راهنمای سریع استفاده از کوییک هیل اندپوینت سکیوریتی

QuickHeal Endpoint Security 6.0

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 می‌توانید با شرکت فناوری ارتباطات و اطلاعات فانوس از طریق ایمیل info@qhi.ir، تلفن ۷۷۱۴۲۵۲۶-۰۲۱ ، پیامک ۳۰۰۰۴۶۲۵ ، وب‌سایت 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.

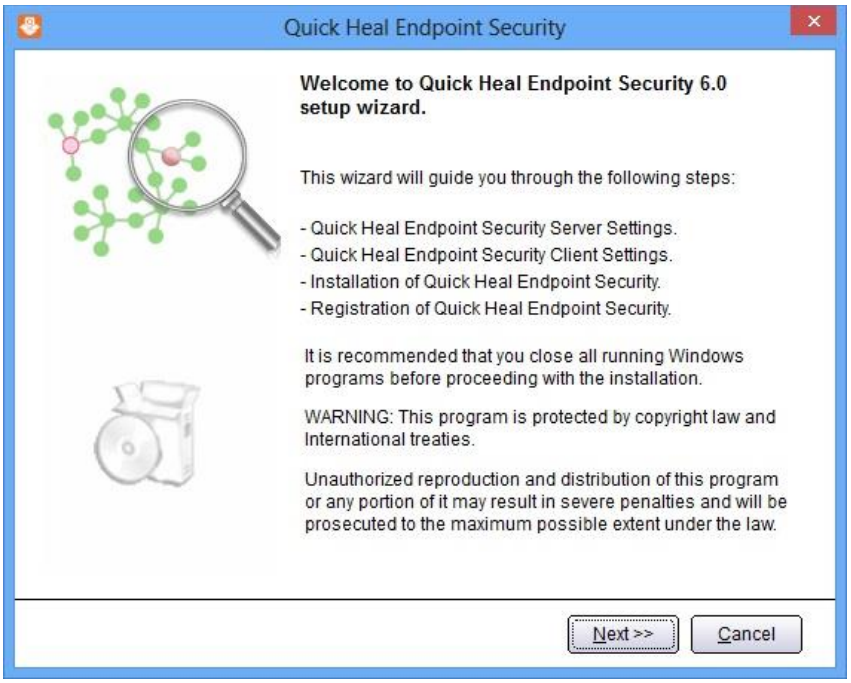
فهرست مطالب

نصب کنسول مدیریتی اندپوینت سکیوریتی کوییک هیل

برای نصب نسخه تحت شبکه کوییک‌هیل با عنوان اندپوینت‌سکیوریتی مراحل زیر را دنبال نمایید:

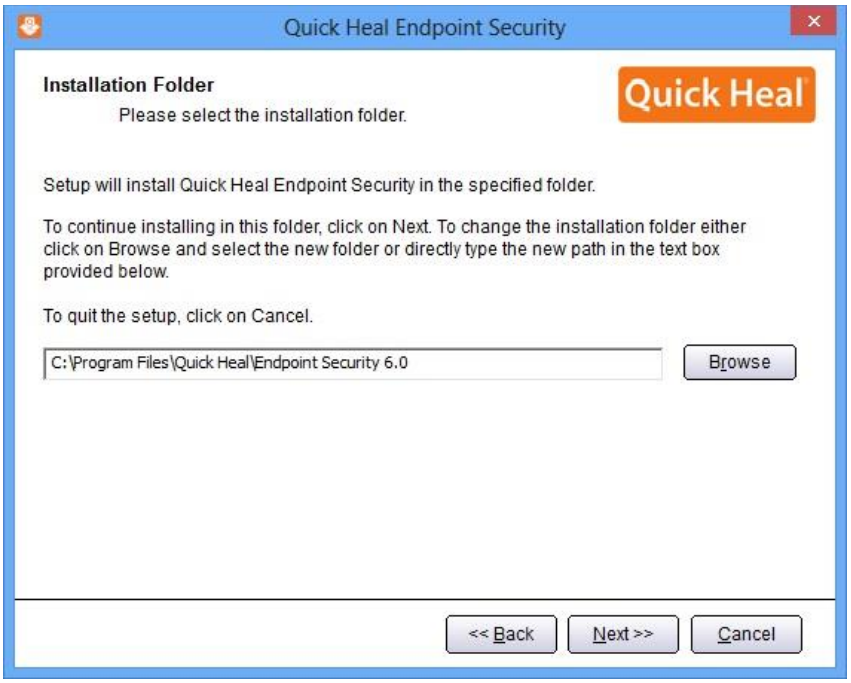
با کلیک بر روی لینک Install ، تصویر زیر نمایش داده می شود:

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

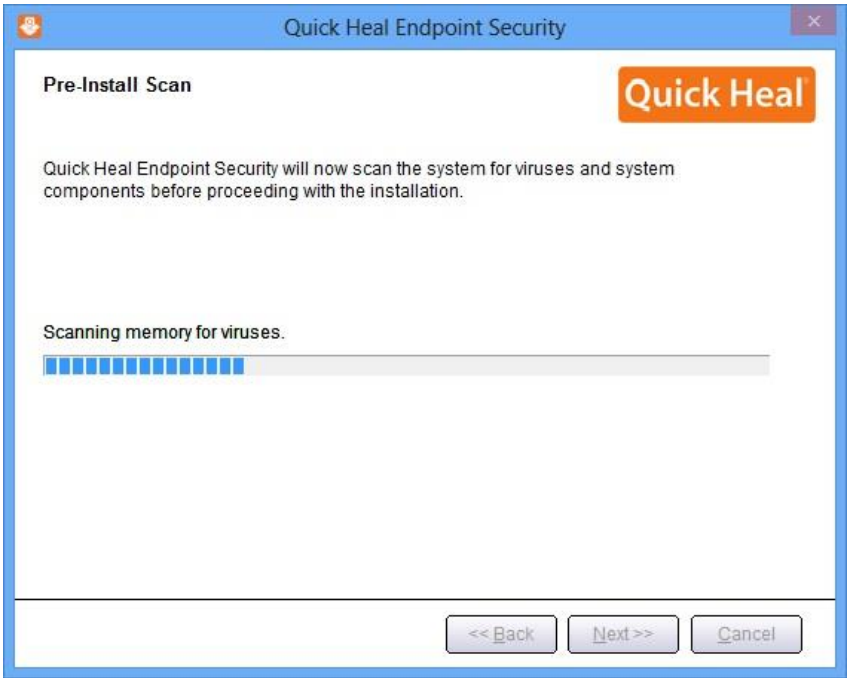


اطلاعات این صفحه مربوط به معرفی اندپوینت می‌باشد. برای ادامه بر روی دکمه Next کلیک کنید.

پس از قرائت توافقنامه حفظ قوانین کپی‌رایت باید گزینه I Agree را انتخاب و بر روی Next کلیک نمایید.

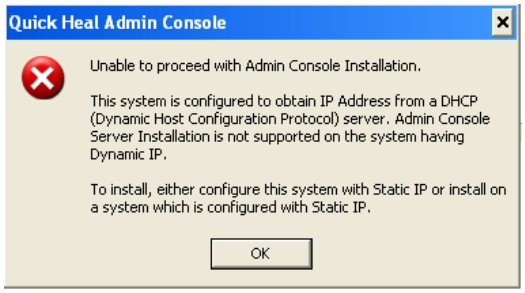


در این مرحله باید مسیر نصب برنامه تعیین شود که می‌توان همان مسیر پیش‌فرض را انتخاب و Next را فشرد.

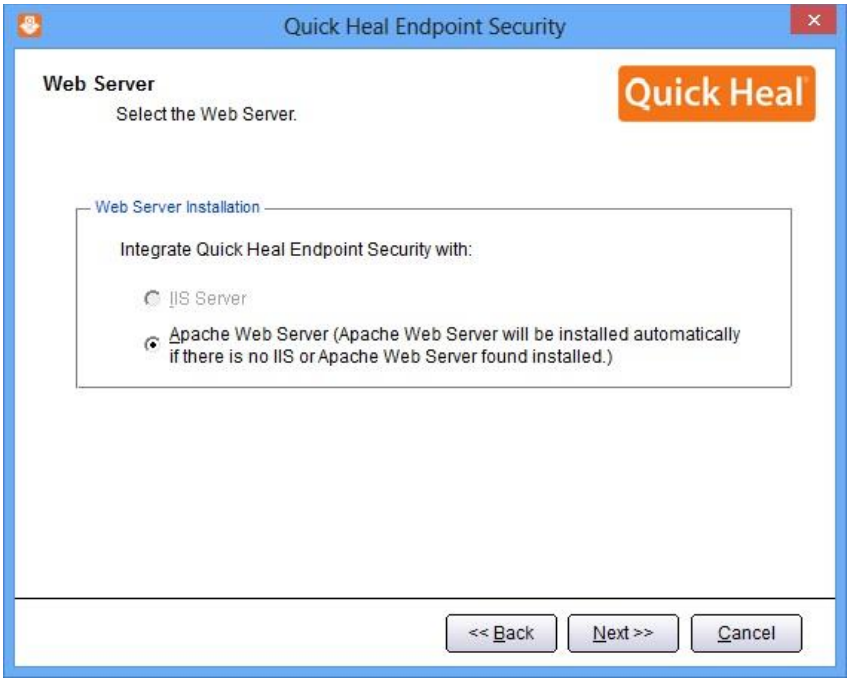


قبل از نصب، مرحله اسکن و ویروسیابی حافظه کامپیوتر نمایش داده می‌شود.

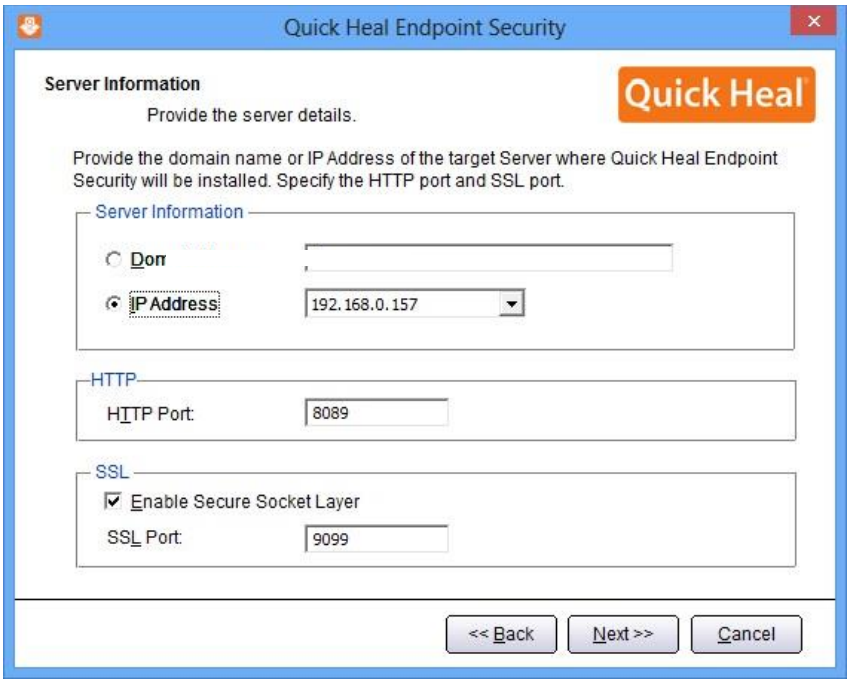
اگر کارت شبکه فعال نباشد و یا یک IP به آن اختصاص نداده باشید، این پیغام نمایش داده خواهد شد. ابتدا کارت شبکه را فعال کرده و به آن IP استاتیک در رنج شبکه اختصاص دهید. (کلاینت‌ها و سرور باید بتوانند به فولدر Share شده یکدیگر دسترسی یابند.)



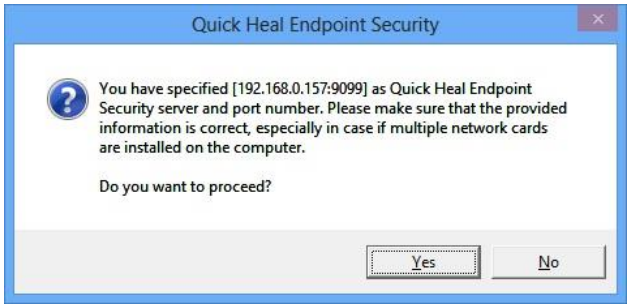
کنسول اندپوینت سکیوریتی بر روی IPهای استاتیک، نصب و فعال می‌شود. در صورتی که سرور موردنظر از IP موقتی و داینامیک (DHCP) استفاده می کند، این پیغام نمایش داده خواهد شد. برای رفع این مشکل یک IP استاتیک به کارت شبکه اختصاص دهید.



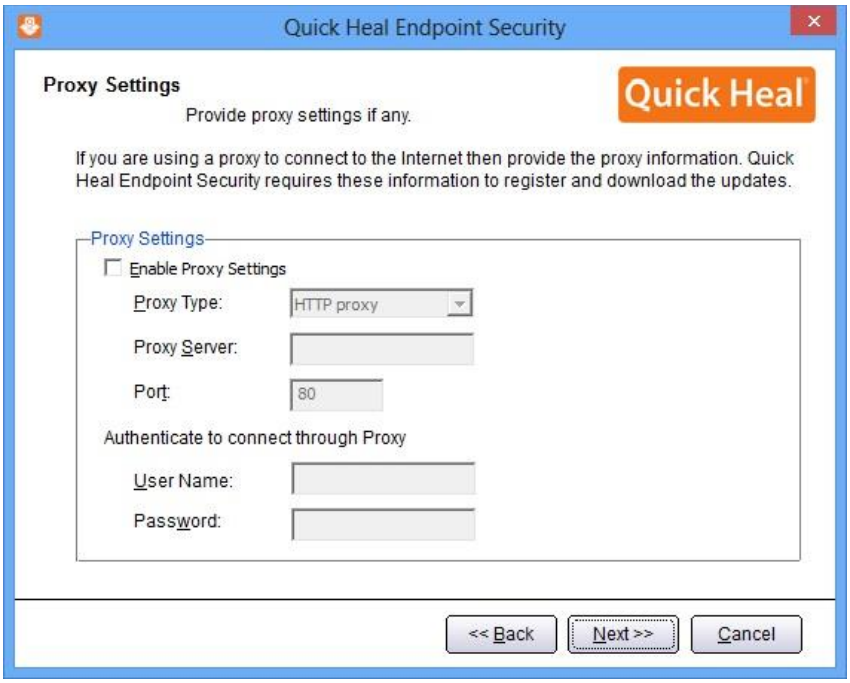
بر روی یکی از گزینه ها کلیک نمایید (ترجیحاً بر روی Apache نصب شود). نصب Apache بصورت خودکار همراه با اندپوینت نصب می‌شود. بر روی Next کلیک نمایید. [در صورتی که مایلید از IIS استفاده نمایید و IIS Server بر روی سیستم شما نصب نیست، باید از مسیر Control Panel/Add or Remove Programs/Add or Remove Components/ Internet Information Services(IIS) نصب انجام گیرد. سپس برنامه مجدداً اجرا گردد.]



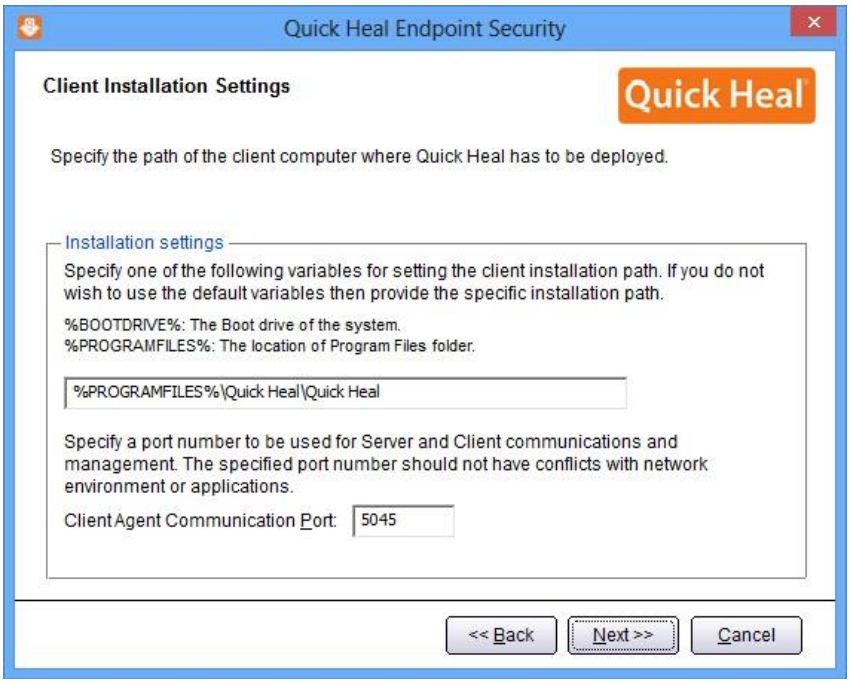
این مرحله تنظیمات مربوط به اطلاعات سرور (در شبکه های مبتنی بر دامنه، ترجیحاً بر روی نام سرور نصب شود) و پورت های HTTP و SSL می‌باشد، در صورتی که پورت‌های فوق در شبکه شما استفاده می‌شوند، آنها را تغییر دهید، در غیر این‌صورت پیش‌فرض را تایید نموده و بر روی Next کلیک نمایید.



برای تائید اطلاعات فوق، بر روی دکمه Yes کلیک نمایید.



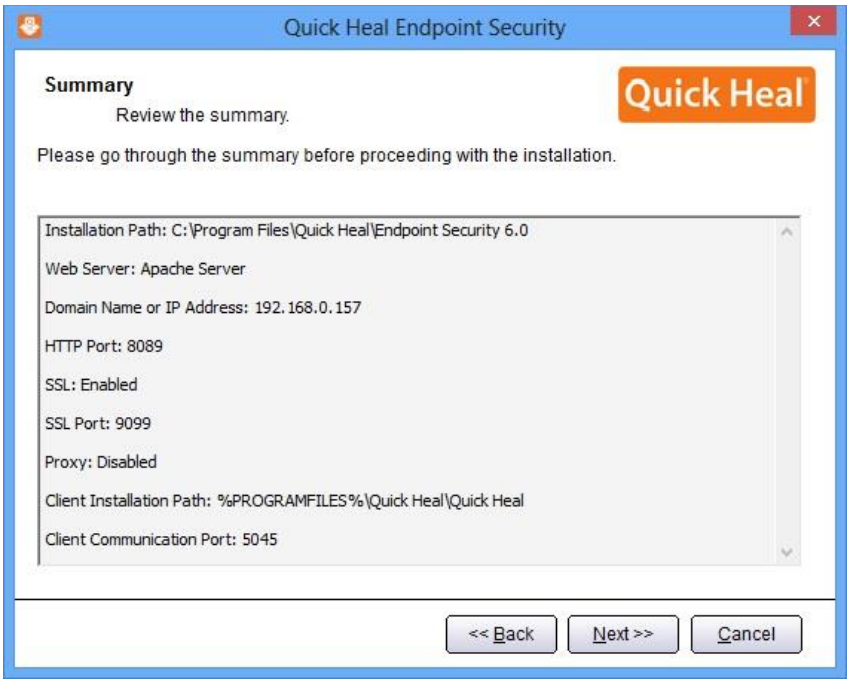
این مرحله انجام تنظیمات مربوط به پراکسی جهت دسترسی به اینترنت می‌باشد. در صورتی‌که نحوه دسترسی به اینترنت از طریق پراکسی باشد، تنظیمات Proxy خود را اعمال نموده و Next را بفشارید.



این صفحه تعیین پورت مربوط به ارتباط کلاینت‌ها با سرور اندپوینت آنتی ویروس است. درصورتی که پورت‌های فوق آزاد می‌باشند، پیش فرض را انتخاب و Next را بفشارید.

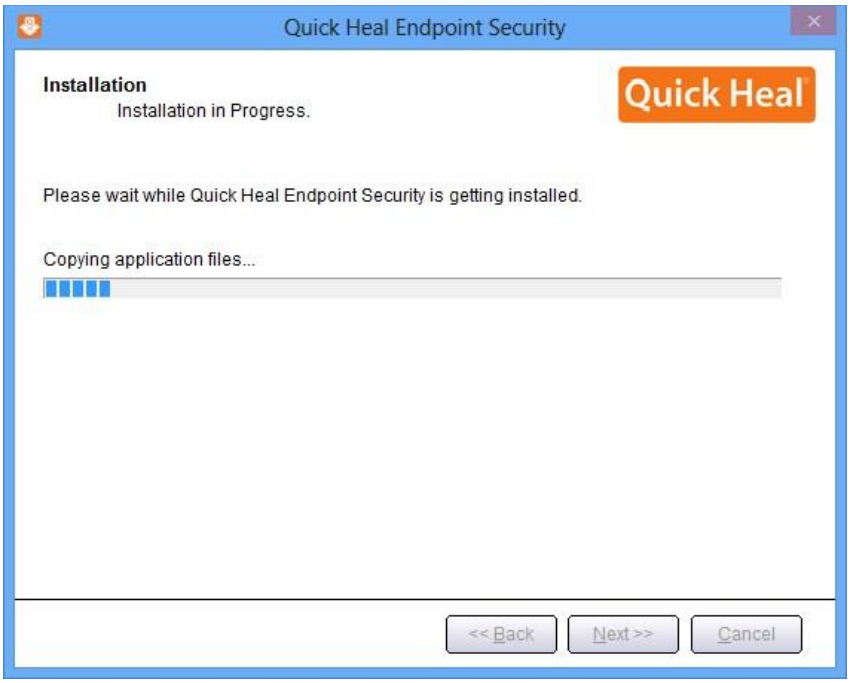
پورت تعیین شده جهت ارتباط بین کلاینت و سرور نباید بر روی سرور قبلاً توسط برنامه‌ی دیگری استفاده شده باشد.

تعیین رمز عبور برای نرم افزار مدیریت سرور و دسترسی به تنظیمات کلاینت از سوی کاربر که به صورت متفاوت باید وارد شود.

