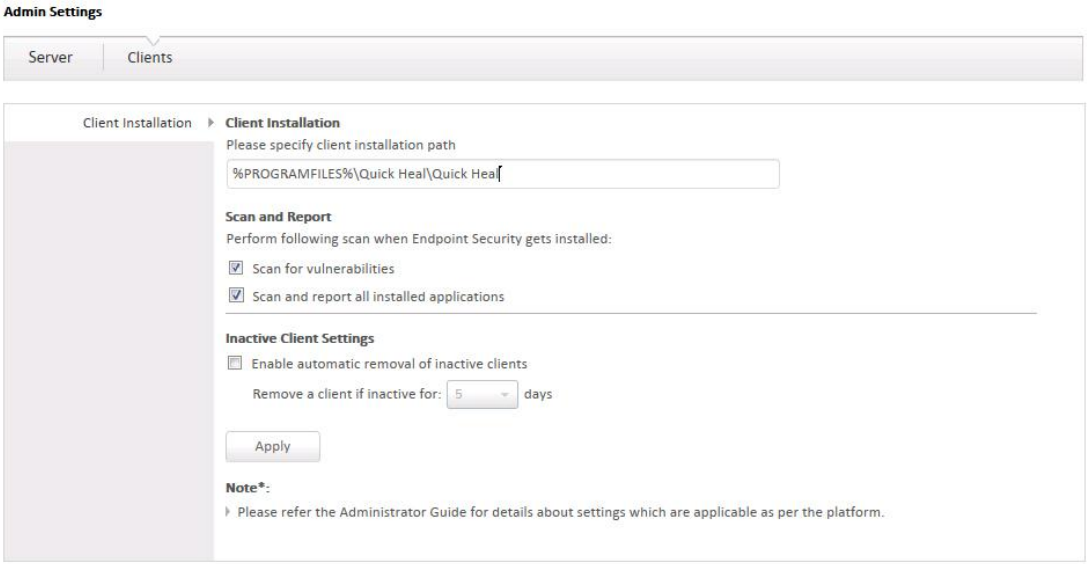
در این بخش می توانید زمان اتمام نشست کنسول تحت وب مدیریتی اندپوینت را مشخص کنید.



Set session time out period: پس از گذشت مقدار زمان مشخص شده به دقیقه و عدم فعالیت کنسول تحت وب، نیاز به ورود مجدد به سامانه می‌باشد.

Client Installation

در سربرگ دوم (Clients) تنظیمات مربوط به فرایند نصب کلاینتها قابل پیکربندی است.



Please specify client installation path: در این بخش می توانید مسیر نصب کلاینت ها را تغییر دهید. در صورت تغییر، نصب کلاینت در مسیر مذکور انجام خواهد پذیرفت.

Scan and Report: در این بخش تنظیمات مربوط به اسکن و گزارش پس از نصب بر روی کلاینت ها قابل پیکربندی است.

Scan for vulnerabilities: پس از اتمام نصب شروع به اسکن آسیب پذیری و حفره می نماید.

Scan and report all installed applications: پس از اتمام نصب شروع به اسکن همه برنامه های نصب شده و تولید گزارش از آنها می نماید.

Inactive Client Settings: تنظیمات کلاینت های غیرفعال در شبکه در این بخش انجام می‌پذیرد.

Enable automatic removal of inactive clients: با فعال کردن این گزینه، اگر کلاینت به تعداد روز مشخص شده در فیلد Remove a client if inactive for به سرور اندپوینت متصل نگردد، اندپوینت آنرا حذف شده در نظر گرفته و لایسنس آن را برای نصب بر روی سیستم دیگر آزاد می کند.