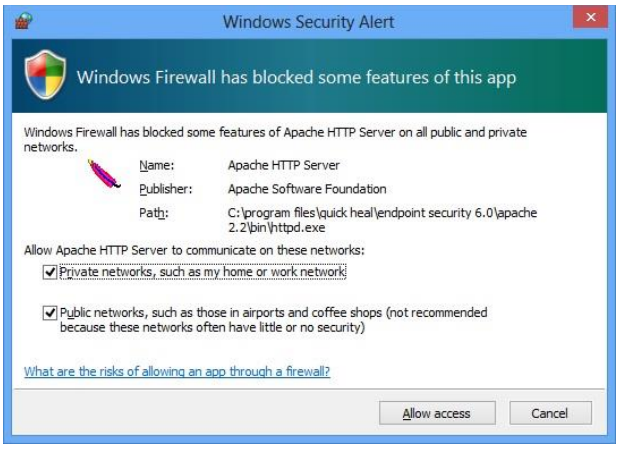


این صفحه خلاصه‌ای از تنظیمات اعمال شده و تایید مراحل کار انجام شده تاکنون را نمایش می‌دهد. برای ادامه بر روی Next کلیک کنید.

در این صفحه تنظیمات مربوط به پیکربندی IP و پورت نمایش داده می‌شود. در انتها به کاربر پیغامی مبنی بر قطع و وصل موقتی خودکار شبکه در هنگام نصب نمایش داده می‌شود.



شروع به نصب آنتی ویروس و کپی فایل‌های مورد نیاز می‌کند.



اگر فایروال ویندوز فعال باشد، اجازه‌ی اجرای Apache را با تیک کردن هر دو گزینه و با کلیک دکمه‌ی Allow Access صادر کنید.

توضیحاتی راجع به اندپوینت، برای ادامه بر روی Next کلیک کنید.

این صفحه به شما اطلاع می‌دهد کوییک‌هیل اندپوینت‌سکیوریتی با موفقیت نصب شده است. تیک بودن Register Quick Heal Endpoint Security، صفحه‌ی رجیستر و ثبت محصول را نمایش داده و گزینه‌ی Configure Update Manager، پنجره پیکربندی مدیریت آپدیت را نمایش خواهد داد.

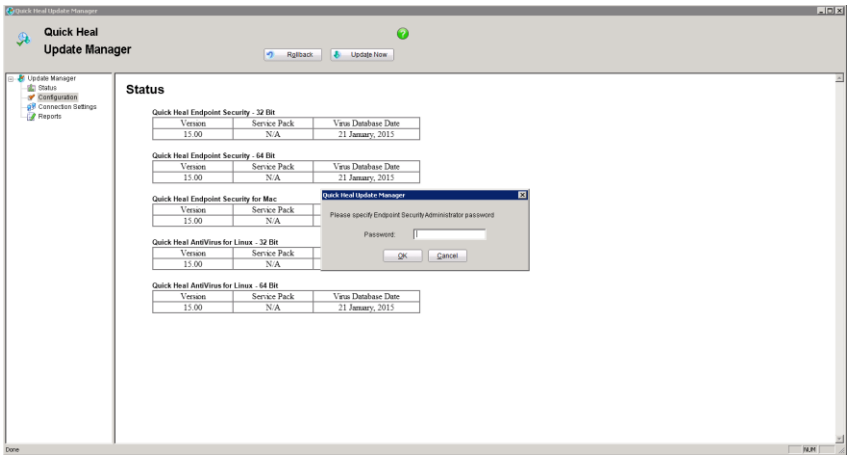
اگر سرور به اینترنت دسترسی نداشته باشد، پنجره فوق نمایش داده می‌شود. ابتدا سرور را به اینترنت متصل کرده و بر روی دکمه Retry کلیک کنید.

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

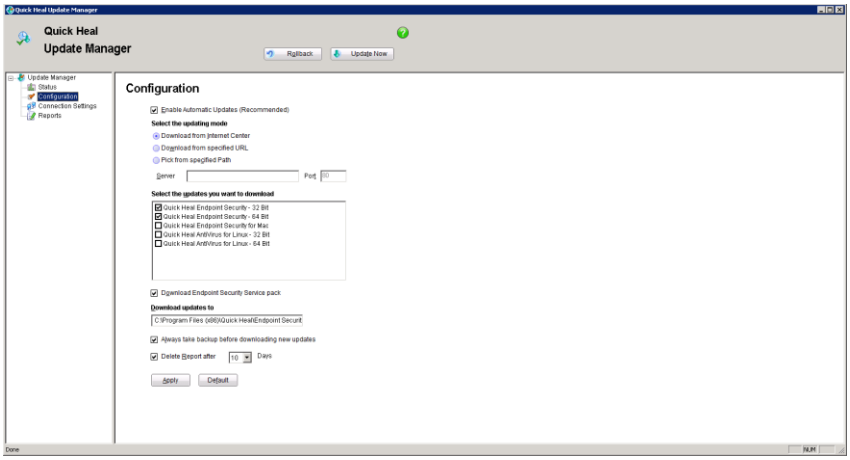
لایسنس یا کلید محصول خود را وارد نمایید. اگر برای اولین بار نصب انجام می گیرد پس از وارد کردن لایسنس، در صفحات بعدی اطلاعات زیر را تکمیل کنید:

Purchased from: Fanoos ICT Co
Register for: Company use / Educational
Name: نام سازمان/شرکت خریدار

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



این قسمت مربوط به تنظیمات نرم افزار Update Manager می باشدکه جهت ورود به تنظیمات می بایست رمز عبور نرم افزار اندپوینت وارد شود.



تنظیمات مربوط به مدیریت آپدیت می باشد که این تنظیمات شامل موارد زیر می باشد:

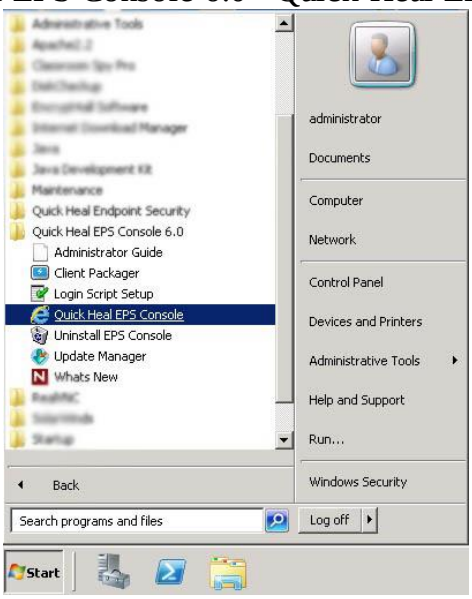
- گرفتن آپدیت بصورت خودکار
- انتخاب نوع آپدیت: آپدیت را از اینترنت یا از آدرس خاص از کامپیوتر دیگر در شبکه محلی دریافت کند.
- انتخاب نوع محصول برای آپدیت (ویندوز ۳۲ بیتی، ویندوز ۶۴ بیتی، لینوکس ۳۲ بیتی، لینوکس ۶۴ بیتی و Mac) که بسته به نوع کلاینت‌های موجود در شبکه خود می‌توانید هر کدام از گزینه‌ها را انتخاب نمایید.
- انتخاب مسیر ذخیره فایل‌های آپدیت
- بکاپ گرفتن از آپدیت های قبلی، قبل از گرفتن آپدیت جدید
- حذف گزارش دریافت Update بعد از تعداد روز انتخاب شده
- تغییرکلمه رمز عبور

این صفحه نشان می‌دهد که نصب و فعالسازی با موفقیت به پایان رسید.

آغاز به کار کنسول مدیریتی متمرکز اندپوینت‌سکیوریتی کوییک‌هیل

۱. اجرای کنسول کوییک‌هیل اندپوینت‌سکیوریتی از روی سرور:

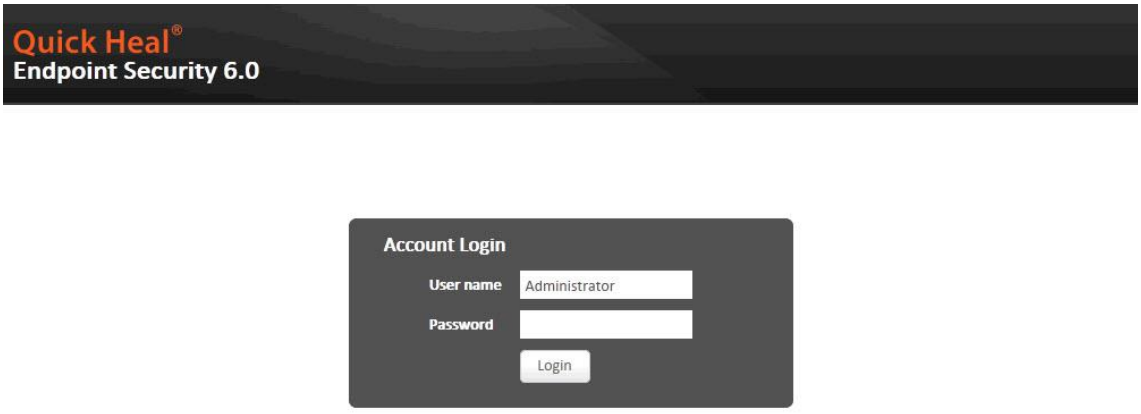
Start > Quick Heal EPS Console 6.0> Quick Heal EPS Console



همچنین می‌توانید کنسول مدیریتی تحت وب اندپوینت را از روی سرور و یا هر یک از کلاینت‌های 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:

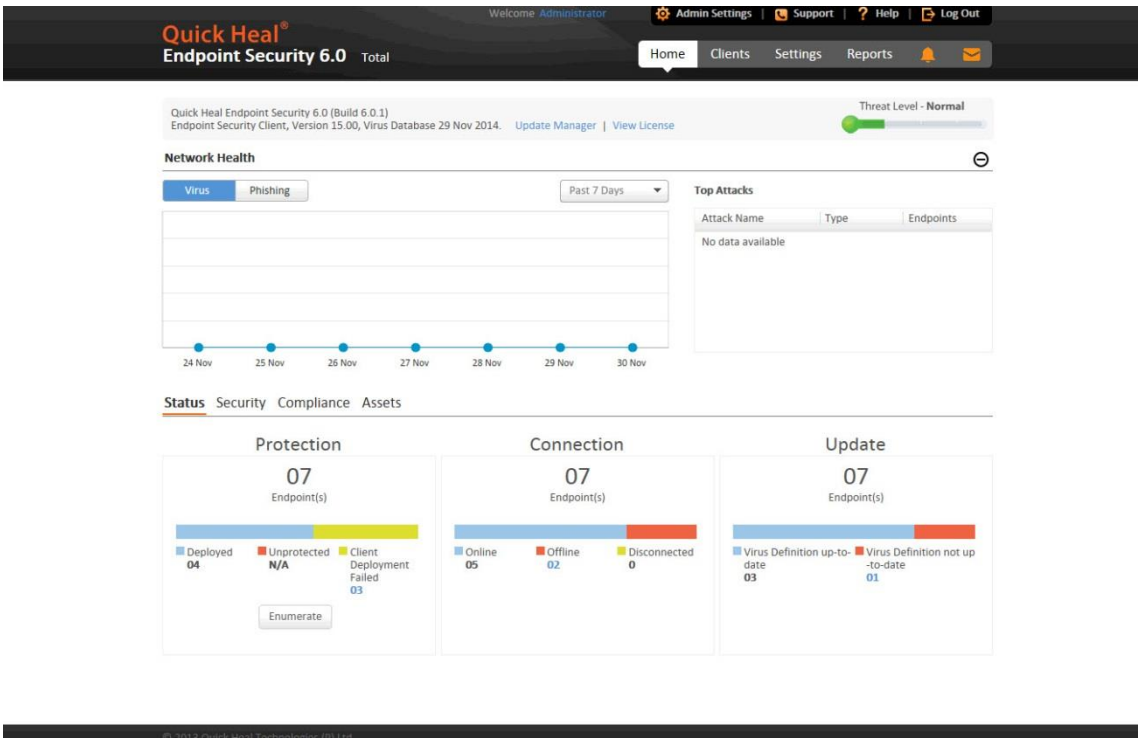
https://IP-Server:9099/qhscan6

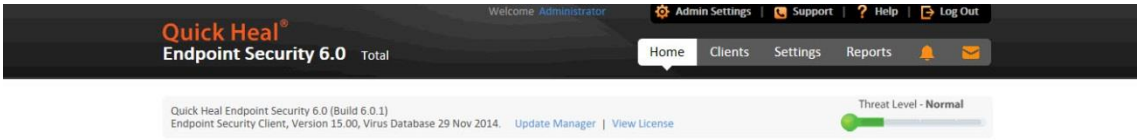
۲. نام کاربری پیش فرض Administrator و رمز عبور، همان رمز مدیریتی است که در زمان نصب تعریف نمودید.



داشبورد مدیریتی

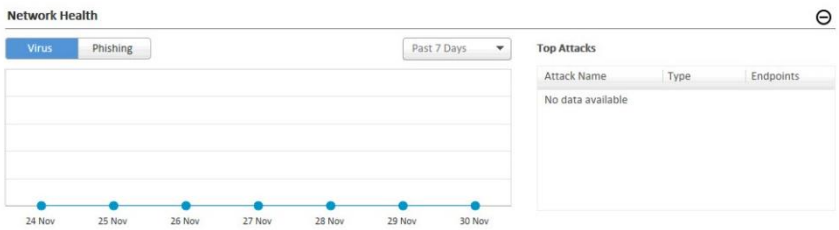
صفحه نخست (داشبورد) خلاصه اطلاعاتی راجع به مسائل امنیتی شبکه ارائه می‌دهد.





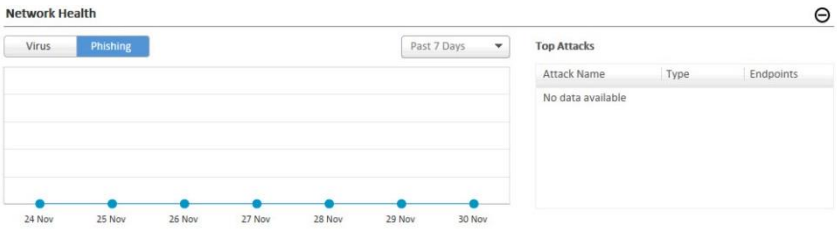
در نوار طوسی رنگ، نام و نسخه محصول به همراه تاریخ بروزرسانی نمایش داده می‌شود. با کلیک بر روی Update Manager می‌توانید وضعیت بروزرسانی اندپوینت را مشاهده و یا تنظیمات دلخواه را اعمال نمایید. اطلاعات مربوط به لایسنس از طریق لینک View License در دسترس می‌باشد. سطح تهدید در شبکه با نمودار رنگی (سبز=عادی،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

۱. وضعیت امنیت شبکه سازمان (ویروس)



باکس Network Health به صورت گرافیکی وضعیت امنیتی و سلامت شبکه را نمایش می‌دهد. سربرگ نخست (Virus)، اطلاعات مربوط به وضعیت انتشار ویروس‌ها را به صورت نمودار نشان می‌دهد. از طریق فرم بازشو View form می‌توانید 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 ها می‌توانید اطلاعات ویروس و کلاینت آلوده مربوطه را دریافت نمایید. سمت چپ این سربرگ در بخش Top Attacks کلاینت‌هایی که بیشترین آلودگی را داشته‌اند لیست می‌شوند.

۲. وضعیت امنیت شبکه سازمان (فیشینگ)



با کلیک بر روی دکمه Phishing، اطلاعات مربوط به وضعیت سایت‌های آلوده و کلاهبردارانه که کاربران قصد بازدید از آنها را داشتند ولی کوییک‌هیل مانع بازدید شده است را به صورت نمودار نشان می‌دهد. سمت چپ این سربرگ در بخش Top Attacks کلاینت‌هایی که بیشترین قصد بازدید از سایت‌های فیشینگ را داشته‌اند لیست می‌کند.

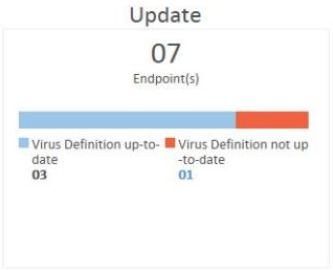
۳. وضعیت کلاینت‌های سازمان (Status)

در ادامه‌ی صفحه، اطلاعات امنیتی سازمان توسط کوییک‌هیل اندپوینت‌سکیوریتی به صورت نمودار و جامع نمایش داده می‌شود. در سربرگ اول (Status) نمای کلی از وضعیت اندپوینت‌سکیوریتی نمایش داده می‌شود:

الف) Protection: در این بخش وضعیت نصب کلاینت‌ها نمایش داده می‌شود. تعداد کل کلاینت‌ها (Endpoints)، تعداد کلاینت‌های نصب شده (Deployed Clients) و تعداد کلاینت‌هایی که هنوز کوییک‌هیل

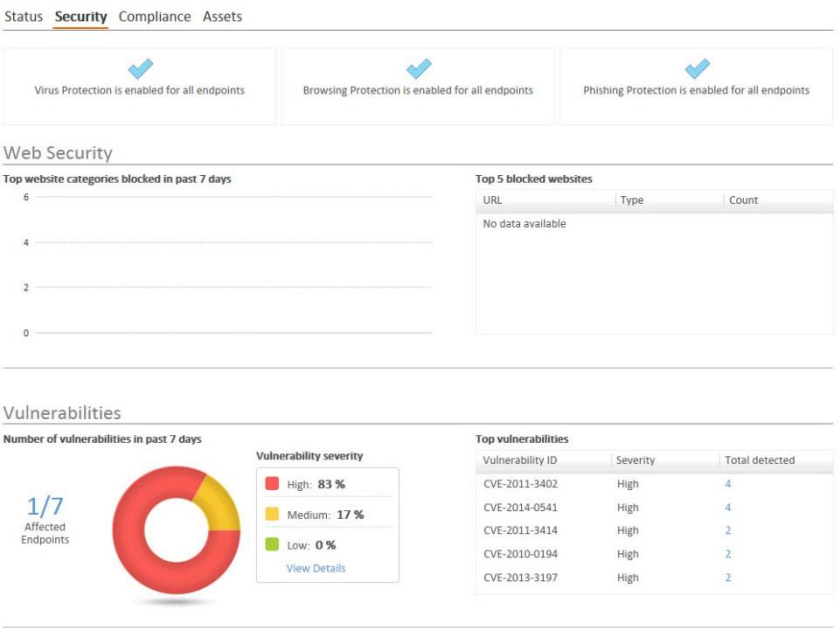
ایجنت برروی آنها نصب نشده و غیرمحافظت شده می‌باشند (Unprotected Computers in the network) و همچنین تعداد کلاینت‌هایی که نصب با موفقیت بر روی آنها صورت نپذیرفته (Client Deployment Failed) نشان داده می‌شود. با کلیک بر روی Enumerate Now، اندپوینت به دنبال تعداد کلاینت‌های جدید در شبکه می‌گردد.

ب) *Connection*: در این بخش وضعیت کلاینت نشان داده می‌شود. تعداد کل کلاینت‌هایی که کوییک‌هیل بر روی آنها نصب شده است (Endpoints)، تعداد کلاینت‌هایی که هم اکنون روشن و آنلاین بوده و ارتباط با سرور دارند (Online)، تعداد کلاینت‌هایی که هم اکنون آفلاین، خاموش و یا ارتباط شبکه ای با سرور ندارند (Offline)، تعداد کلاینت‌هایی 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، (Disconnected) نمایش داده می‌شود.



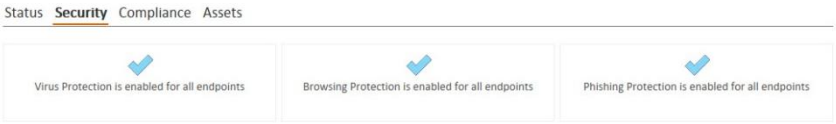
ج) *Update*: وضعیت بروزرسانی در این بخش نشان داده می‌شود. تعداد کلاینت‌ها (Endpoints)، تعداد کلاینت‌های بروز شده (Virus Definition up-to-date) و تعداد کلاینت‌هایی که آپدیت نشده اند (Virus Definition not up-to-date) در این بخش نمایش داده می‌شود.

٤. وضعیت امنیتی سازمان (*Security*)



در سربرگ دوم (Security) نمای کلی از امنیت شبکه سازمان نمایش داده می‌شود:

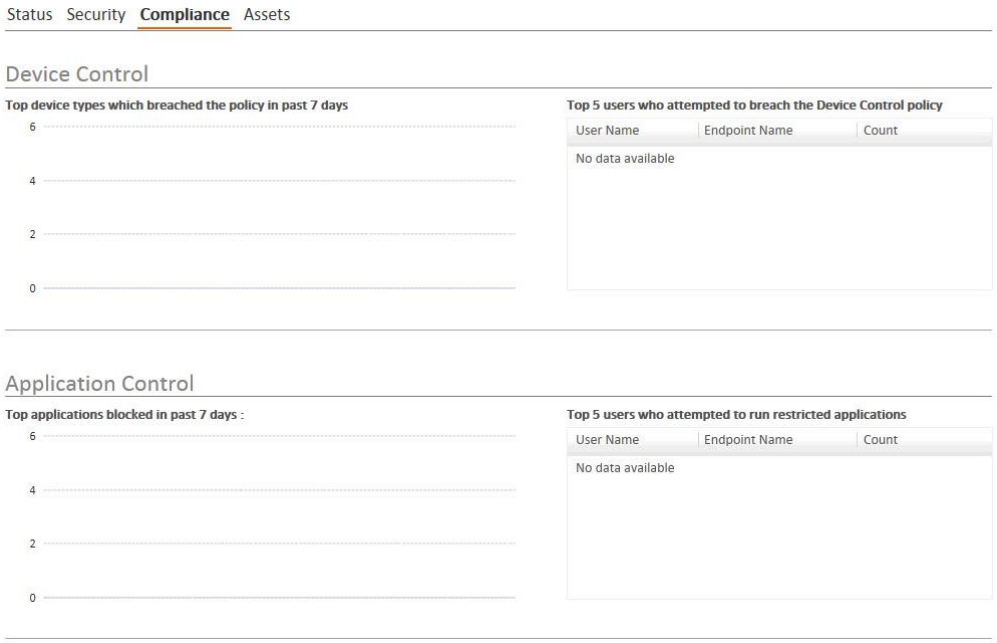
الف) Security: در این بخش می توانید اطلاعات کلی از نحوه برقراری امنیت و فعال بودن ماژول‌های امنیتی کلاینت های خود داشته باشید. در صورتی که محافظت ویروس بر روی همه کلاینت‌ها فعال باشد عبارت (Virus Protection is enabled for all endpoints)، اگر محافظت مرورگر و اینترنتی بر روی همه کلاینت‌ها فعال باشد عبارت (Browsing Protection is enabled for all endpoints) و در صورتی که محافظت فیشینگ و مقابله با سایت‌های کلاهبردارانه بر روی همه کلاینت‌ها فعال باشد، عبارت (Phishing Protection is enabled for all endpoints) نشان داده می‌شود.