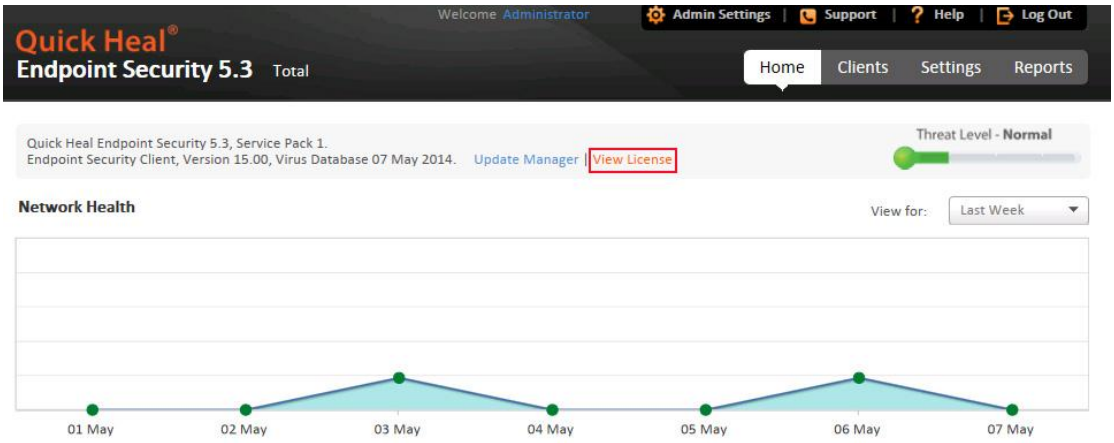
مدیریت لایسنس

پس از انقضای مدت زمان اعتبار لایسنس و اجرا پروسه مالی سفارش خرید، زمان اعتبار اندپوینت‌سکیوریتی کوییک‌هیل خود را افزایش دهید.

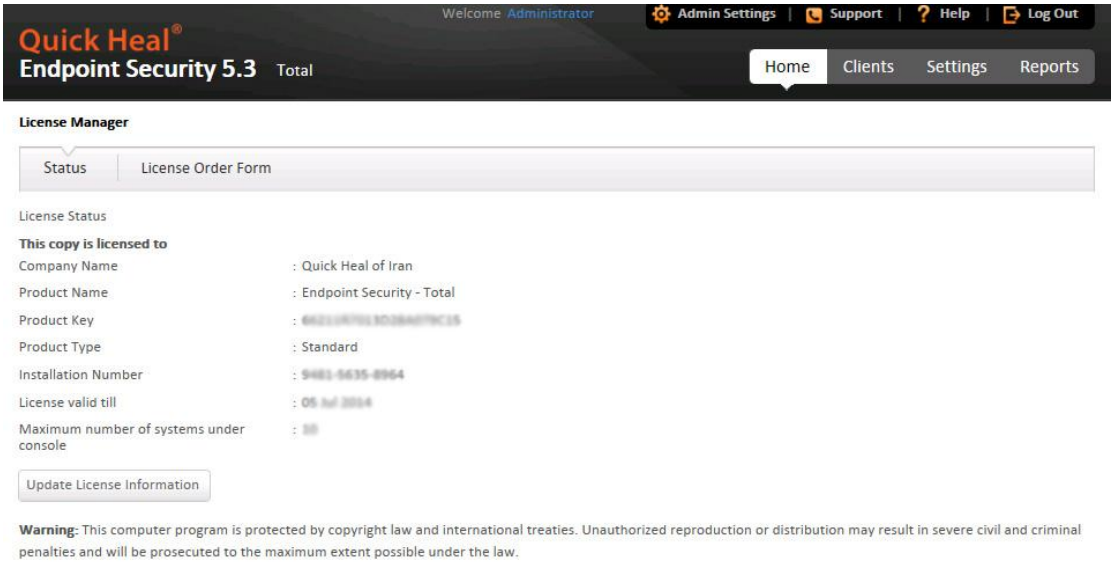
همچنین یکی از قابلیت های کوییک‌هیل در بخش لایسنسینگ، امکان افزودن تعداد کلاینت پس از خرید اولیه است. به عنوان نمونه پس از مدتی تعداد کلاینت ها شبکه شما افزایش یافته و نیاز به افزایش تعداد لایسنس مجاز دارید، بدون نیاز به نصب کنسول مجزا، یا خرید لایسنس کامل مجدد، تنها کافی است به تعداد مورد نیاز افزوده شده لایسنس خریداری نمایید.

همچنین امکان ارتقای نسخه محصول از Quick Heal Endpoint Security Business به نسخه کاملتر Total بدون نیاز به نصب و حذف مجدد کنسول سرور و کلاینت ها میسر می‌باشد.

همه فرایندهای فوق تنها با فشردن یک دکمه صورت می‌پذیرد.



برای اعمال تغییرات لایسنس (افزایش تعداد کلاینت یا تمدید اعتبار و یا ارتقای نسخه) کافی است پس از سفارش خرید لایسنس برای اعمال تغییرات از روی نوار توسی رنگ ابتدای صفحه نخست بر روی لینک باز شود.Status و سربرگ License Manager کلیک می‌نمایید تا صفحه مربوط به View License



برای اعمال تغییرات و بروزرسانی وضعیت لایسن، بر روی دکمه *Update License Information* کلیک نمایید.

نصب بر روی کلاینت

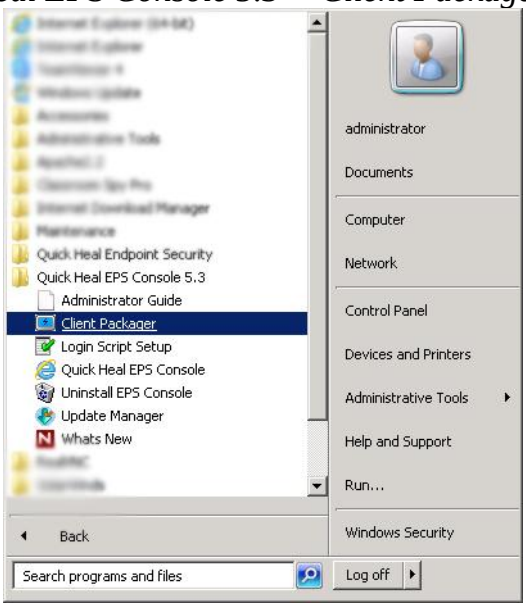
همانطور که در بخش Client Deployment شرح داده شد، ٦ روش مختلف نصب وجود دارد که بسته به سلیقه مدیر و پیکربندی شبکه قابل انتخاب است. در این بخش به ٢ نمونه از روش های پرکاربرد اشاره می کنیم. این روش ها بر روی انواع ساختارهای شبکه (Domain-based و Workgroup) قابل استفاده است.

الف) استفاده از Client Packager

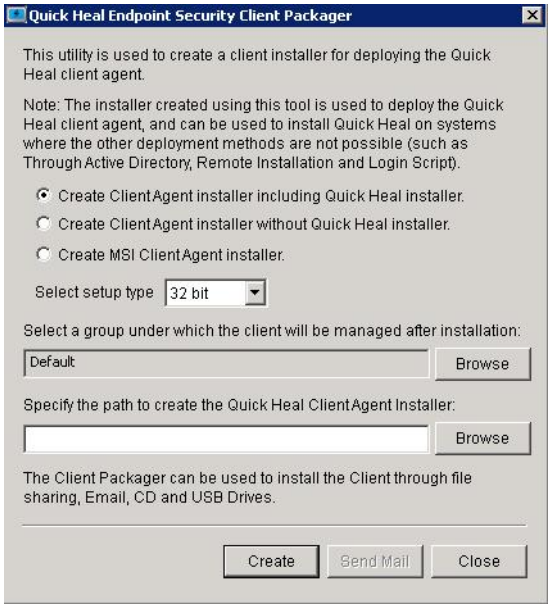
ساده ترین راه نصب بر روی کلاینت ها، می‌باشد. یک فایل پکیجر نصب کننده ساخته و آن را بر روی کلاینت ها (ازطریق به اشتراک گذاری در شبکه و یا فلش) منتقل و اجرا می کنید.