ب) Web Security: در این بخش اطلاعات مربوط به امنیت وب نشان داده می‌شود. در این بخش می‌توانید اطلاعات مربوط به تعداد سایت‌های آلوده و نیز مسدود شده توسط مدیر که کاربران قصد مشاهده آنها را داشتند را ملاحظه نمایید. در صورتی که مدیر، یک گروه از سایت‌ها و یا آدرس‌های اینترنتی خاصی را مسدود نماید، لیست پربازدیدترین گروه‌ها در سمت چپ و پر بازدیدترین آدرس‌های اینترنتی در سمت راست نشان داده می‌شود.

ج) 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. در سمت راست (Top vulnerabilities) میزان خطرپذیری حفره‌های کلاینت‌های شبکه، بسته به میزان تهدید آسیب پذیری لیست می‌شوند.

۵. وضعیت مدیریت ابزار و برنامه سازمان (*Compliance*)

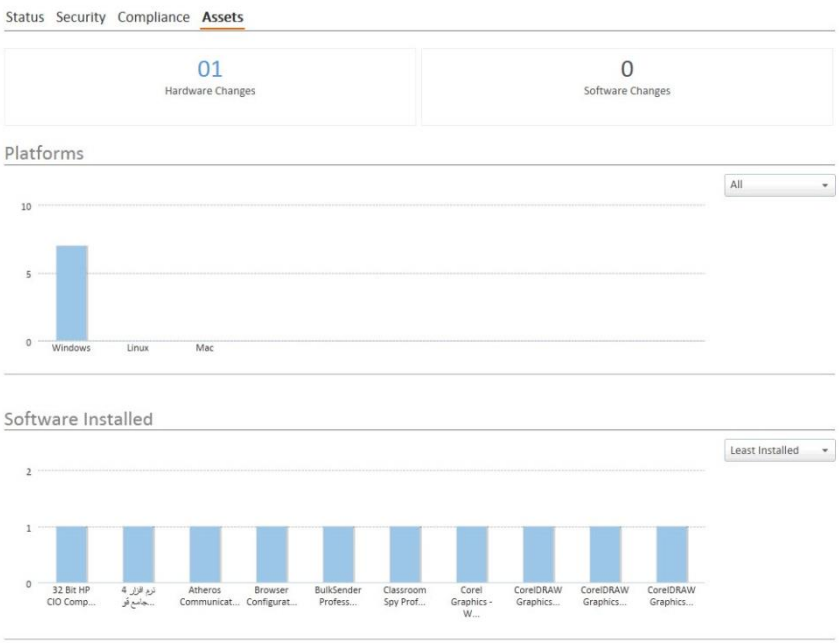


در سربرگ دوم (Compliance) نمای کلی از وضعیت مدیریت بر روی ابزارها و برنامه‌های کلاینت‌های سازمان نمایش داده می‌شود:

الف) Device Control: در صورتی که از گزینه‌ی مسدود کردن دستگاه های حافظه های جانبی USB (فلش، هارد اکسترنال)، CD/DVD Rom، بلوتوث، WiFi و... استفاده نمایید، اطلاعات مربوط به مسدودسازی آنها در این بخش قابل مشاهده می‌باشد. می‌توانید انواع دستگاه های مسدود شده ای که در ۷ روز اخیر قصد شکستن سیاست‌گذاری مربوطه را داشتند را در سمت چپ به صورت نمودار گرافیکی مشاهده فرمایید. در سمت راست اطلاعات ۵ کاربری که بیشترین قصد را برای نقض سیاست‌گذاری کنترل ابزار را داشتند لیست می‌شوند.

ب) *Application Control*: در این بخش اطلاعات مربوط به کنترل برنامه و مسدودسازی برنامه‌ها ارائه می‌گردد. در سمت چپ اطلاعات بیشترین برنامه‌های ممنوعه در ۷ روز اخیر را نشان می‌دهد. در سمت راست اطلاعات ۵ کاربری که بیشترین تلاش برای اجرای برنامه‌های مسدود شده را داشتند، لیست می‌شوند.

۶. وضعیت دارایی‌های سرمایه‌ای سازمان (*Assets*)

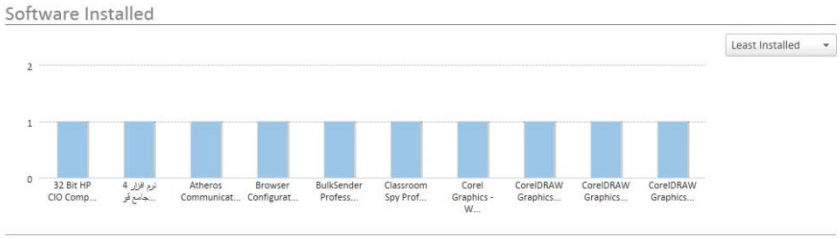


در سربرگ چهارم (Assets) نمای کلی از دارایی‌های سازمان شامل مشخصات سخت‌افزاری و نرم‌افزاری کلاینت‌های شبکه سازمان نمایش داده می‌شود:

الف) *Assets*: در آغاز این سربرگ، هرگونه تغییرات سخت افزاری (Hardware Changes) و نرم‌افزاری (Software Changes) صورت پذیرفته بر روی کلاینت‌ها لیست می‌شوند. با کلیک بر روی تعداد تغییر می‌توانید از اطلاعات کلاینت‌ها و تغییر صورت پذیرفته بر روی آنها مطلع گردید.

ب) *Platforms*: در این بخش، اطلاعات پلتفرم‌ها و سیستم‌های عاملی که در شبکه استفاده می‌شوند لیست می‌شود. این اطلاعات شامل نام و تعداد سیستم عامل (ویندوز، لینوکس و مک) که در سازمان مورد استفاده قرار می‌گیرد می‌باشد.

با کلیک بر روی All از منوی بازشونده و انتخاب نام کلی سیستم عامل (Windows / Linux / Mac) می‌توان اطلاعات کامل‌تری از آنها مثلاً نوع ویندوز و تعداد و مشخصات کلاینت‌ها را دریافت کرد.



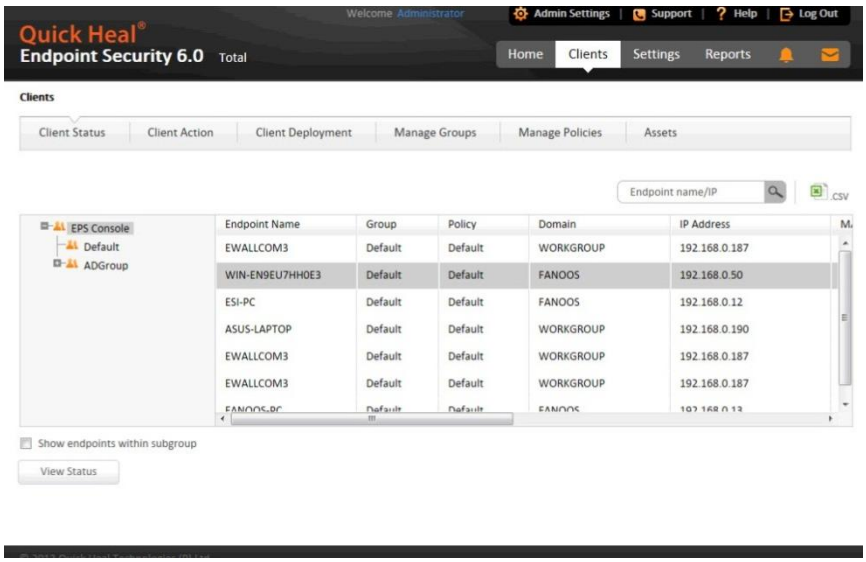
ج) *Software Installed*: در این بخش، لیست آخرین نرم‌افزارهای نصب شده بر روی کلاینت‌ها به همراه نمودار فراوانی مربوطه نمایش داده می‌شود.

با کلیک بر روی Latest Installed از منوی بازشونده و انتخاب Most Installed می‌توان لیست نرم‌افزارهایی که بیشترین نصب بر روی کلاینت‌ها را داشته اند به همراه جزئیات بیشتر دریافت کرد.

کلاینت ها Clients

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

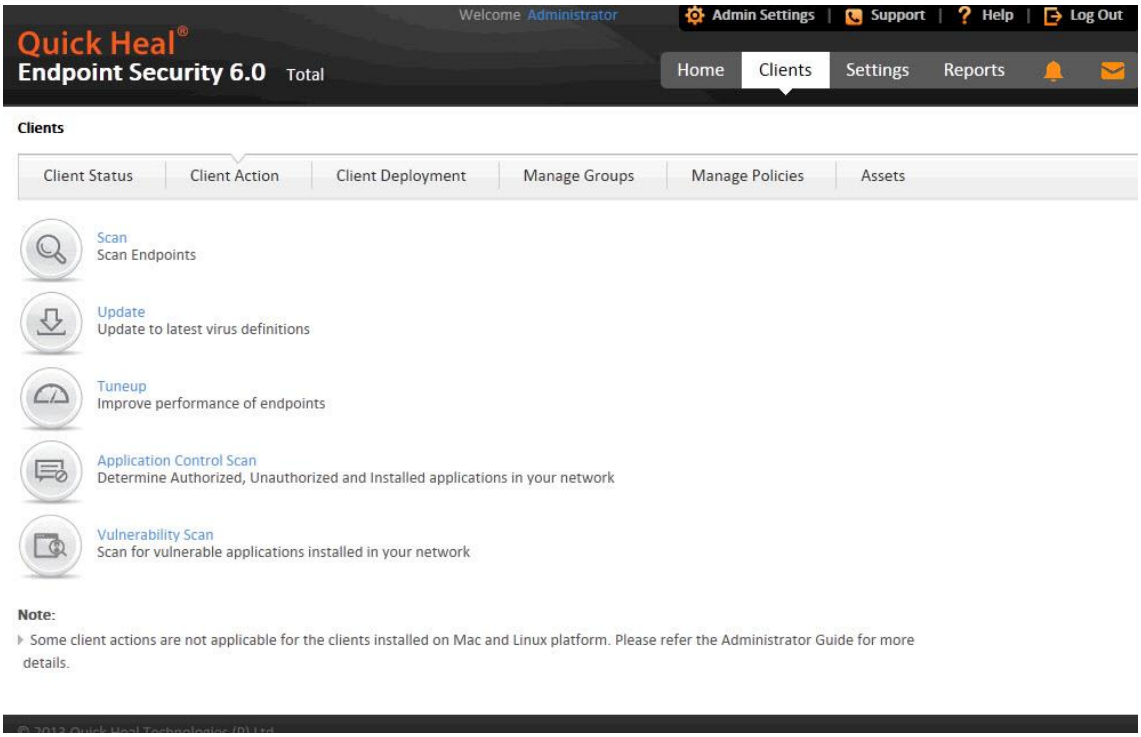
الف) Client Status



این سربرگ وضعیت کلاینت‌ها را نشان می‌دهد. در این صفحه می‌توانید کلاینت همه گروه ها و گروه‌های خاص را مشاهده نمایید. با کلیک بر روی نام گروه در درختواره سمت چپ می‌توانید 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 دکمه‌ی View Status، اطلاعات کاملی از کلاینت مربوطه ارائه می‌گردد. با تیک کردن گزینه Show computers within subgroup همه‌ی کلاینت های عضو زیرگروه انتخابی لیست می‌گردند.

ب) سربرگ Client Action:

عملیات قابل اجرا بر روی کلاینت‌ها در این صفحه لیست می‌شود:



.

در این صفحه می‌توانید از راه دور، کلاینت‌ها را ویروسیابی و اسکن نمایید. حتی امکان ارسال دستور اسکن زمان Boot نیز وجود دارد.

فرایند بروزرسانی کلاینت‌ها به صورت خودکار صورت می‌پذیرد. اما اگر مدیر شبکه بخواهد در مواردی خاص (مثلاً کلاینتی مدتی به شبکه متصل نبوده و مدیر می‌خواهد فوراً اقدام به بروزرسانی آن نماید) می‌تواند از راه دور دستور بروزرسانی کلاینت را صادر نماید.

مدیر شبکه می‌تواند یک یا گروهی از کلاینت‌ها را از راه دور بهینه سازی نماید تا با برطرف شدن مشکلات سیستم، سرعت و عملکرد رایانه‌ها بهبود یابد.

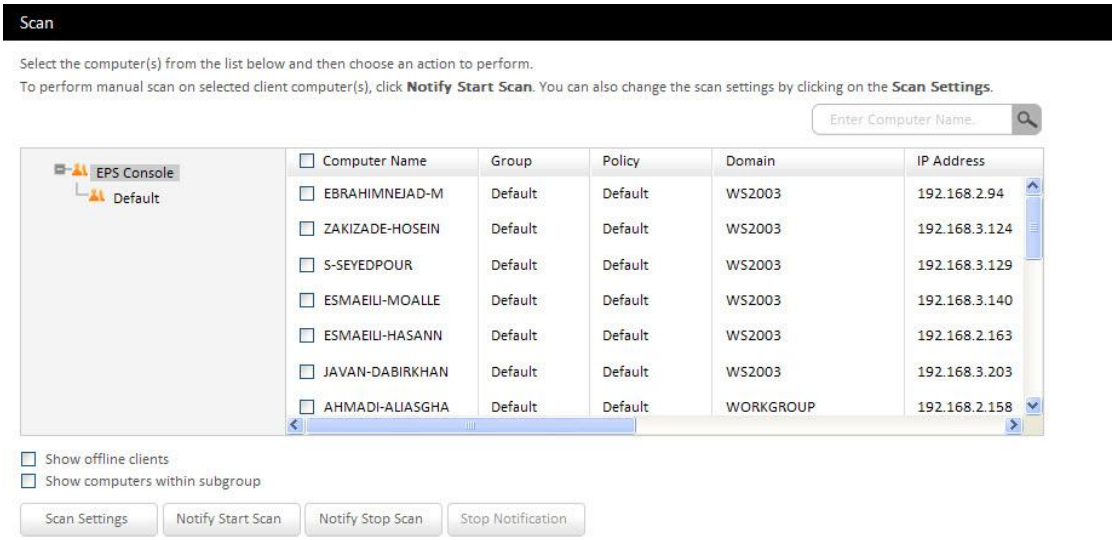
پویش و تولید گزارش از برنامه‌های نصب شده بر روی یک کلاینت و اعمال محدودیت اجرا در صورت اعمال سیاست‌گذاری از راه دور ممکن می‌باشد.

پس از نصب کوییک‌هیل برروی کلاینت‌ها گزارش کاملی از کلیه دارایی‌های سخت‌افزاری و نرم‌افزاری به همراه لیست کلیه آسیب‌پذیری‌های کلاینت‌ها تولید و به سرور ارسال می‌گردد.

همچنین امکان اسکن، بروزرسانی بهینه‌سازی، کنترل برنامه‌ها و اسکن آسیب‌پذیری به صورت برنامه‌ریزی شده، در زمان‌های خاص و به صورت خودکار وجود دارد.

Scan:

برای اسکن و ویروسیابی کلاینت‌ها از راه دور از این گزینه استفاده می‌شود. با کلیک بر روی این گزینه پنجره جدیدی باز می‌شود که می‌توانید کلاینت‌های مورد نظر را از گروه مربوطه انتخاب و اسکن نمایید.



از طریق جعبه متنی بالایی می‌توانید نام یا IP کامپیوتر موردنظر را جستجو نمایید.

برای نمایش کلاینت‌های آفلاین گزینه Show offline clients را تیک کنید.

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

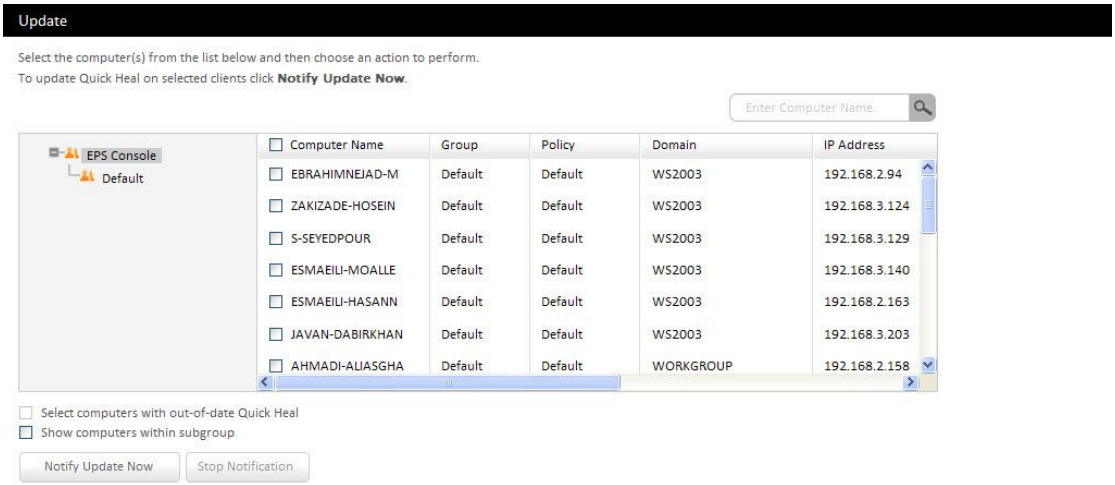
تنظیمات اسکن از طریق دکمه Scan Settings قابل تغییر می‌باشد.

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

در صورتی که می‌خواهید 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 می‌توانید بر روی Stop Notification کلیک کنید تا ارسال دستور، متوقف گردد.

Update:



بروزرسانی کلاینت‌ها 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، می‌توانید از این گزینه استفاده نمایید.

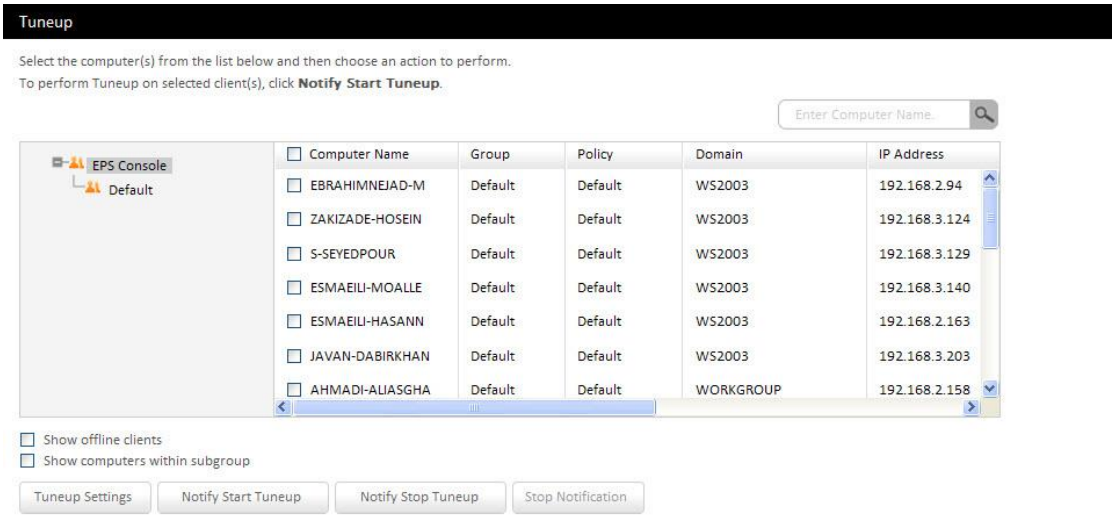
Select computers with out-of-date Quick Heal: این گزینه کامپیوترهای بروز نشده را انتخاب می‌کند.

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

Stop Notification: ارسال دستور بروزرسانی را متوقف می‌کند.

Tuneup:

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



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

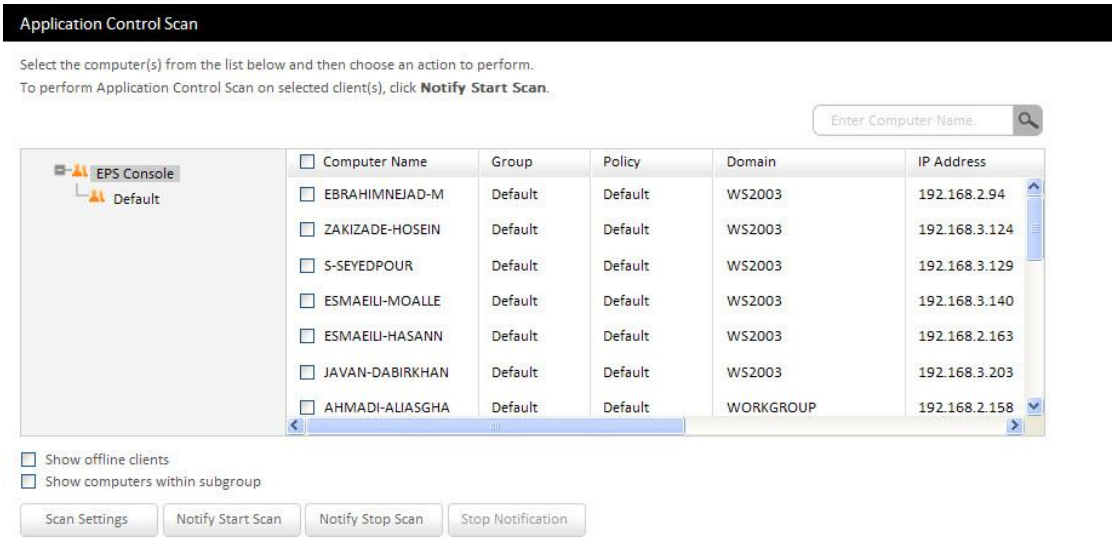
Notify Start Tuneup: ارسال دستور شروع بهینه سازی به کلاینت/کلاینت‌های انتخابی.

Notify Stop Tuneup: ارسال دستور توقف بهینه سازی به کلاینت/کلاینت‌های 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 کلاینت‌های مورد نظر نموده و گزارش آن را در بخش Report ملاحظه فرمایید.



Scan Settings: با کلیک بر روی این دکمه می‌توانید تنظیمات اسکن برنامه ها را تغییر دهید. می‌توانید 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.

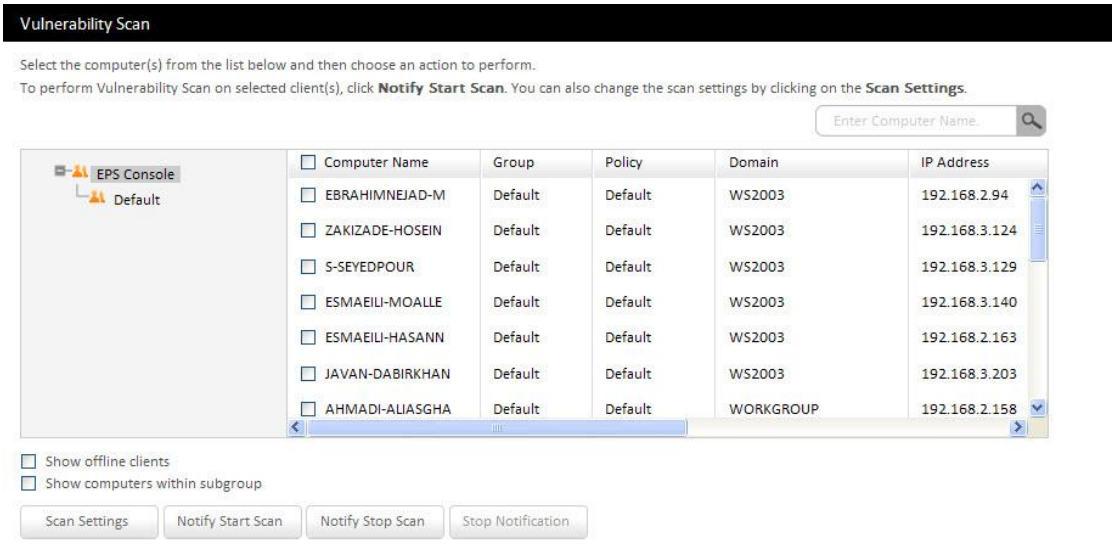
Notify Start Scan: ارسال دستور شروع به کار اسکن برنامه ها به کلاینت/کلاینت‌های انتخابی.

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

Stop Notification: توقف فرایند ارسال دستور به کلاینت.

Vulnerability Scan:

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

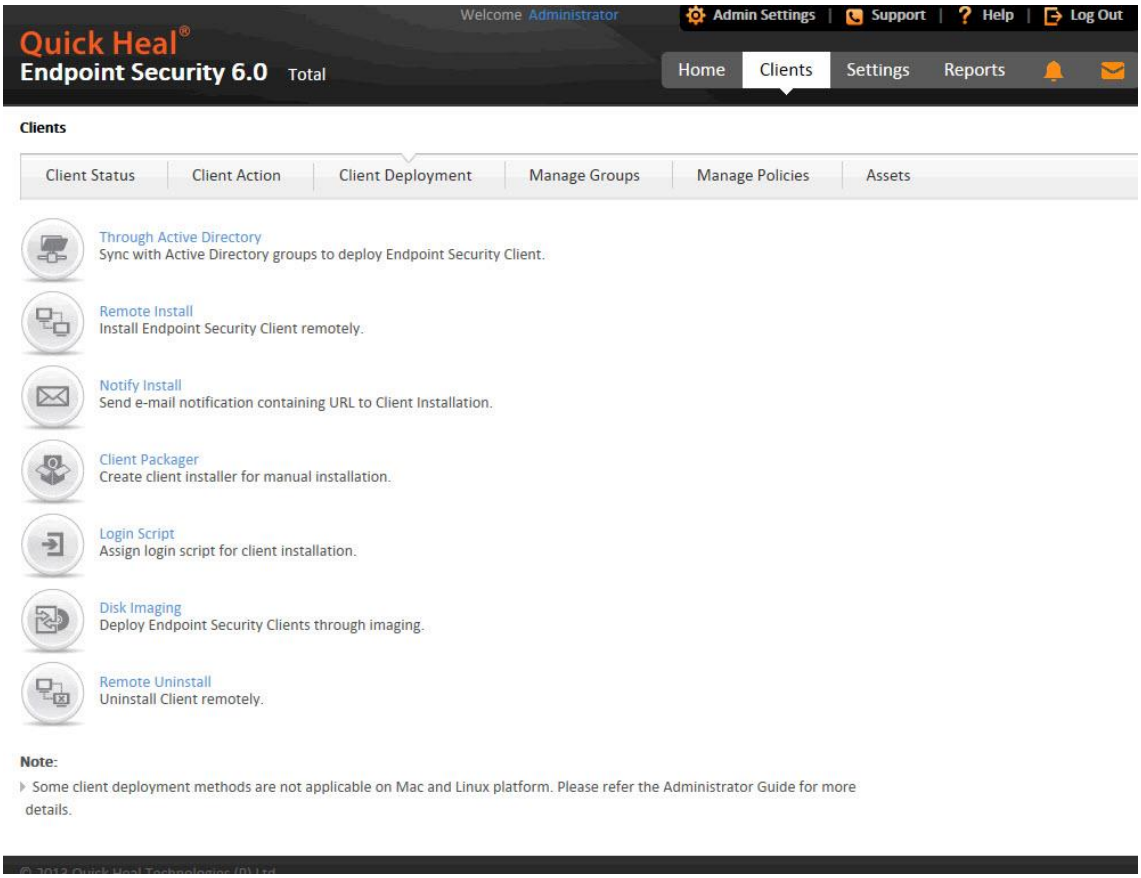


با کلیک بر روی Scan Settings می‌توانید تعیین کنید که آسیب‌پذیری های مایکروسافت و شرکت‌های دیگر یا فقط آسیب‌پذیری های مایکروسافت و یا تنها آسیب‌پذیری های شرکت‌های دیگر مورد بررسی و کاوش قرار گیرند.

- ✓ 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 کلاینت‌ها در این بخش انجام می‌پذیرد.



اندپوینت‌سکیوریتی کوییک‌هیل از ٦ روش نصب و یک روش حذف پشتیبانی می‌کند. متناسب با پیکربندی شبکه و مطابق سلیقه خود می‌توانید یکی از این ٦ روش نصب را استفاده می‌کنیم.

١. Through Active Directory: با استفاده از این ویژگی می‌توانید نصب Client Agent کوییک‌هیل را از طریق کنترلر دامنه Active Directory انجام دهید. برای ارتباط با سرور Active Directory ابتدا باید یک گروه جدید ایجاد و سپس با کلیک راست بر روی گروه گزینه‌ی synchronize with Active Directory را انتخاب و اطلاعات یک عضو با سطح دسترسی ادمین دامنه را به آن وارد نمایید. توضیحات بیشتر در صفحه‌ی ٣٦ راهنمای اندپوینت‌سکیوریتی ٦.٠ موجود است.

٢. Remote Install: امکان نصب کلاینت ایجنت کوییک‌هیل از راه دور در این قسمت پیش بینی شده است. راهنمای کامل‌تر در صفحه‌ی ٣٧ نمای اندپوینت‌سکیوریتی ٦.٠ موجود است.

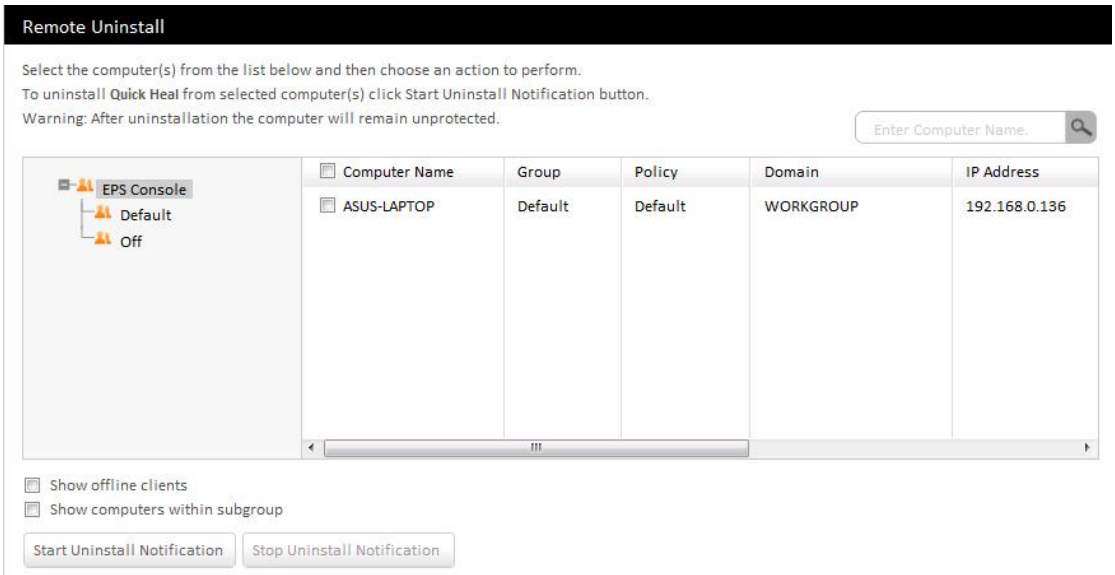
٣. Notify Install: در صورت تمایل می‌توانید با استفاده از این روش یک ایمیل اطلاع رسانی جهت نصب کوییک‌هیل به کاربران شبکه ارسال نمایید. این ایمیل شامل لینک نصب کوییک‌هیل می‌باشد. در ضمن می‌توانید این لینک (https://SERVER-IP:9099/qhscan6/install.htm) را از طریق IE بر روی هرکلاینت بدون ارسال ایمیل، اجرا نموده و اقدام به نصب از راه دور کوییک‌هیل نمایید.

٤. Client Packager: ساده‌ترین و کارآمدترین 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 می‌کنید. 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.

٥. Login Script: این روش تنها در شبکه های مبتنی بر دامنه قابل اجرا می‌باشد. 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 می‌دهید، 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.

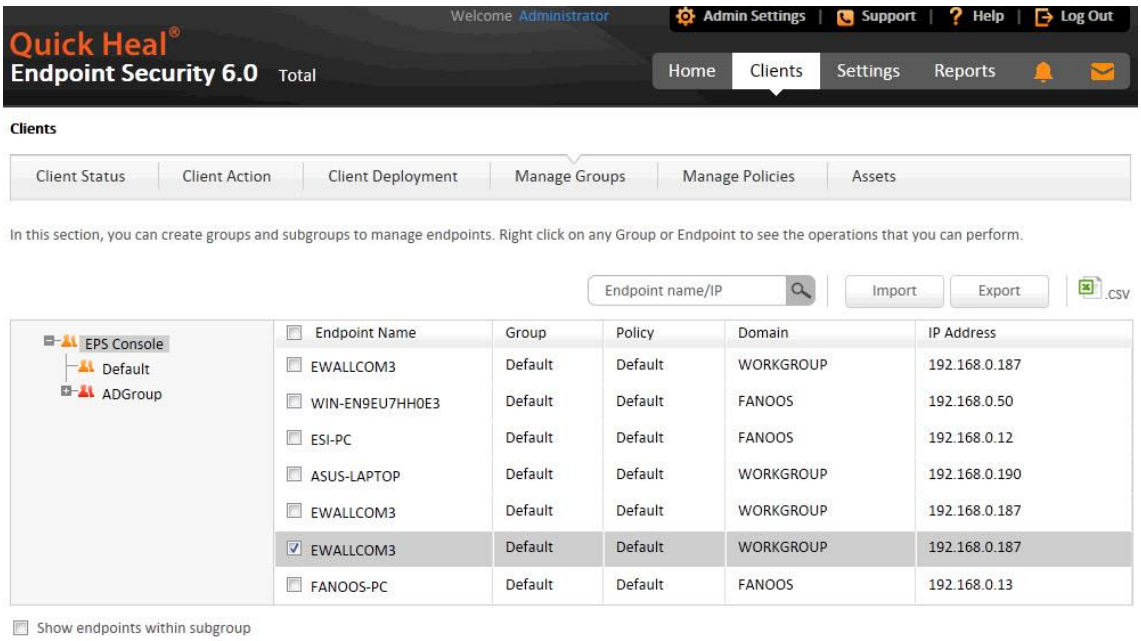
Remote Uninstall: اگر کاربر به هر شکلی کوییک‌هیل را از روی کلاینت حذف نماید، پس از راه‌اندازی مجدد، کوییک‌هیل به صورت خودکار بر روی آن نصب می‌گردد. برای حذف از روی کلاینت‌ها تنها مدیر می‌تواند از این گزینه استفاده نماید.



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 کلاینت‌ها را برعهده دارد.



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

پس از ایجاد و قراردادن کلاینت‌ها در گروه موردنظر، پالیسی باید بر روی این گروه اعمال گردد تا سیاست‌های خاص بر روی کلاینت‌های گروه اجرا شود. برای اعمال سیاست گذاری بر روی گروه کلیک راست کرده و گزینه Set Policy را انتخاب و از منوی بازشونده سیاستی که از قبل ساخته شده را انتخاب می‌کنیم. 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: می‌توانید یک زیرگروه به گروه موجود اضافه نمایید.

Delete Group: گروه مورد نظر حذف می‌گردد.

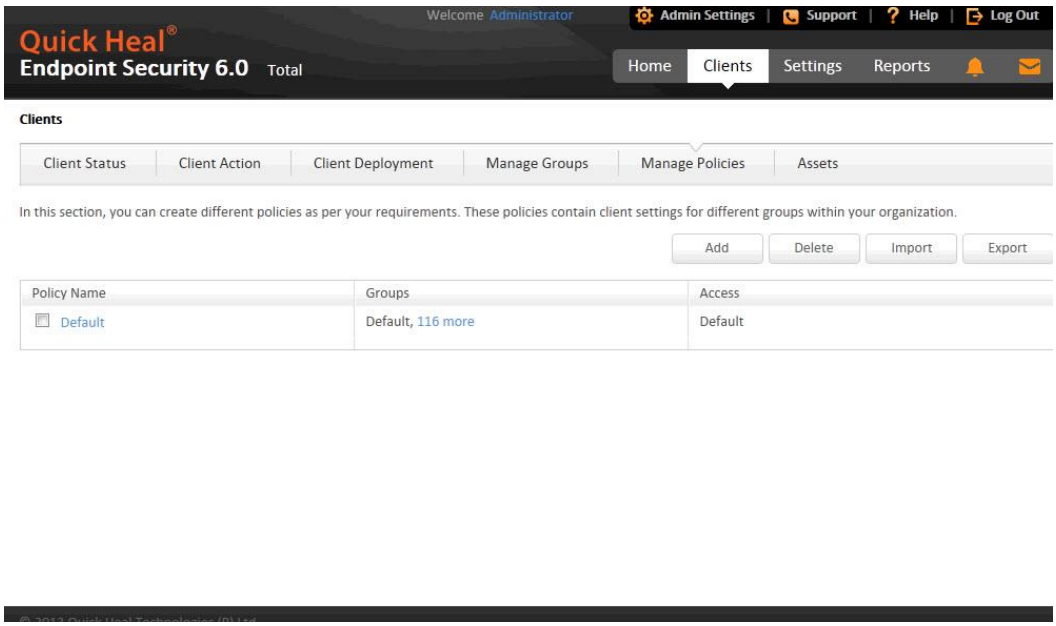
Rename Group: تغییر نام گروه، از این بخش صورت می‌پذیرد.

Import from Active Directory: در صورتی‌که می‌خواهید لیست کلاینت‌ها را از اکتیودایرکتوری وارد نمایید، از این گزینه استفاده می‌کنید.

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

هـ) سربرگ Manage Policy

این بخش مدیریت سیاست گذاری کلاینت‌ها را برعهده دارد.



در این بخش تعاریف مربوط به سیاست گذاری آنتی ویروس کلاینت‌ها صورت می‌پذیرد. همه تنظیمات آنتی ویروس کوییک‌هیل کلاینت‌های شبکه در این بخش قابل تعریف می‌باشد. با کلیک بر روی اسم هر پالیسی می‌توانید آن را ویرایش نمایید.

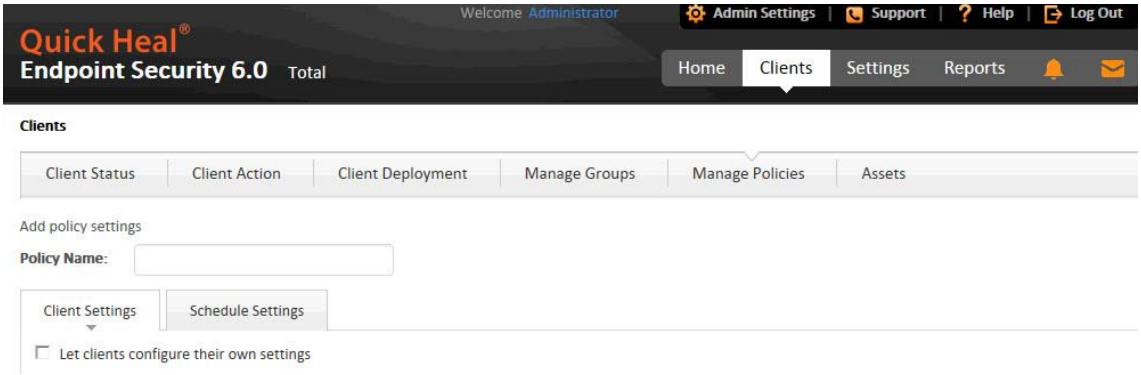
Add: افزودن سیاست گذاری.

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 می‌خواهید ایجاد نمایید را وارد نمایید.

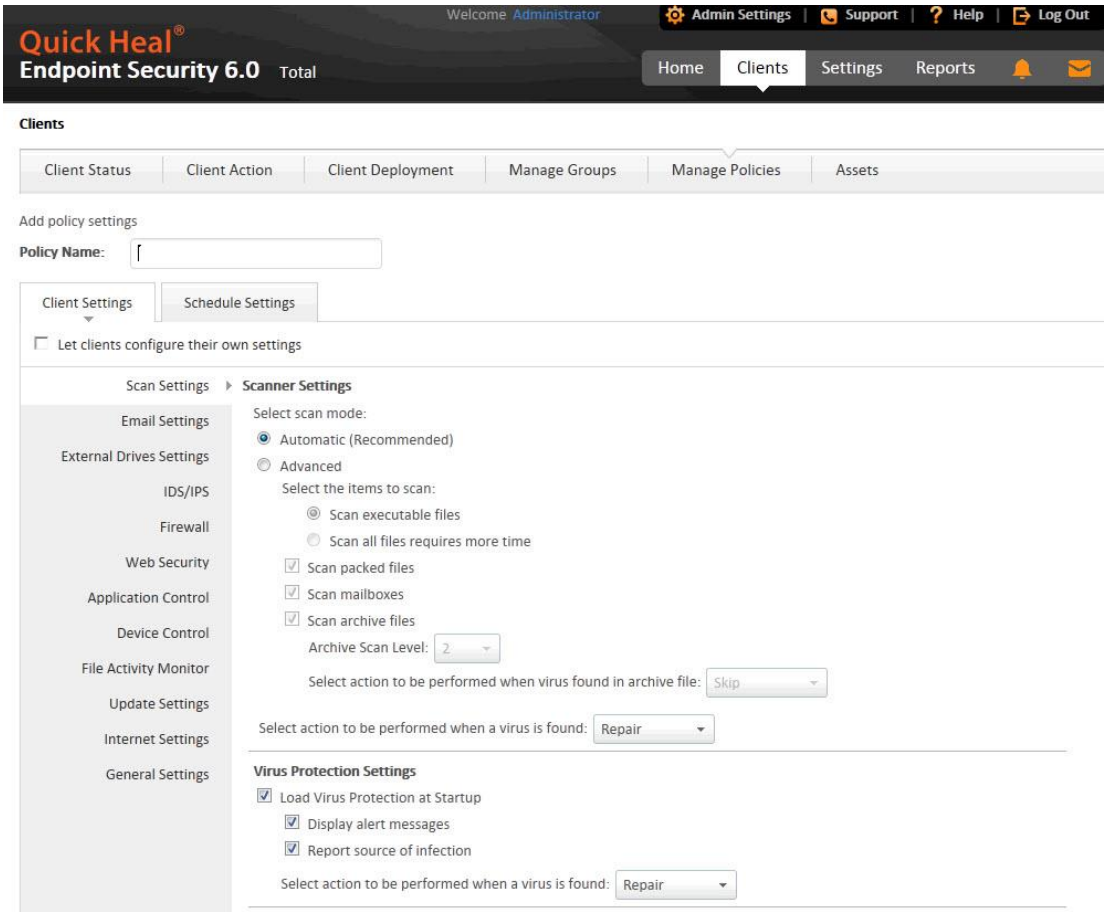
این صفحه دارای دو سربرگ Client Settings (تنظیمات کلاینت) و Schedule Settings (تنظیمات زمانبندی) می‌باشد.

سربرگ Client Settings

این سربرگ شامل تنظیمات اصلی پالیسی کلاینت‌ها می‌باشد.

Let clients configure their own settings: در صورتی که این گزینه تیک باشد، پیکربندی کلاینت‌های عضو این سیاست‌گذاری، از حالت متمرکز خارج شده و به آنها اجازه می‌دهیم 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 می‌توانید پیکربندی بیشتری را در حالت Advanced انجام دهید.

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

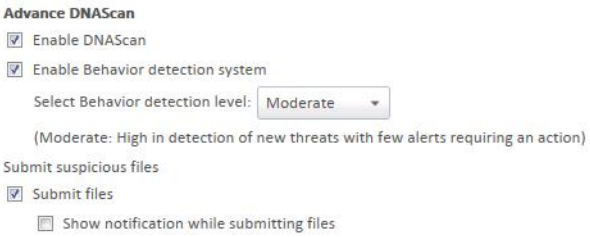
Virus Protection Settings

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) و یا از آن صرف‌نظر (Skip) می‌کند.

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 می‌کند.