برای ساختن فایل Client Packager از مسیر زیر سرور استفاده کنید:

Start > Quick Heal EPS Console 5.3 > Client Packager



پس از اجرای برنامه ساخت کلاینت پکیجر، صفحه زیر نمایش داده می‌شود:



Create ClientAgent installer including Quick Heal installer: اولین گزینه را انتخاب کنید. با انتخاب این گزینه کلاینت ایجنت به صورت کامل شامل نصب کننده کوییک‌هیل ساخته می‌شود.

Create ClientAgent installer without Quick Heal installer: با انتخاب این گزینه، فقط عامل نصب کننده کلاینت ایجنت ساخته می‌شود و فایل های آنتی ویروس بعد از نصب از بستر شبکه به کلاینت منتقل می‌گردد.

Create MSI ClientAgent installer: با انتخاب این گزینه نوع نصب کننده به صورت MSI مایکروسافت تولید می‌شود.

Select setup type: بسته به نوع معماری کلاینتی، نوع ClientAgent می‌تواند ۳۲ یا ٦٤ بیتی باشد.

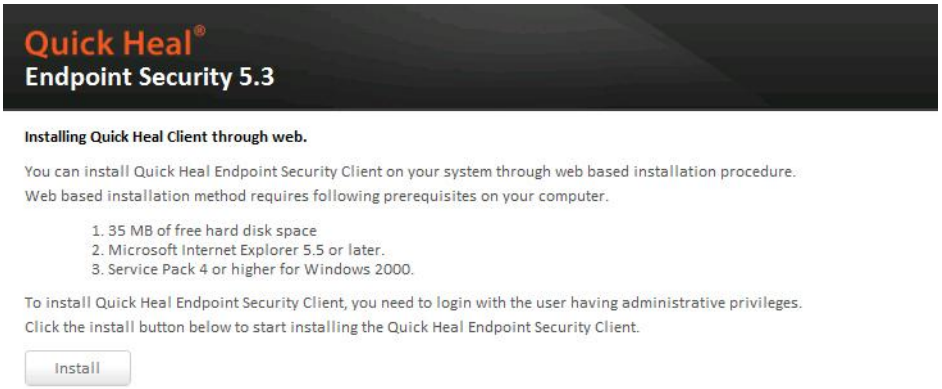
Select a group under which the client will be managed after installation: اگر از قبل گروه و پالیسی در سرور اندپوینت تعریف کرده اید، می توانید گروه را در این بخش تعیین کنید تا پکیجر متناسب با آن گروه ساخته شود. همچنین می توانید گروه را به صورت Default رها کرده و پس از نصب بر روی کلاینت، آن را عضو گروه مناسب خود نمایید.

Specify the path to create the Quick Heal ClientAgent installer: مسیر ساخت کلاینت ایجنت در این قسمت مشخص می‌شود. می توانید Browse کرده و مسیر Desktop را مشخص کنید.

Create: پس از انتخاب نوع کلاینت ایجنت و مسیر بر روی این دکمه کلیک کنید.

Send Mail: امکان ارسال کلاینت ایجنت به صورت ایمیل نیز درنظر گرفته شده است.

ب) نصب با استفاده از وب



راه دیگر نصب بر روی کلاینت ها استفاده از IE، می‌باشد. در این روش آدرس زیر را در اینترنت اکسپلورر کاربر وارد کرده و برروی دکمه Install کلیک می کنید:

https://SERVER-IP:PORT/qhscan503/install.htm

مثل:

https://192.168.0.1:9098/qhscan503/install.htm

پس از مدتی، فرایند نصب برروی کلاینت انجام می‌پذیرد.

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.