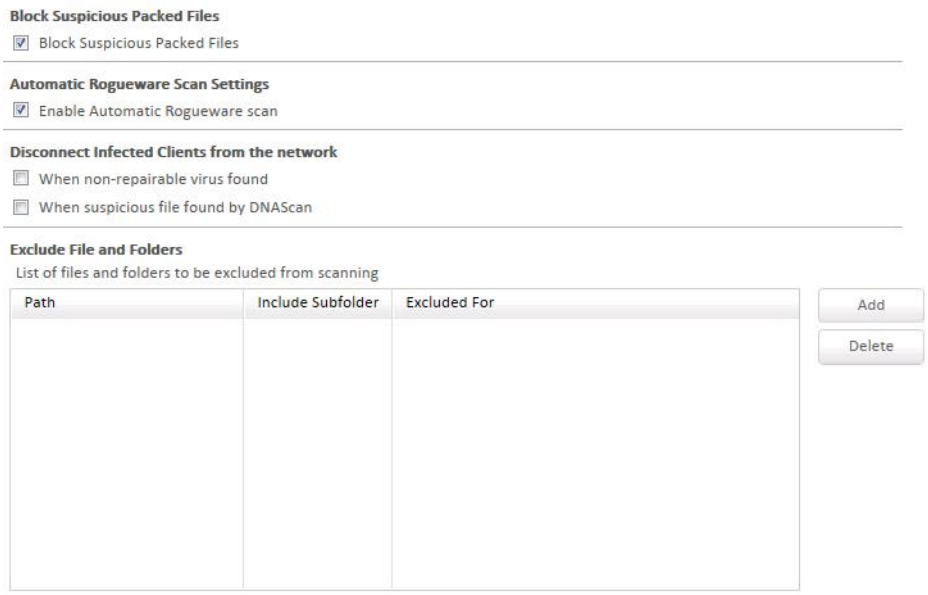
Enable DNAScan: با تیک بودن این گزینه دی.ان.ای اسکن کوییک‌هیل فعال می‌گردد.

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 می‌توانید 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 فایل های 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.

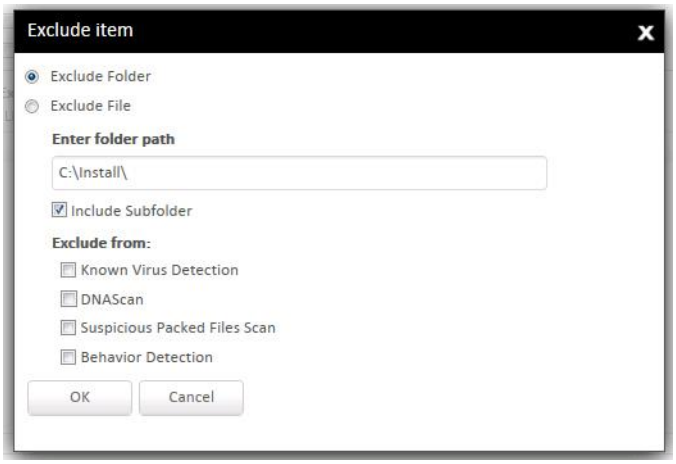
When non-repairable virus found: اگر این گزینه فعال بوده و ویروسی پیدا شود که قابل تعمیر نباشد، ارتباط کلاینت آلوده از شبکه قطع می‌گردد.

When suspicious file found by DNAScan: اگر این گزینه فعال بوده و فایل مشکوکی توسط DNAScan کوییک‌هیل پیدا شود، ارتباط کلاینت مشکوک از شبکه قطع 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 هایی که تمایل ندارید مورد اسکن قرار گیرند، می‌توانید فایل یا پوشه را از ویروسیابی شدن استثناء نمایید. پس از افزودن (Addکردن) آن فولدر یا فایل و افزوده شدن در لیست مربوطه، کلاینت‌های عضو آن پالیسی، فایل یا فولدر موردنظر را اسکن نمی‌کنند.

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



اگر می‌خواهید پوشه ای را از اسکن استثناء کنید گزینه‌ی Exclude Folder و اگر می‌خواهید فایل خاصی را استثناء کنید گزینه‌ی Exclude File را انتخاب کنید.

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

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

Exclude from: در این بخش موارد استثناء مشخص می‌گردد.

Known Virus Detection: با تیک بودن این گزینه، همه ویروس‌های شناخته شده، از اسکن استثناء می‌گردند.

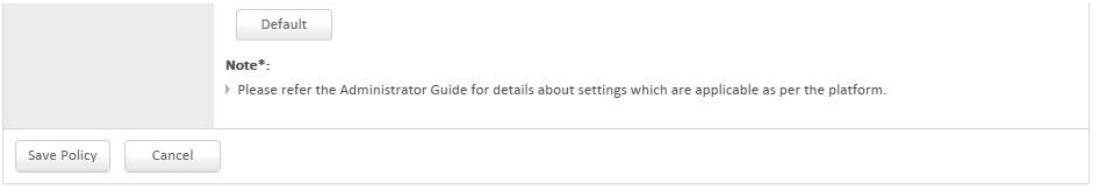
DNAScan: عدم پویش DNAScan از پوشه یا فایل مورد نظر در این بخش تعیین می‌گردد.

Suspicious Packed Files Scan: استثناء شدن از اسکن فایل‌های بسته ای مشکوک.

Behavior Detection: استثناء شدن از انجین رفتارشناسی کوییک‌هیل.

Exclude Extensions:

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

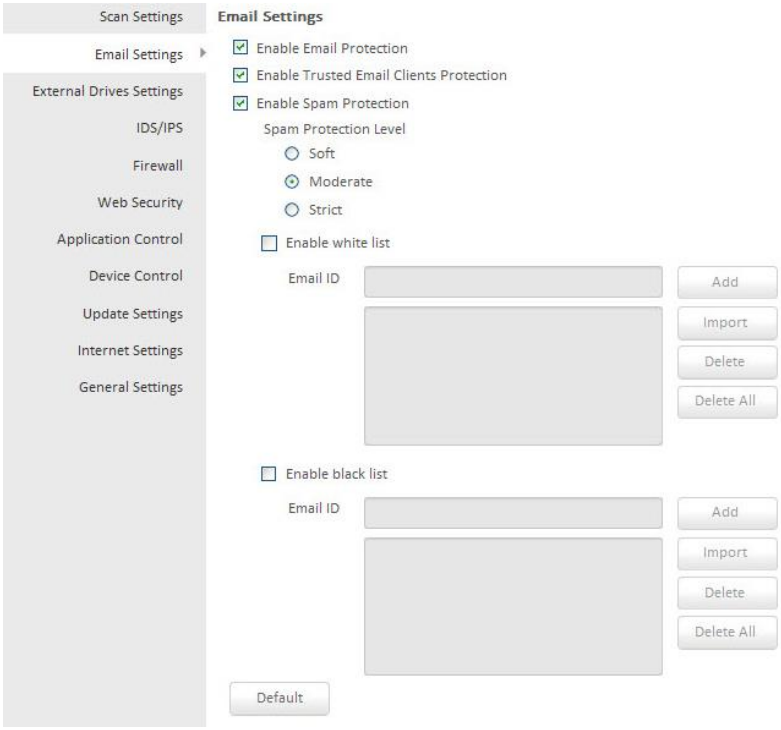


Default: تغییرات تنظیمات صورت گرفته را می‌توانید به حالت پیش فرض بر گردانید.

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 می‌توانید 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 کلاینت‌های ایمیل مطمئن (مانند Outlook) فعال می‌گردد.

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

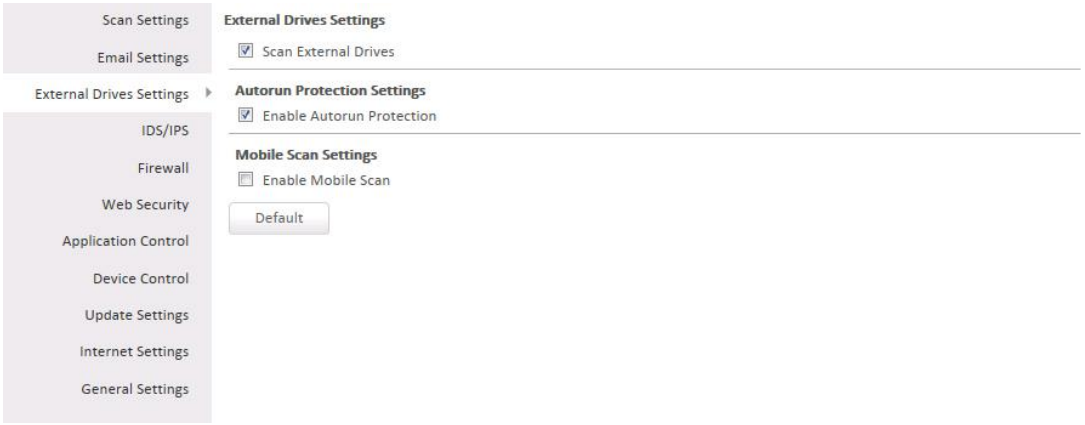
Spam Protection Level: این گزینه سطح حفاظت و دقت آنتی اسپم که می‌توان نرم (Soft)، متوسط (Moderate) و یا سخت (Strict) باشد را تعیین می‌کند.

Enable white list: با تیک کردن این گزینه لیست سفیدی از ایمیل ها را می‌توانید 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 می‌توانید تعیین نمایید که آنتی اسپم همواره آنها را به عنوان ایمیل مخرب و هرزنامه درنظر می‌گیرد.

External Drives Settings

این بخش شامل تنظیمات مربوط به اسکن دستگاه های خارجی می‌باشد.



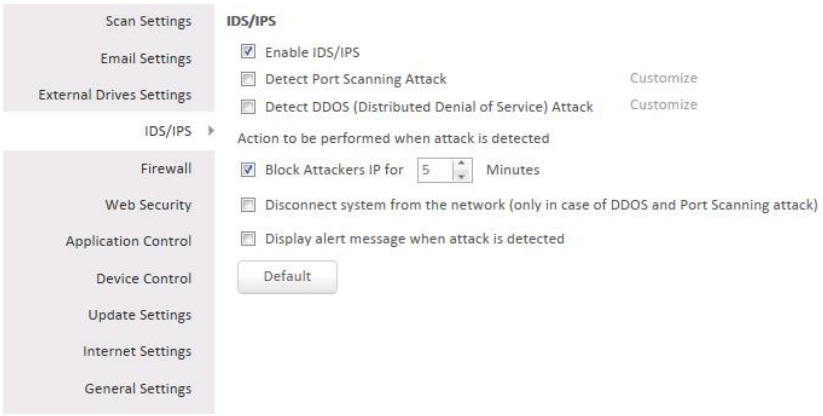
Scan External Drives: در صورتی که این گزینه تیک باشد، به محض اتصال فلش یا حافظه های USB، کوییک‌هیل به صورت خودکار اقدام به اسکن آنها می‌کند.

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

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 می‌کند 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 می‌کند تا پکت‌های شبکه ورودی و خروجی به کلاینت، مورد تحلیل قرار گرفته و مانع از اجرای حملات و نفوذ به سیستم‌های رایانه‌ای گردد. نسل اول فایروال‌ها کنترل حملات را تنها بر روی پورت انجام می‌دادند. از آنجا که برای برقراری ارتباط همواره باید پورت‌هایی بر روی کلاینت باز می‌بود، هکرها از آنها سوء استفاده می‌کردند. از این رو IDS/IPS رفتار پکت‌ها را بررسی کرده 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 می‌کند. با کلیک بر روی Customize، می‌توانید 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: عکس‌العملی که در هنگام شناسایی حملات صورت می‌گیرد در این بخش تعیین می‌گردد.

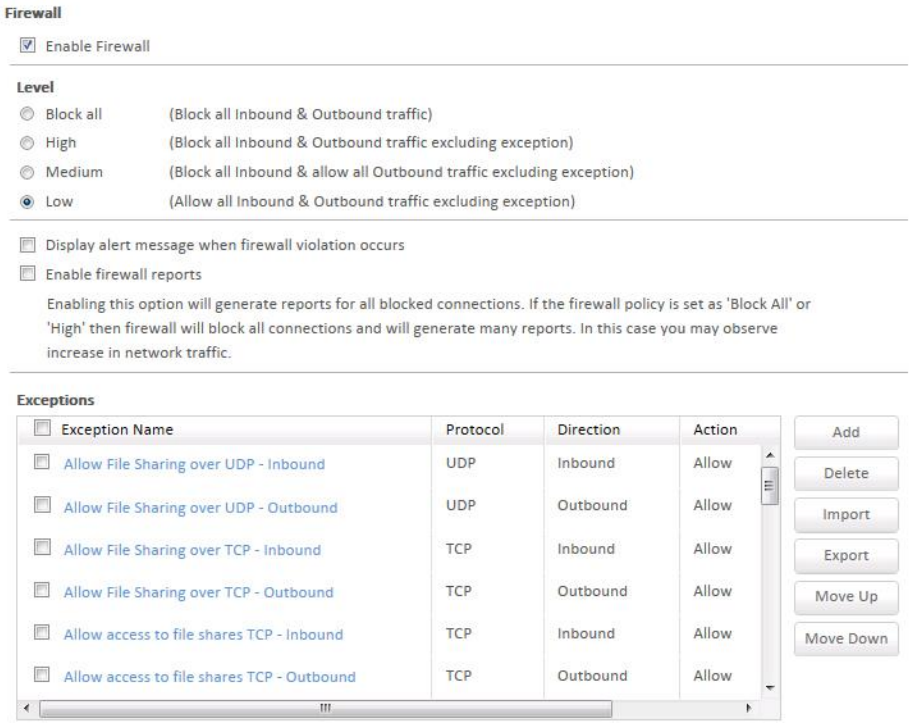
Block Attackers IP for: در این بخش می‌توانید آدرس های IP مهاجم را برای مدت زمانی به دقیقه مسدود نمایید.

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

Display alert message when attack is detected: در صورت بروز حملات، پیغام مناسب به کاربر نشان داده می‌شود.

Firewall

تنظیمات مربوط به فایروال کوییک‌هیل بر روی کلاینت‌ها در این بخش تعیین می‌گردند. ادمین می‌تواند با استفاده از رول‌های پیش فرض و یا تعریف رول جدید، پورت‌هایی 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 ترافیک‌های ورودی و خروجی به همه پورت‌ها را مسدود می‌کند.

High (Block all Inbound & Outbound traffic excluding exception): همه ترافیک‌های ورودی و خروجی را مسدود می‌کند بجز ترافیک‌هایی که در حالت استثناء قرار گرفته اند.

Medium (Block all Inbound & allow all Outbound traffic excluding exception): همه ترافیک‌های ورودی را مسدود کرده و همه ترافیک‌های خروجی و ترافیک‌هایی که در حالت استثناء قرار گرفته اند را مجاز می‌کند.

Low (Allow all Inbound & Outbound traffic excluding exception): همه ترافیک‌های ورودی و خروجی و همچنین استثناها را مجاز می‌کند.

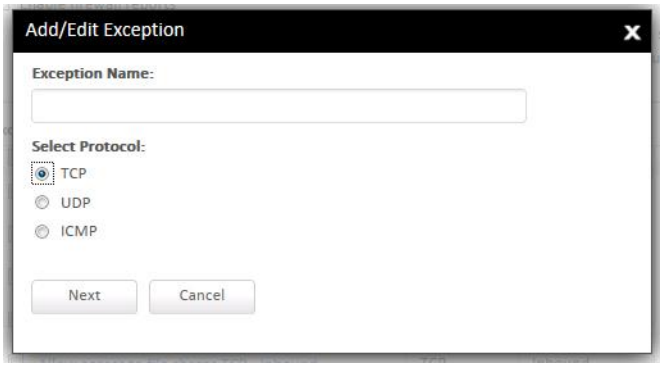
Display alert message when firewall violation occurs: اگر این گزینه فعال باشد، در هنگام حملات، فایروال پیغام اخطار مناسب به کاربران نشان می‌دهد.

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 استثناء (Exception Name)، پروتکل (Protocol) که می‌تواند TCP/UDP/ICMP باشد، جهت (Direction) که می‌تواند ورودی (Inbound) یا خروجی (Outbound) باشد، اقدام مربوطه (Action) که می‌تواند مجاز (Allow) یا غیرمجاز(Deny) و وضعیت (Status) که می‌تواند فعال (On) یا خاموش (Off) باشد قابل مشاهده است. با کلیک بر روی وضعیت جاری می‌توانید آن را فعال  و یا غیرفعال  کنید.

Add: برای افزودن رول استثنای جدید از این دکمه استفاده می‌شود. پس از فشردن این دکمه، صفحه‌ای باز می‌گردد که می‌توانید پورت خاصی را مجاز یا غیر مجاز نمایید. به عنوان مثال شما از یک برنامه اتوماسیون اداری استفاده می‌کنید که از پورت خاصی استفاده می‌کند، 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 استثناء وارد نمایید.

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

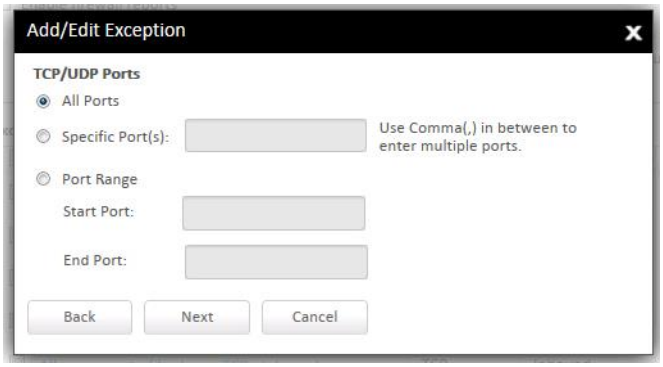
Select Direction: در این بخش جهت ترافیک را تعیین می‌کنید. جهت ترافیک می‌تواند ورودی (Inbound)، خروجی (Outbound) یا هر دو جهت باشد. سپس دکمه Next را کلیک کنید.

IP Address: در این بخش آدرس‌های IP که قانون فایروال باید بر روی آنها اعمال شود را مشخص می‌کنید.

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

IP Address: می‌توانید 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 برای اعمال قانون تعیین می‌کنید. 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.

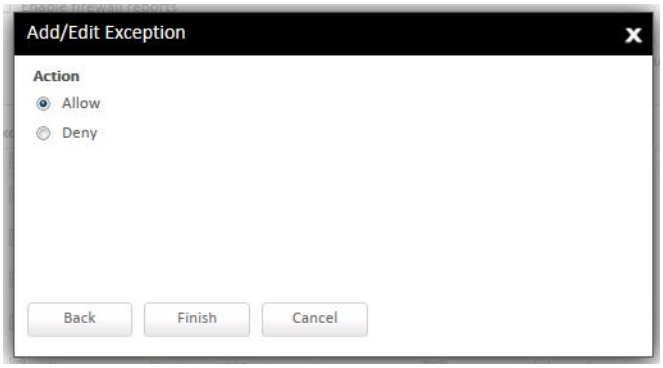


TCP/UDP Ports: در این بخش پورت‌هایی را که قانون فایروال باید بر روی آنها اعمال شود، مشخص نمایید.

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

Specific Port(s): می‌توانید 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. (مثلاً اگر می‌خواهید رول را بر روی پورت‌های ۸۰ و ٤٤٣ اعمال کنید می‌نویسید 80,443)

Port Range: اگر این گزینه تیک باشد، یک محدوده پورت را برای اعمال قانون تعیین می‌کنید. 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 می‌کنید که نوع اقدام چگونه باشد. Allow به معنای مجاز کردن رول و Deny به معنای غیرمجاز کردن رول می‌باشد. اگر می‌خواهید دسترسی به پورت و یا IP خاصی را باز کنید باید Allow را انتخاب کنید.

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 می‌توانید از رول هایی که قبلاً صادر شده در این کنسول استفاده نمایید.

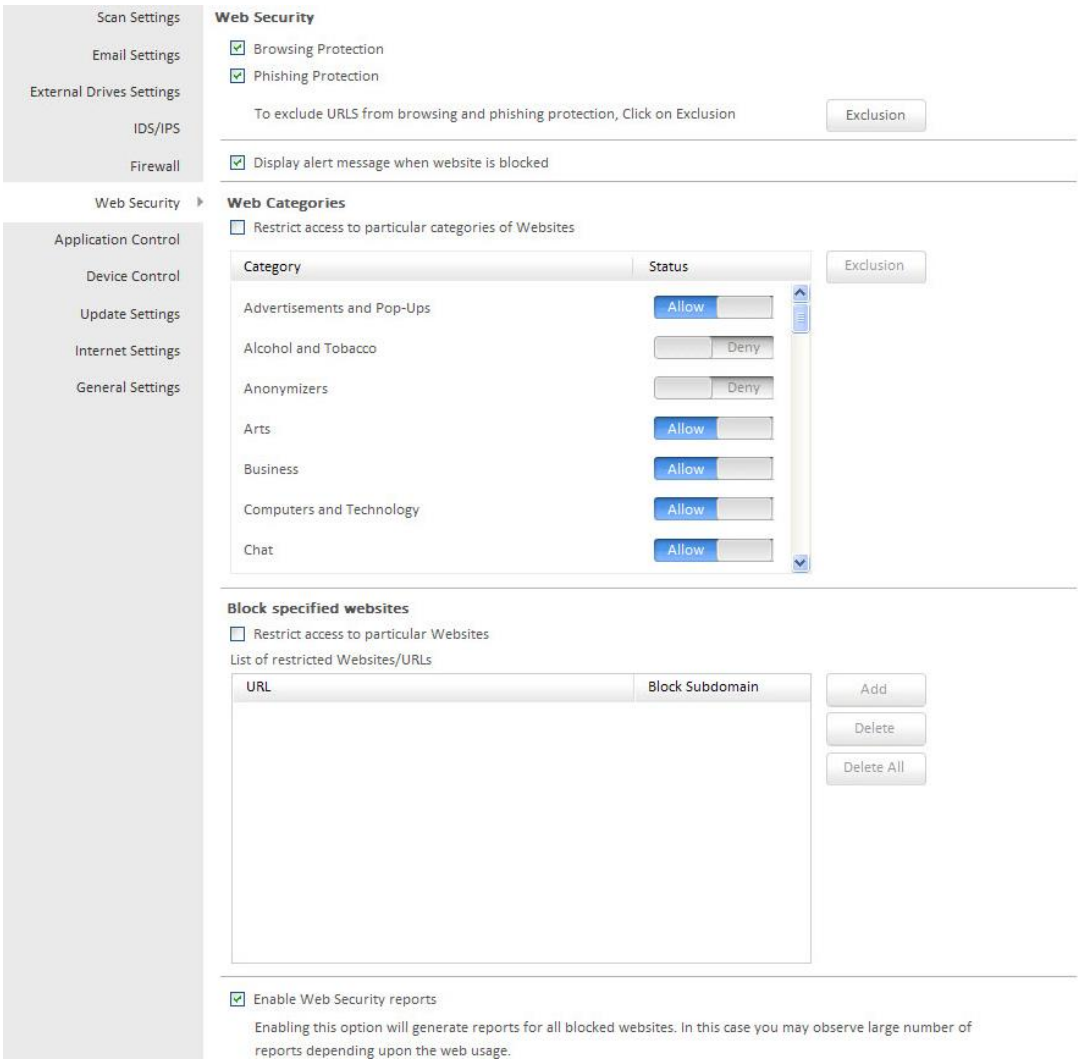
Export: با انتخاب یک یا چند رول و کلیک بر روی این گزینه می‌توانید یک پشتیبان از رول ها گرفته و آنها را بر روی کنسول های دیگر یا در زمان نصب مجدد استفاده کنید.

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

Move Down: با انتخاب رول دلخواه و کلیک بر روی این دکمه می‌توانید 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 می‌کند.

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

Exclusion: با کلیک بر روی این دکمه، می‌توانید 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. می‌توانید دسته خاصی از وب‌سایت ها (مثلاً 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 می‌توانید دسترسی به دسته بندی خاصی از وب‌سایت 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.

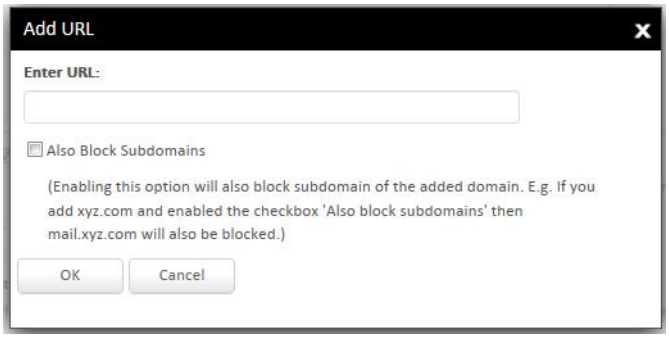
Exclusion: با کلیک بر روی این دکمه، می‌توانید سایت خاصی که عضو گروه بوده را از عمل پیش‌بینی شده برای آن گروه مستثنی کنید. مثلاً همه سایت های بازی، بجز یک سایت خاص بسته شود. پس از کلیک، پنجره ای باز می‌شود که می‌توانید نام سایت را در آن وارد و با تیک کردن Also Exclude Subdomains همه زیردامنه های آن سایت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

Block specified websites

در این بخش می‌توانید سایت های موردنظرتان را – خارج از اینکه عضو کدام دسته قرار دارند – مسدود نمایید.

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

با فشردن دکمه‌ی Add، پنجره‌ی زیر برای وارد کردن آدرس سایت موردنظر جهت مسدود شدن نمایش داده می‌شود:



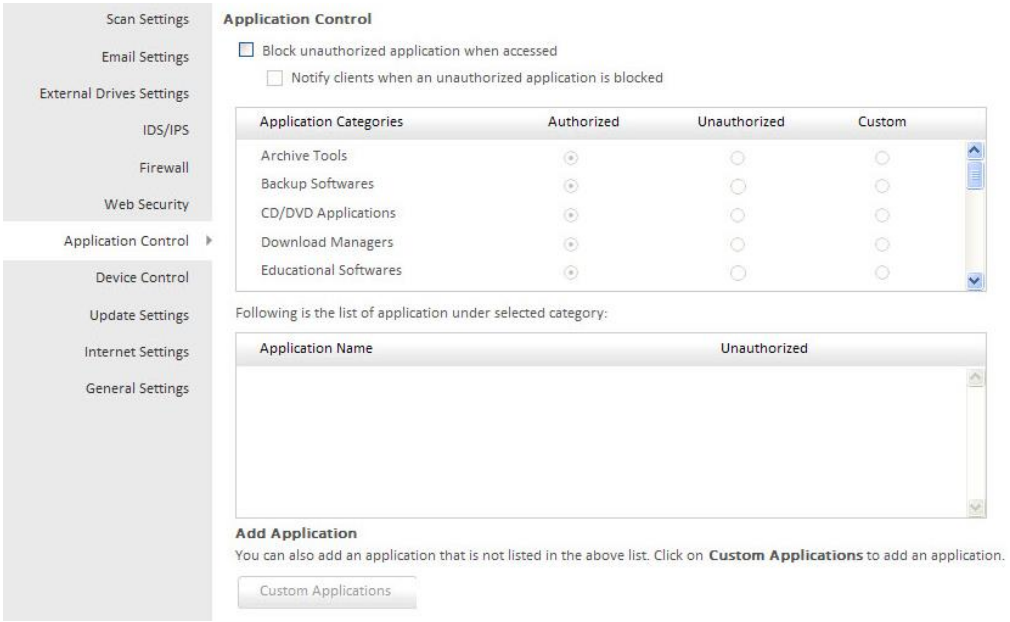
Enter URL: آدرس سایتی را که می‌خواهید از دسترس کاربران خارج شود، در این بخش وارد نمایید. (مثلاً yahoo.com)

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

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

Application Control

یکی از ویژگی‌های کوییک‌هیل اندپوینت‌سکیوریتی، کنترل برنامه‌ها (Application Control) می‌باشد. این ویژگی امکان مسدود کردن برنامه های کاربران را به صورت کامل فراهم می‌آورد. به عنوان مثال مدیر سیستم می‌تواند 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 می‌دهد، اما کوییک‌هیل ویژگی معرفی برنامه سفارشی (Custom Applications) را ارائه داده است که می‌توانید فایل exe. خود را به کوییک‌هیل معرفی نمایید تا آن را از دسترس خارج نماید.

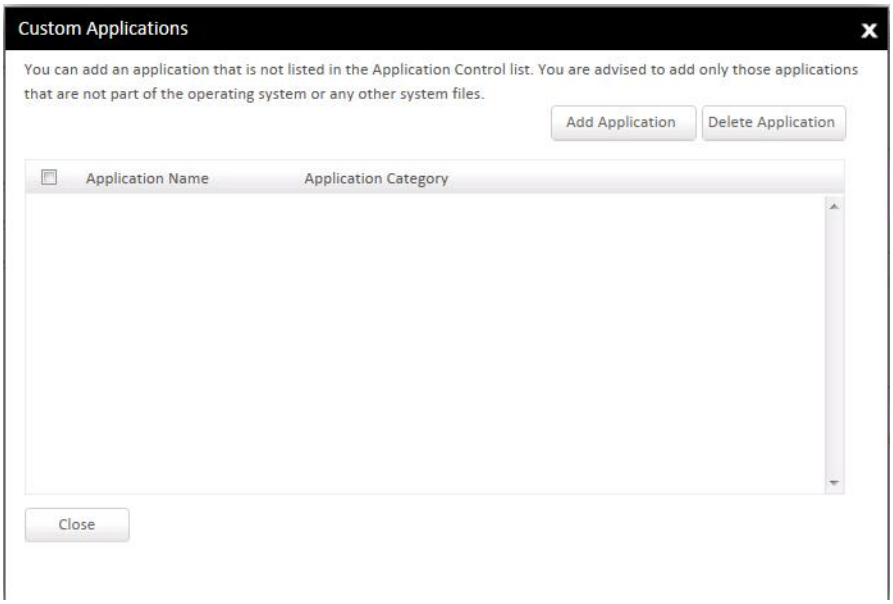


Block unauthorized application when accessed: برای فعال کردن قابلیت کنترل برنامه ها این گزینه باید تیک باشد. با فعال بودن این قابلیت، اجرای برنامه های غیرمجاز (unauthorized) برای کاربران ناممکن می‌گردد.

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 مسدود شدن برنامه توسط مدیریت به او نشان داده خواهد شد.

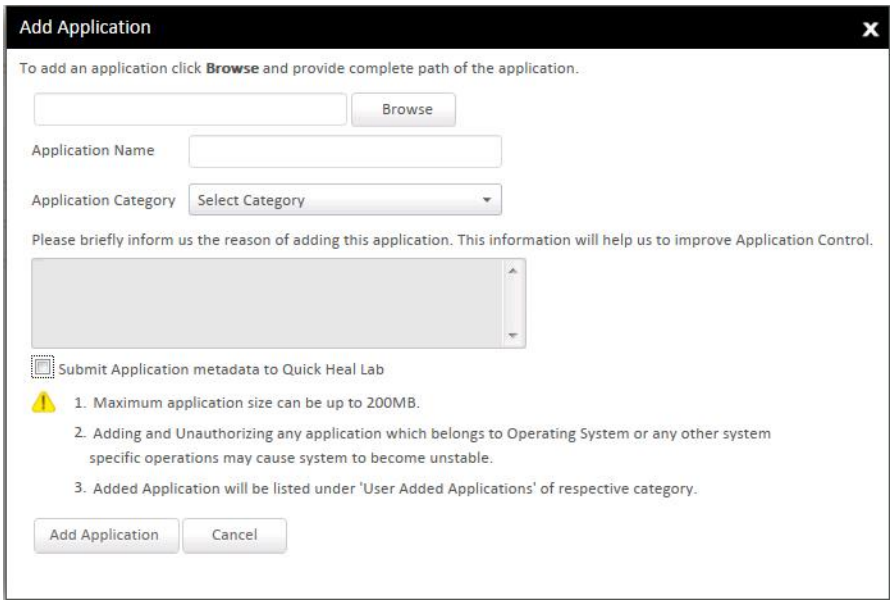
Application Categories: در این جدول دسته بندی برنامه های مختلف وجود دارد. با انتخاب گزینه Authorized، Unauthorized یا Custom در باکس بالایی می‌توانید کل نرم افزارهای آن گروه را مجاز، غیرمجاز و یا سفارشی نمایید. در صورتی که مایلید یک یا چند برنامه عضو آن گروه را غیرمجاز کنید باید گزینه Custom آن گروه 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 (مثلاً کرک شدن) با فایل اجرایی استاندارد تفاوت دارد، می‌توانید 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 می‌توانید از لیست پیش فرض انتخاب کنید تا این برنامه در آن گروه قرار گرفته و امکان کنترل آن فراهم گردد. می‌توانید 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 می‌توانید فایل را به لابراتوار کوییک‌هیل ارسال نمایید. در فرم بالای این گزینه، علت افزودن برنامه را به کوییک‌هیل توضیح می‌دهید. (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، می‌توانید گروهی را که برنامه به آن اضافه شده (مثلاً Others)، غیرمجاز نمایید. همچنین می‌توانید آن گروه را در حالت Custom قرار داده و در باکس دومی فقط برنامه موردنظرتان را غیرمجاز کنید.

Device Control

در این بخش می‌توانید بیش از ۲۵ نوع مختلف از ابزارها و دستگاه های جانبی را مدیریت نمایید. انواع مختلف ابزار شامل ابزارهای ذخیره‌سازی (Storage Devices)، وایرلس (Wireless)، اینترفیس‌ها و واسطه‌ها (Interface)، کارت‌خوان‌ها (Card Readers)، گوشی‌های موبایل (Mobile & Portable Devices)، دوربین‌ها (Camera) به صورت کامل بر روی کلاینت‌های شبکه قابل مدیریت می‌باشند.

مدیر شبکه می‌تواند ابزارهای اصلی و جانبی همه و یا گروهی از کلاینت‌ها را کنترل کند، مثلاً گروهی از کلاینت‌ها امکان خواندن و نوشتن (Allow) بر روی فلش‌ها و حافظه‌های USB را داشته باشند اما گروهی نتوانند از فلش‌ها استفاده نمایند (Block) و گروهی هم فقط بتوانند اطلاعات فلش‌ها را بخوانند (Read Only) و اطلاعات سازمان به خارج نشت پیدا نکند.

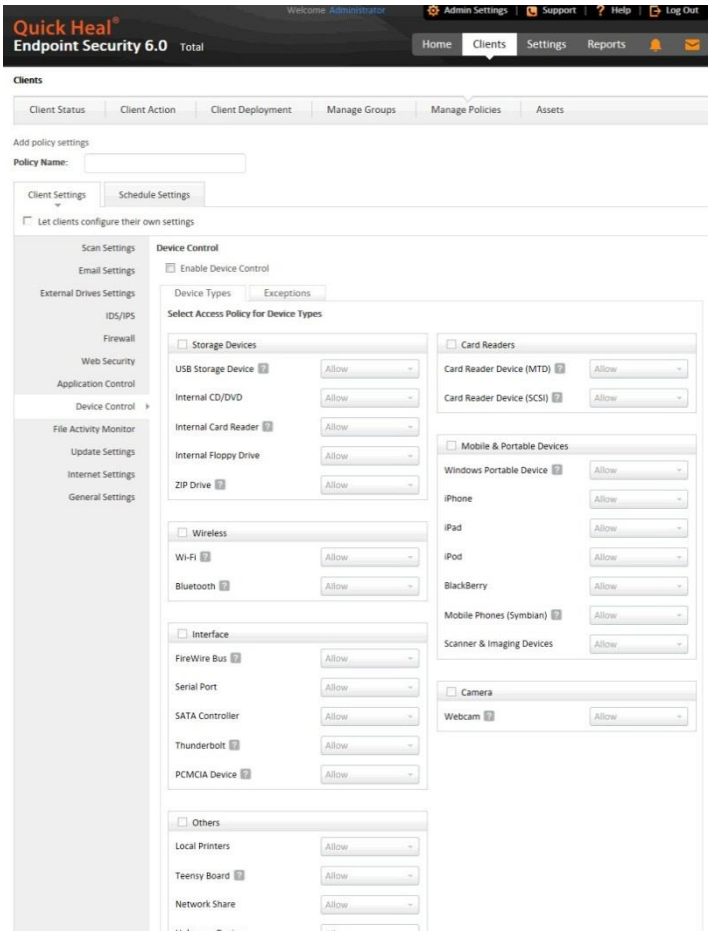
چهار دلیل عمده برای استفاده از این ویژگی عبارتند از:

الف) سیاست‌های امنیتی بر روی اطلاعات و منابع سازمان اعمال گردد.

ب) کلاینت‌ها بدون آلودگی بوده و بدافزاری از ابزارها بر روی سیستم منتقل نگردد.

ج) ویژگی Autorun موجب انتقال آلودگی نشود.

د) برنامه‌ها و داده‌های غیرضروری موجب کند شدن سیستم نگردد.

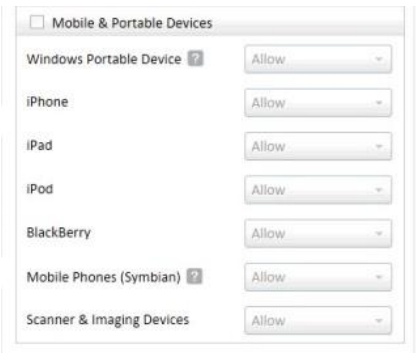


الف) Storage Device: در این بخش می‌توانید انواع حافظه‌های USB (مانند فلش ها، هاردهای اکسترنال و...)، CD/DVD-Romهای داخلی (Internal CD/DVD)، کارت‌خوان‌های حافظه داخلی (Internal Card Reader)، داریوهای فلاپی داخلی (Internal Floppy Drive) و درایوهای ZIP را مدیریت نمایید.

ب) Wireless: در این بخش می‌توانید سیاست‌گذاری‌های امنیتی خود را بر روی ارتباطات بی‌سیم کلاینت‌های شبکه سازمانی خود اعمال نمایید. شبکه وایرلس(Wi-Fi) و بلوتوث(Bluetooth) همه‌ی کلاینت‌ها یا گروهی از آنها در این بخش قابل مدیریت و کنترل می‌باشند. اگر می‌خواهید در صورت در دسترس بودن شبکه کابلی، وایرلس کلاینت را غیرفعال نمایید، گزینه Blocked if wired connection is available را در بخش Wi-Fi انتخاب نمایید. امکان مسدود کردن کامل (Block)، و یا مجاز کردن (Allow) نیز وجود دارد.

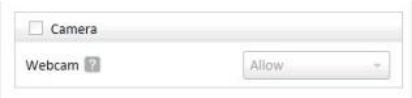
ب) Interface: در این بخش انواع اینترفیس‌های کامپیوترها قابل مدیریت می‌باشد. اینترفیس‌ها شامل FireWire Bus، Serial Port، SATA Controller، Thunderbolt و PCMCIA Device می‌باشند.

ج) Card Readers: در این بخش کارت‌خوان‌های حافظه‌ای (Card Reader Device (MTD)) و کارت‌خوان‌های SCSI (Card Reader Device (SCSI)) بر روی کلاینت‌ها قابل مدیریت می‌باشد.



د) Mobile & Portable Devices: این قسمت ارتباطات گوشی‌های موبایل به کلاینت‌های شبکه قابل مدیریت می‌باشند. انواع گوشی‌های هوشمند موبایل مبتنی بر ویندوز و اندروید که از پروتکل Media Transfer Protocol برای اتصال به ویندوز استفاده می‌کنند (Windows Portable Device)، انواع محصولات اپل

مانند iPod،iPad،iPhone، بلک‌بری (BlackBerry)، گوشی‌های نوکیا مبتنی بر سیمبین (Mobile Phones (Symbian) و اسکنرها و ابزارهای عکاسی (Scanner & Imaging Devices) قابل مدیریت می‌باشند.



هـ) Camera: انواع دوربین‌های وب کم داخلی و خارجی در این بخش قابل مسدود کردن و یا مجاز کردن می‌باشند.

و) Others: دستگاه های جانبی دیگر مانند چاپگرهای محلی (Local Printers)، سیستم‌های میکروکنترلر مبتنی بر USB (Teensy Board)، اشتراک‌گذاری شبکه (Network Share) و حتی دستگاه های ناشناخته (Unknown Device) در این بخش قابل مدیریت می‌باشند.

گزینه های قابل انتخاب برای هریک از ابزارها عبارتند از:

Allow: با انتخاب این گزینه، استفاده از ابزار مجاز می‌گردد.

Block: این گزینه سبب می‌شود تا ابزار موردنظر غیرمجاز و برای کاربران عضو گروه مسدود گردد.

Read only: در صورت انتخاب این گزینه، تنها امکان خواندن از ابزار ممکن بوده ولی نمی‌توان اطلاعاتی از روی کلاینت وارد دستگاه های جانبی نمود (جلوگیری از سرقت اطلاعات).

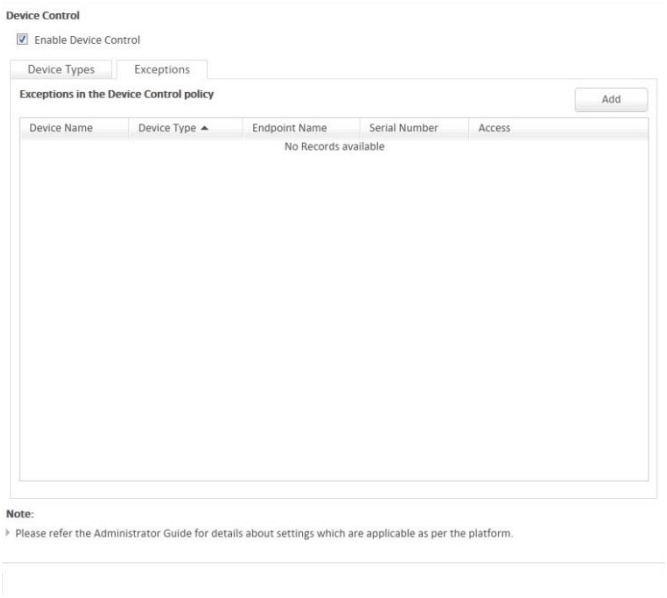
Block if wired connection is available: این گزینه قابل استفاده برای ابزارهای وایرلس می‌باشد. در صورتی که اتصال کابلی به شبکه فراهم باشد، وایرلس WiFi کاربران مسدود خواهد شد.

مستثنی کردن ابزار

مدیر امنیت شبکه می‌تواند با مسدود کردن ابزار، همه‌ی کاربران عضو گروه موردنظر را از اجرا نشدن ابزار منع نماید. اما این قابلیت در EPS 6.0 در نظر گرفته شده است تا بتوان یک یا چند ابزار را از سیاست موردنظر مستثنی نمود. به عنوان مثال مدیر می‌تواند همه دیسک‌های فلش‌ها را مسدود کرده، اما حافظه فلش خود را برای کار کردن در سیستم مجاز نماید.

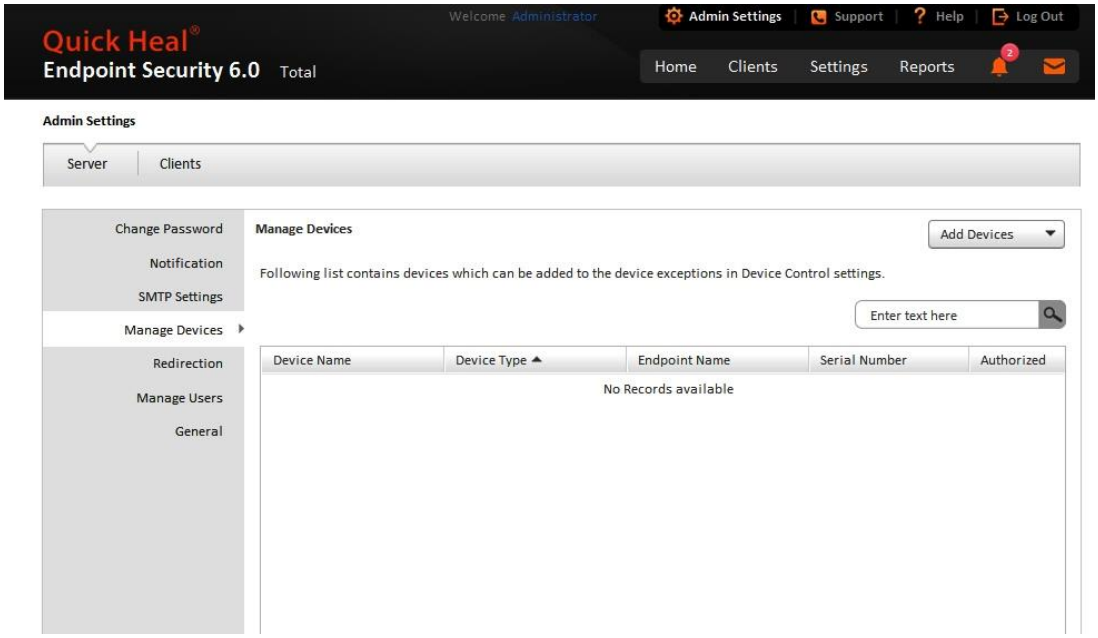
برای انتخاب دستگاه جانبی موردنظر، ابتدا می‌بایست آن ابزار را به سیستم متصل نموده و در بخش Admin Settings -> Server -> Manage Devices ابزار را به لیست اندپوینت معرفی نمایید. (در ادامه توضیح داده می‌شود)

سپس از سربرگ دوم (Exceptions) از لیست دستگاه های معرفی شده، دستگاه جانبی خود را Add و سطح دسترسی موردنظر (Allow) را برای آن تعیین نمایید.

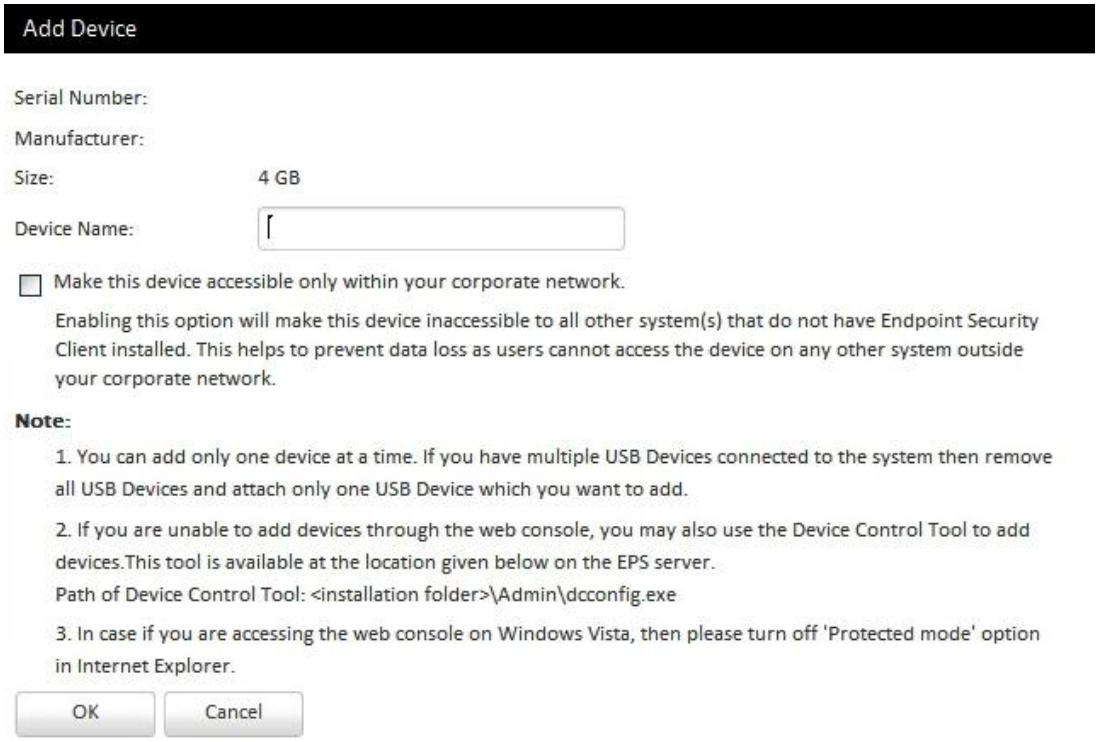


معرفی حافظه USB فلش به لیست Device Control

در این بخش می‌توانید 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 می‌توانید ابزار USB خود را به اندپوینت‌سکیوریتی معرفی کنید.

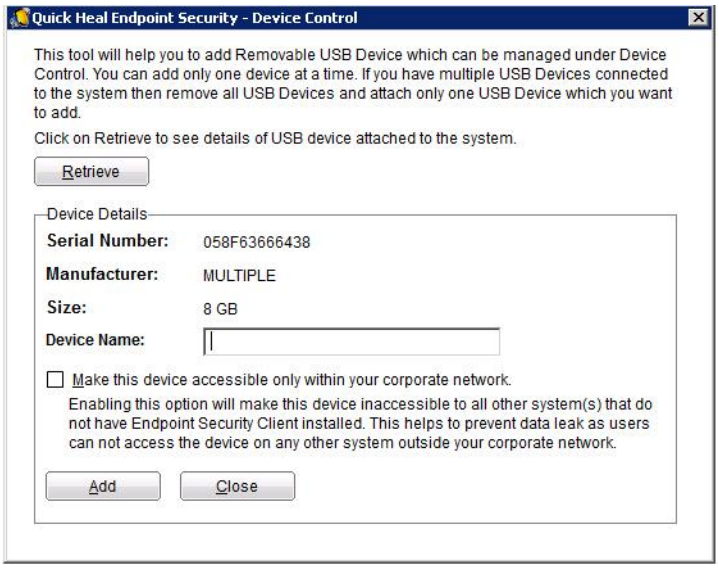


Make this device accessible only within your corporate network:

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:

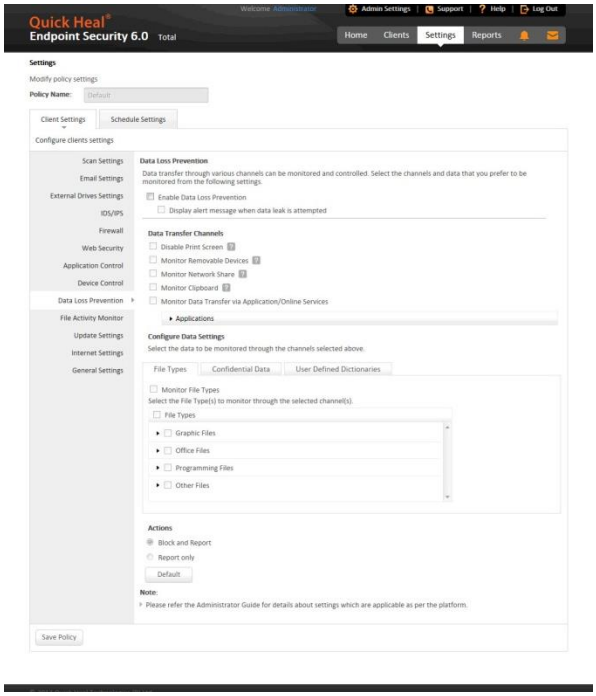
\Quick Heal Installing Path\Admin\dcconfig.exe

مانند:

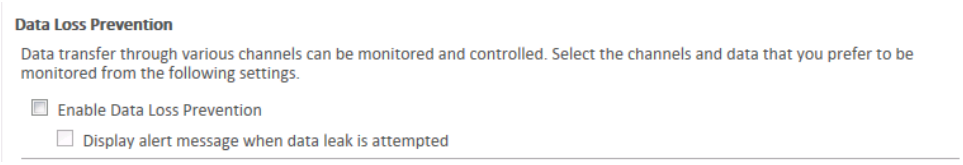
C:\Program Files (x86)\Quick Heal\Endpoint Security 6.0\Admin\dcconfig.exe

Data Loss Prevention

بسته DLP نسل آتی امنیت سازمانی محسوب می‌شود که برای جلوگیری از نشت اطلاعات حساس سازمانی مورد استفاده قرار می‌گیرد. این پکیج همه کانال‌های نشت اطلاعات محرمانه به خارج از سازمان را کنترل و مدیریت می‌نماید.



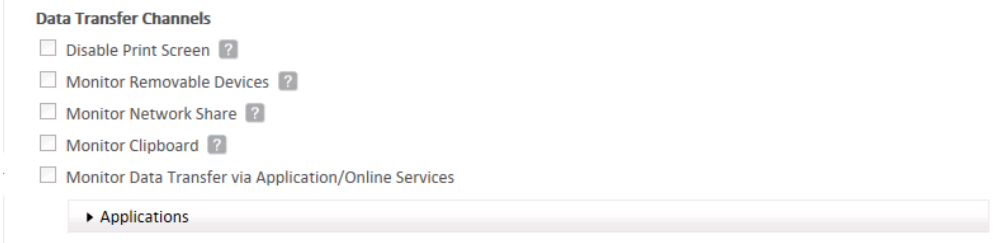
الف) Data Loss Prevention: در این بخش می‌توانید پکیج DLP را فعال یا غیر فعال نمایید:



Enable Data Loss Prevention: برای فعال شدن بسته DLP این گزینه باید تیک شود.

Display alert message when data leak is attempted: در صورت تلاش برای نشت اطلاعات، پیغام مناسب نمایش داده شود.

ب) Data Transfer Channels: در این بخش کانال‌های نقل و انتقال اطلاعات قابل پیکربندی می‌باشند:



Disable Print Screen: با غیرفعال کردن ویژگی Print Screen امکان تصویربرداری از صفحه نمایش در محیط ویندوز مسدود خواهد شد.

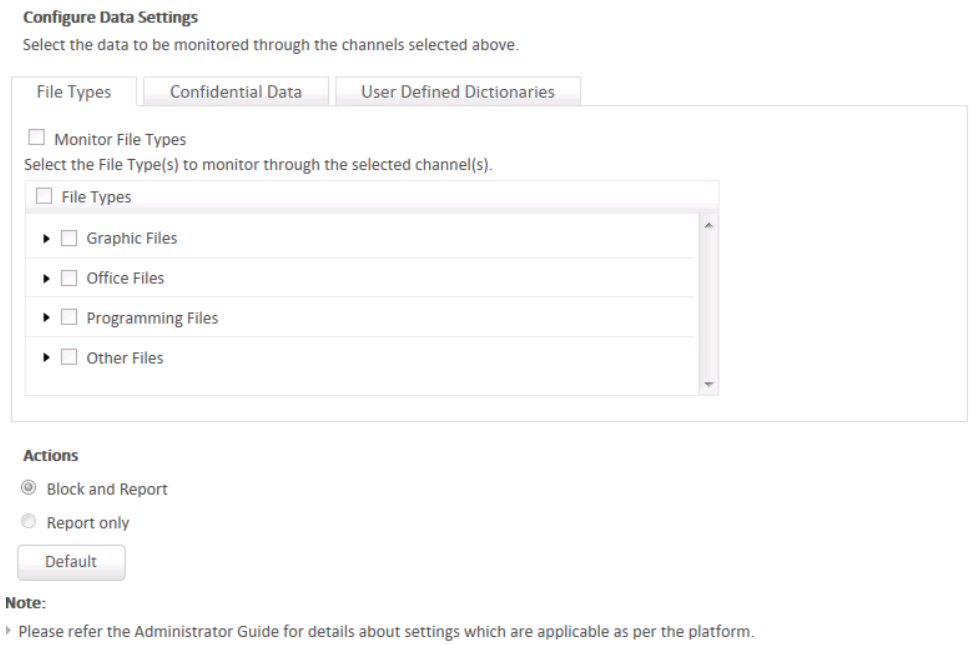
Monitor Removable Devices: ابزارهای جانبی جداشدنی (مانند فلش‌های USB) مانیتور و کنترل می‌شوند.

Monitor Network Share: هرگونه نقل و انتقال اطلاعات در بستر شبکه داخلی که از طریق اشتراک‌گذاری انجام می‌پذیرد مانیتور می‌شوند.

Monitor Clipboard: هرگونه Copy و Paste اطلاعات محرمانه سازمان (شامل اطلاعات محرمانه و اطلاعاتی که توسط کاربر به عنوان اطلاعات محرمانه تعریف شده) در حافظه موقت (کلیپبورد) مانیتور می‌شود.

Monitor Data Transfer via Application/Online Services: هرگونه نقل و انتقال اطلاعات سازمان از بستر نرم‌افزارها و خدمات آنلاین مبتنی بر فناوری ابری مانیتور و کنترل می‌شوند. این نرم‌افزارها و خدمات آنلاین شامل انواع مرورگرها (مانند Chrome)، برنامه‌های مدیریت ایمیل (مانند Outlook)، نرم‌افزارهای چت و پیام‌رسان (مانند Yahoo Messenger)، خدمات مبتنی بر فناوری ابری و اشتراک‌گذاری آنلاین فایل (مانند Google Drive Client)، شبکه‌های اجتماعی و غیره (مانند GoToMeeting) می‌باشند.

ج) *Configure Data Settings*: داده‌های محرمانه‌ای که می‌توانند توسط DLP مانیتور گردند در این بخش تعریف و پیکربندی می‌گردند:



Monitor File Types: در این قسمت می‌توانید انواع مختلف فایل و زیرمجموعه‌ی آنها را برای کنترل انتخاب کنید. انواع فایل‌های گرافیکی (مانند jpg)، فایل‌های اسناد اداری (مانند word)، فایل‌های برنامه‌نویسی (مانند c) و غیره (مانند zip) قابل انتخاب و مانیتور می‌باشند.

Confidential Data: یک سری فایل‌های محرمانه در این بخش به صورت پیش‌فرض تهیه شده است. این اطلاعات شامل اطلاعات کارت‌های بانکی (Credit/Debit Cards) و اطلاعات شخصی (Personal) می‌باشد که قابل انتخاب می‌باشند.

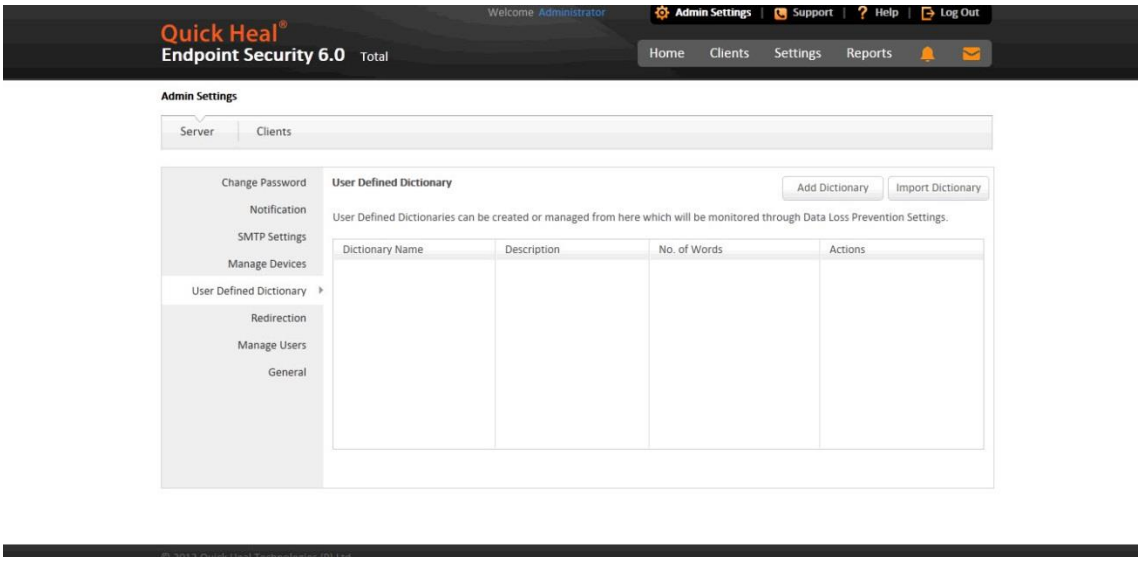
User Defined Dictionaries: مدیر شبکه می‌تواند از اطلاعات حساس و محرمانه سازمان خود یک دیکشنری تعریف نموده و کلمات حساس را وارد آن نماید تا مورد بازرسی قرار گیرند. برای تعریف دیکشنری از منوی Admin Settings -> Server -> User Defined Dictionary می‌توانید استفاده کنید. بعد از تعریف دیکشنری‌ها، در این بخش می‌توانید از هر کدام از دیکشنری‌ها استفاده نمایید.

- **Match whole world:** اگر این گزینه تیک باشد، در صورتی که کلمه‌ی تعریف‌شده در دیکشنری دقیقاً برابر با این کلمه باشد تحت رهگیری قرار می‌گیرد. اما اگر این گزینه انتخاب نشود، اگر کلمه در ابتدا، وسط یا انتهای یک کلمه یا عبارت باشد، نیز رهگیری می‌گردد.
- **Match Case:** در صورتی که این گزینه تیک باشد، بزرگ و کوچک بودن حروف انگلیسی در پیمایش مدنظر قرار خواهد گرفت.

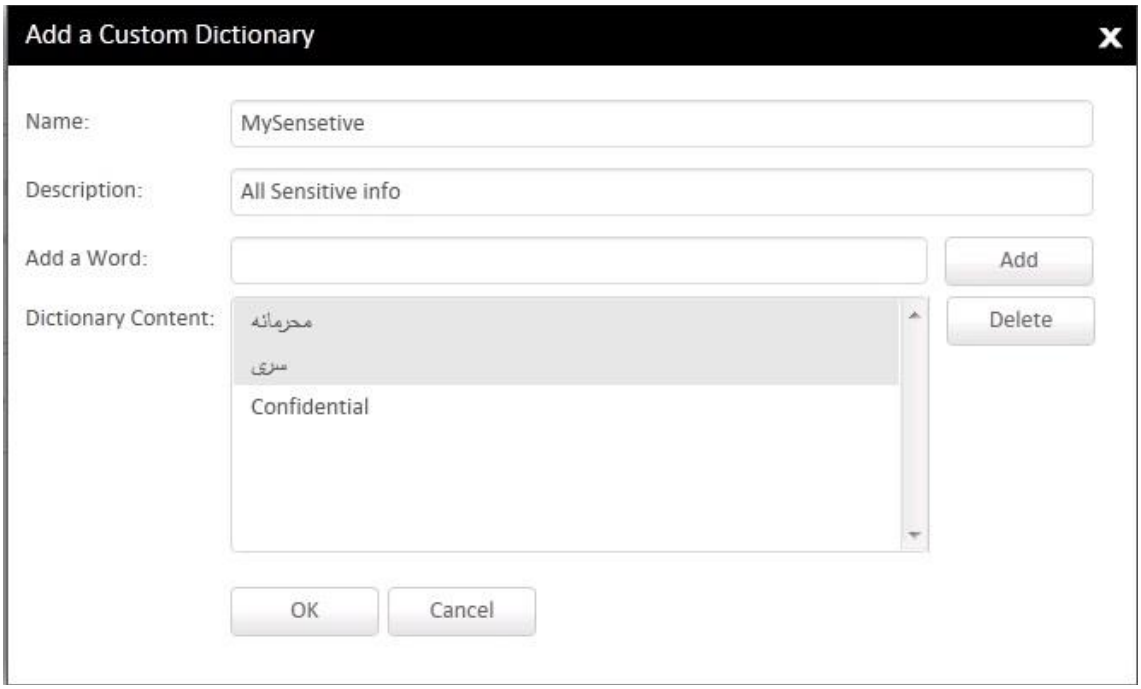
Actions: در این بخش می‌توانید اقدامی که بر روی کلمات محرمانه صورت می‌پذیرد را تعیین نمایید. به عنوان مثال می‌توانید تعیین کنید، در صورتی که یک کلمه از دیکشنری از کانال‌های تعیین شده در حال عبور بود، عبور آن را مسدود و گزارش ارسال نماید (Block and Report) و یا تنها گزارش انتقال اطلاعات را ارسال نماید (Report only).

تعریف دیکشنری جدید

در این بخش می‌توانید دیکشنری‌های مربوط به بخش DLP را مدیریت کنید. این بخش از طریق منوی بالای صفحه Admin Settings قابل دسترس است.



Add Dictionary: با کلیک بر روی این دکمه می‌توانید یک دیکشنری جدید به اندپوینت‌سکیوریتی اضافه کنید.



- **Name:** در این فیلد نام دیکشنری جدید را وارد می‌کنید.
- **Description:** توضیحات به دلخواه در رابطه با دیکشنری در این بخش وارد می‌شود.

- Add a Word: در این فیلد، کلمات حساسی که مایلید بر روی آنها مانیتور صورت پذیرد را وارد می‌کنید. در هر بار یک کلمه را وارد و بر روی Add کلیک می‌کنید.
- Dictionary Content: لیست کلمات دیکشنری که قرار است DLP بر روی آنها کار کند در این بخش نشان داده می‌شود.

نکته: شما می‌توانید چندین دیکشنری تعریف نمایید و برای هر پالیسی یک یا چند دیکشنری را به دلخواه فعال نمایید.

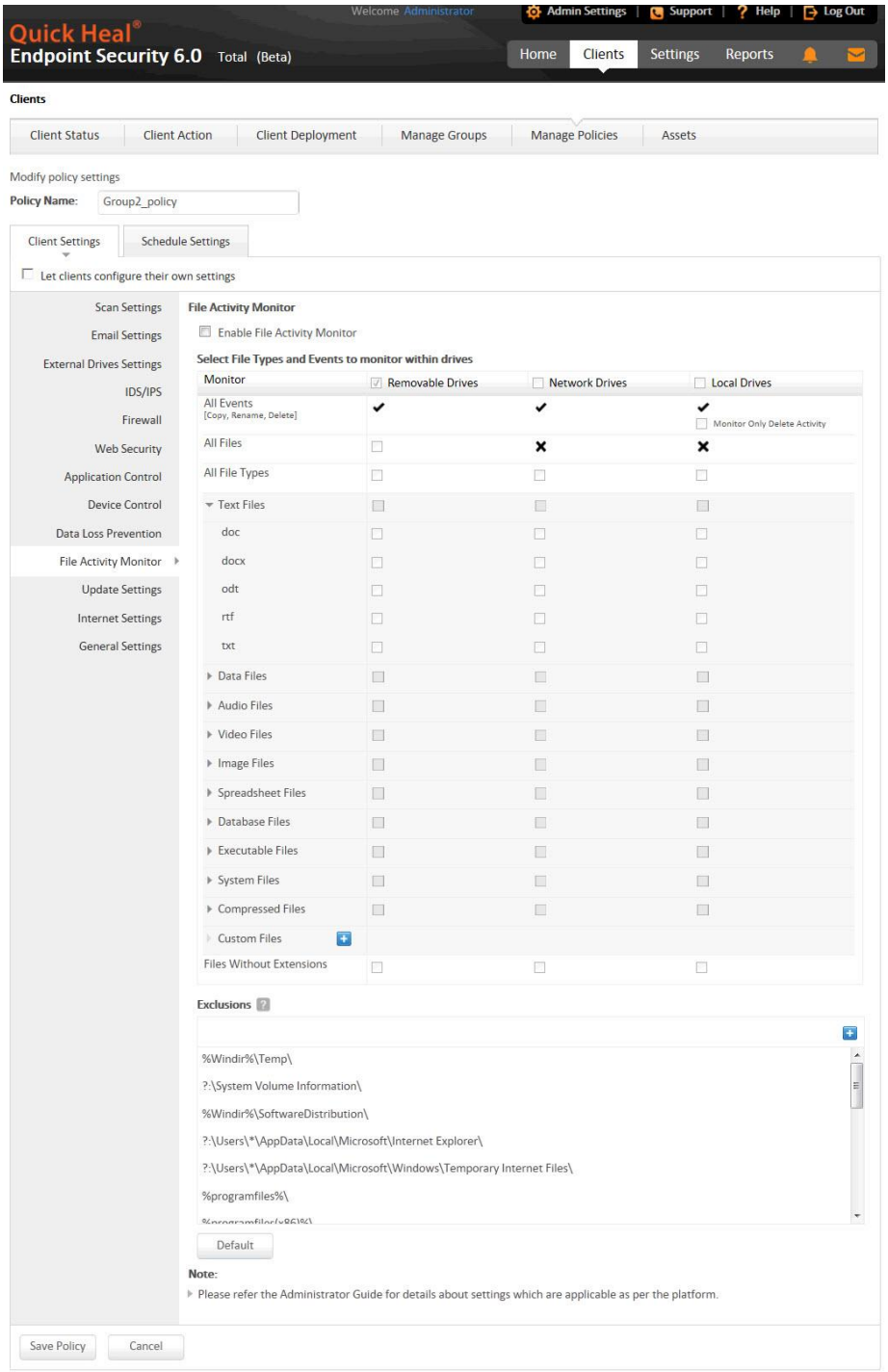
File Activity Monitor

مانیتورینگ فعالیت فایل (FAM) یکی از ویژگی‌های مدیریتی امنیت اطلاعات می‌باشد. با استفاده از این ماژول می‌توانید هرگونه فعالیت فایل‌ها را رصد نمایید.

Enable File Activity Monitor: با تیک کردن این گزینه ماژول FAM فعال می‌شود.

Select File Types and Events to monitor within drives: در این بخش نوع فایل، فعالیت مورد نظر و مسیری که FAM بر روی آنها اعمال می‌شود قابل تعیین می‌باشد:

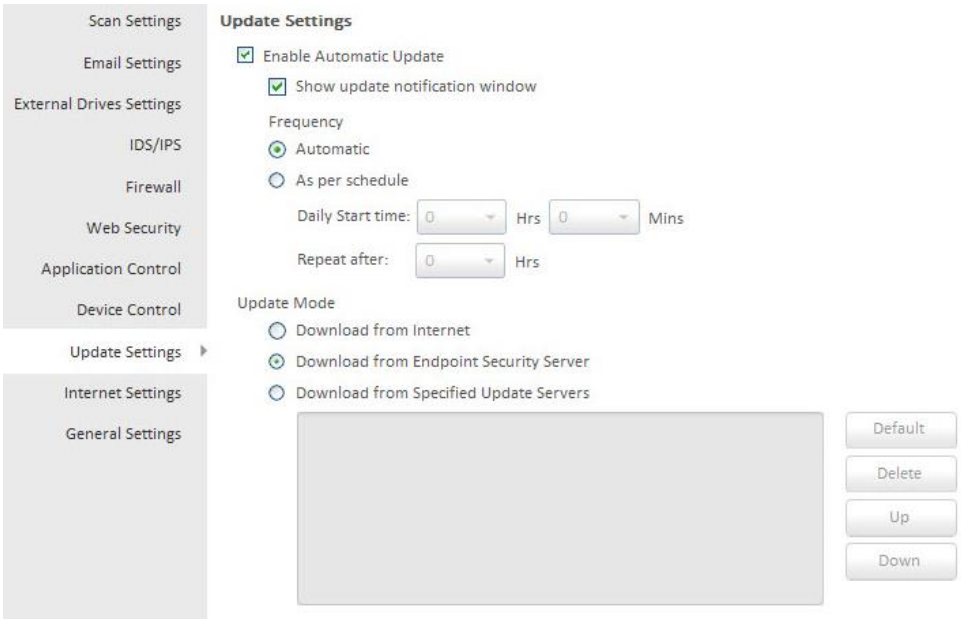
فعالیت بر روی فایل‌ها شامل کپی (Copy)، تغییر نام (Rename) و حذف (Delete) می‌باشد. انواع مختلف فایل مانند فایل‌های متنی، صوتی، تصویری، اجرایی، سیستمی و... قابل انتخاب جهت مانیتور می‌باشند. همچنین امکان تعریف نوع‌های جدید فایل (Custom Files) و نیز فایل‌های بدون پسوند، نیز در نظر گرفته شده است. فایل‌ها بر روی درایوهای جداشدنی (USB)، داریوهای شبکه و درایوهای محلی (مانند C:\) قابل رصد می‌باشند.



Exclusions: در این بخش می‌توانید مسیرها، فولدرها و فایل‌هایی را که می‌خواهید مانیتور بر روی آنها انجام نپذیرد تعیین نمایید. تعدادی از مسیرها (مانند ویندوز) از ردیابی مستثنی شده اند.

Update Settings

تنظیمات بروزرسانی کلاینت‌ها در این بخش قابل پیکربندی می‌باشد. امکان بروزرسانی خودکار، زمانبندی و مسیر سرور بروزرسانی در این بخش تعیین می‌گردند. 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 کلاینت‌ها را می‌توانید در این بخش تعیین نمایید.

Automatic: بازه زمانی بروزرسانی کلاینت‌ها به صورت خودکار تعیین می‌گردد.

As per schedule: اگر این گزینه فعال باشد، بروزرسانی کلاینت‌ها را می‌توانید زمانبندی و برنامه‌ریزی نمایید.

Daily Start time: ساعت آغاز بروزرسانی را می‌توانید تعیین نمایید.

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

Update Mode: در این قسمت حالت آپدیت تعیین می‌گردد.

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

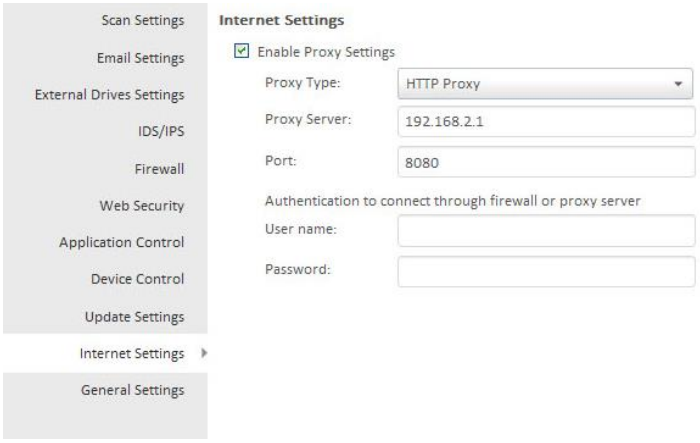
Download from Endpoint Security Server: اگر این گزینه انتخاب باشد، کلاینت‌ها از سرور اندپوینت بروزرسانی خود را دریافت می‌کنند.

Download from Specified Update Servers: اگر یک آپدیت سرور مجزا برای بروزرسانی درنظر گرفته اید (مثلاً در دفتر دیگر) می‌توانید مشخص کنید که این کلاینت‌ها از آن سرور بروزرسانی آپدیت شوند.

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

Internet Settings

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



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

Proxy Type: نوع پراکسی را در این قسمت مشخص می‌کنید. پراکسی می‌تواند HTTP Proxy، SOCKS V4 یا SOCKS V5 باشد.

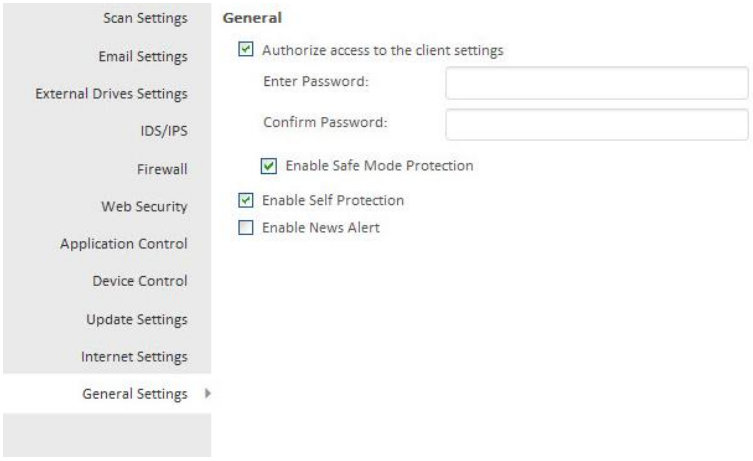
Proxy Server: آدرس IP پراکسی سرور را در این بخش وارد کنید.

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 کلاینت‌ها 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 موردنظر برای کلاینت کوییک‌هیل را وارد نمایید.

Confirm Password: مجدداً 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 می‌دهد.

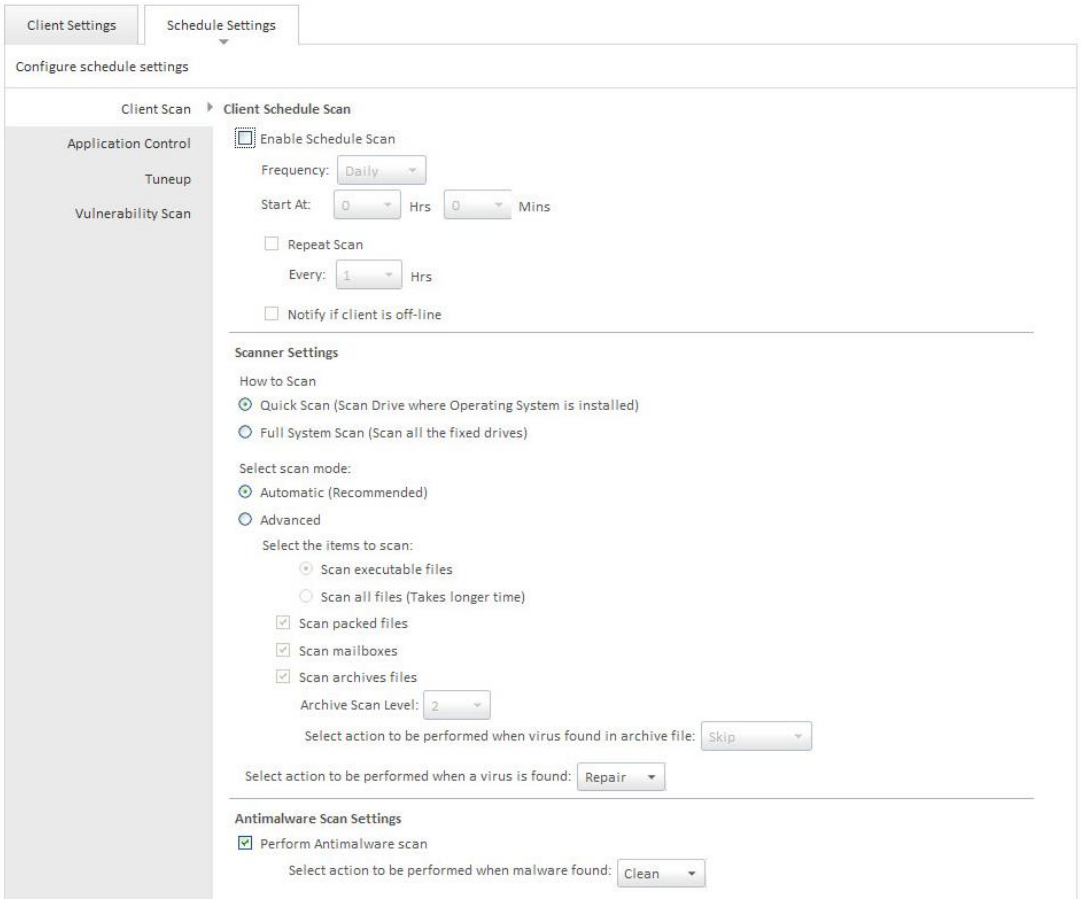
Enable Self Protection: در صورتی که این گزینه فعال باشد، کوییک‌هیل از خود در برابر هرگونه تغییر ناخواسته توسط ویروس محافظت می‌کند.

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 می‌توانید اسکن کلاینت‌ها، 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 می‌توانید 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 می‌توانید در این بخش تعیین کنید. دوره های اسکن می‌تواند به صورت روزانه یا هفتگی باشد.

در صورتی که فرکانس اسکن به صورت Daily باشد، زمان آغاز (Start At) و تکرار اسکن (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:

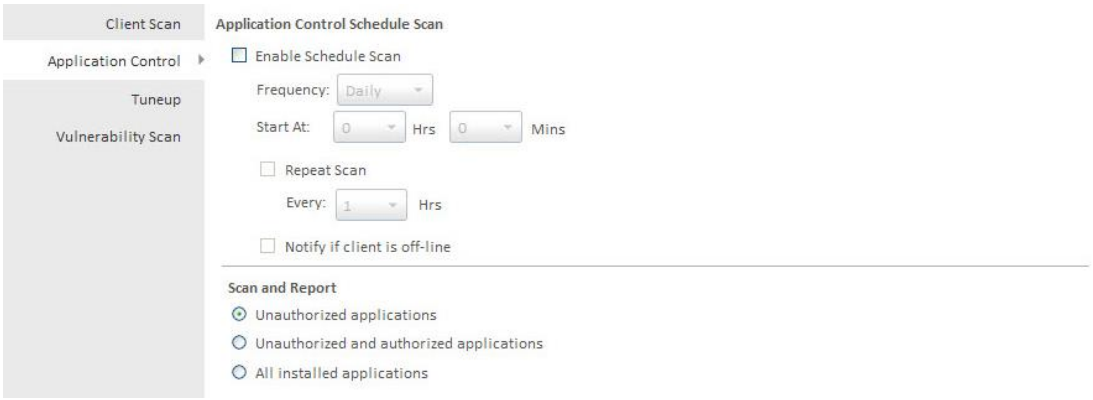
در این بخش تنظیمات اسکن ضد بدافزار تعیین می‌گردد.

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 می‌یابد، تعیین می‌گردد، این عمل می‌تواند Clean (پاکسازی) یا صرف نظر (Skip) باشد.

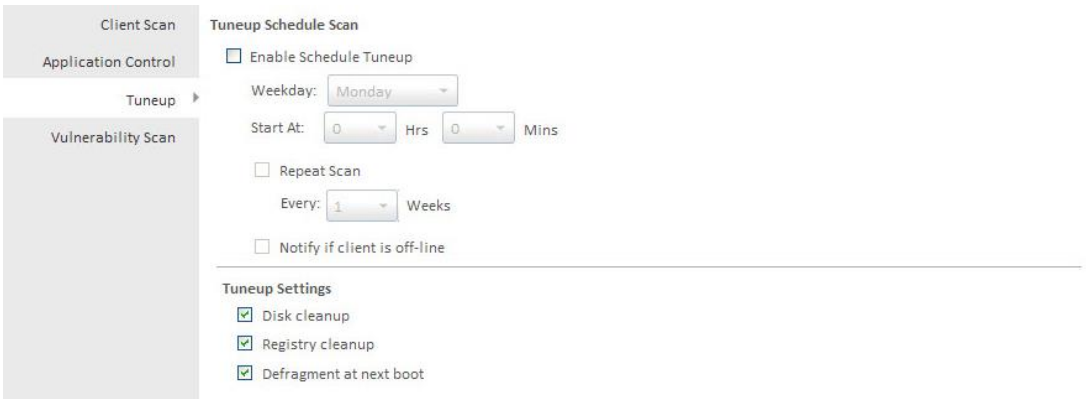
Application Control Schedule Scan

در این بخش می‌توانید اسکن برنامه ها را زمانبندی نمایید تا در زمان مشخص شروع به اسکن برنامه‌های غیرمجاز (Unauthorized applications)، برنامه های مجاز و غیرمجاز (Unauthorized and authorized applications)، همه‌ی 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

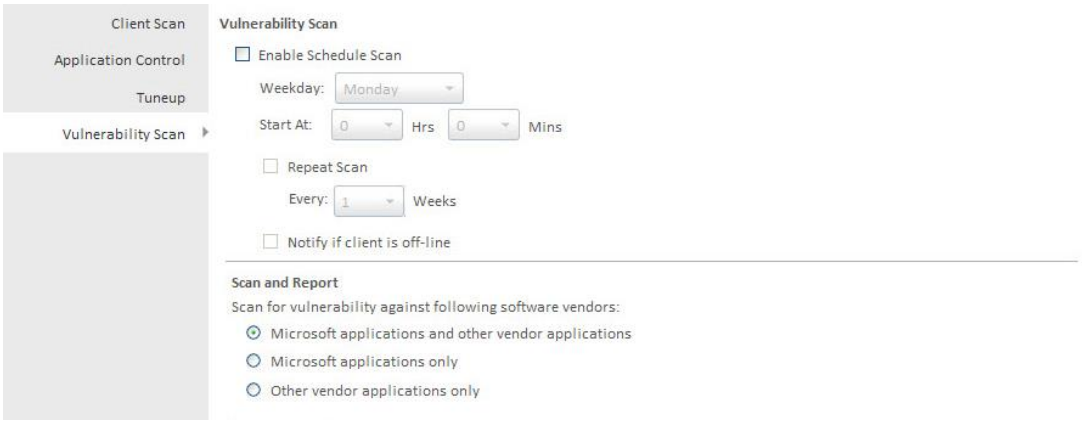
Disk cleanup: پاکسازی دیسک انجام می‌گیرد.

Registry cleanup: پاکسازی رجیستری صورت می‌پذیرد.

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

Vulnerability Scan

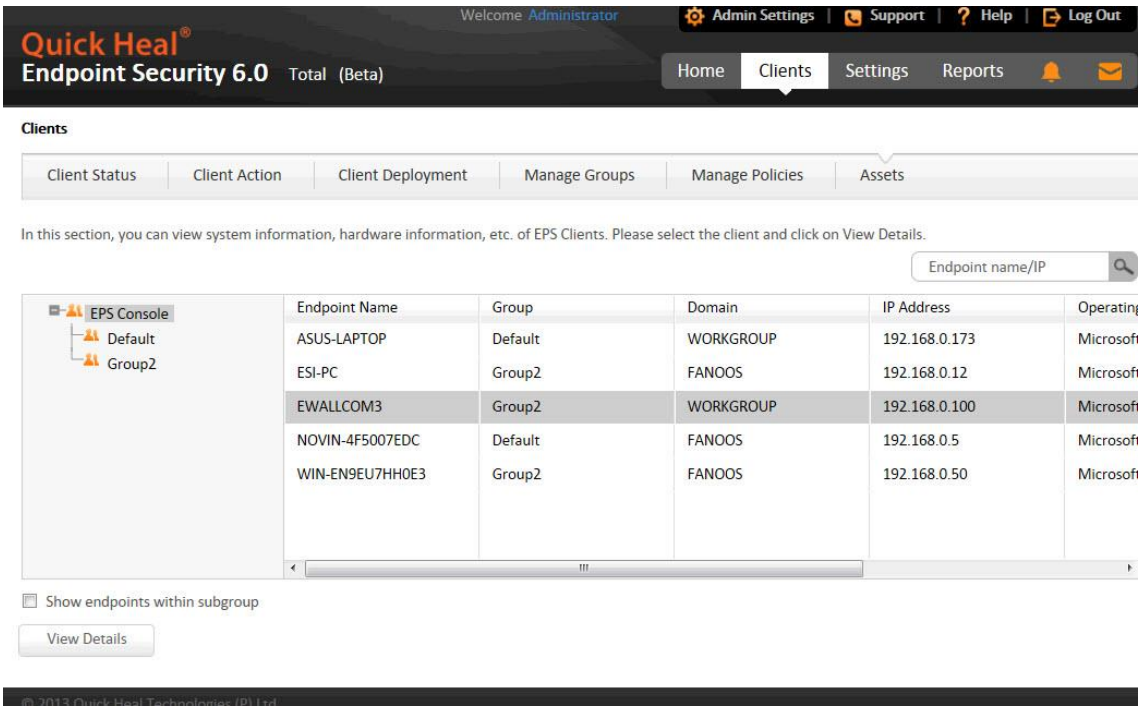
اسکن آسیب پذیری در این بخش قابل برنامه ریزی و زمانبندی است. در قسمت ابتدایی زمانبندی مشخص می‌گردد.



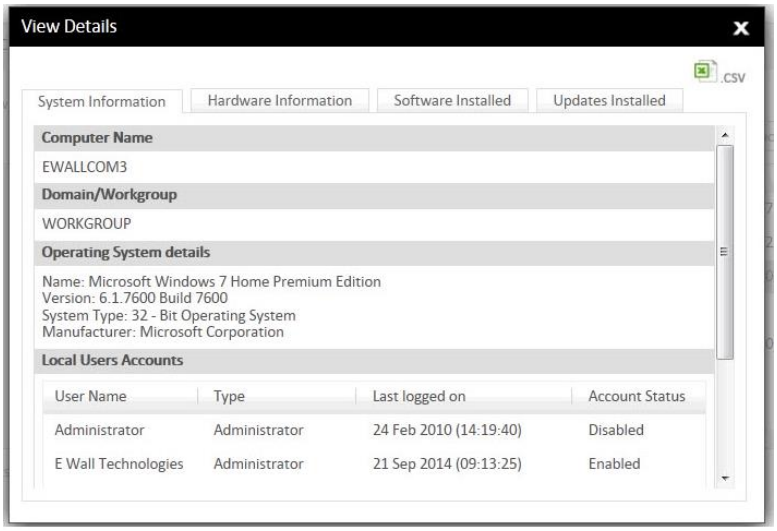
در بخش دوم می‌توانید تعیین کنید که برنامه های مایکروسافت و شرکت‌های دیگر(Microsoft applications and other vendor applications)، فقط برنامه های مایکروسافت (Microsoft applications only) و یا فقط برنامه های شرکت‌های دیگر (Other vendor applications only) اسکن آسیب پذیری گردد.

Assets

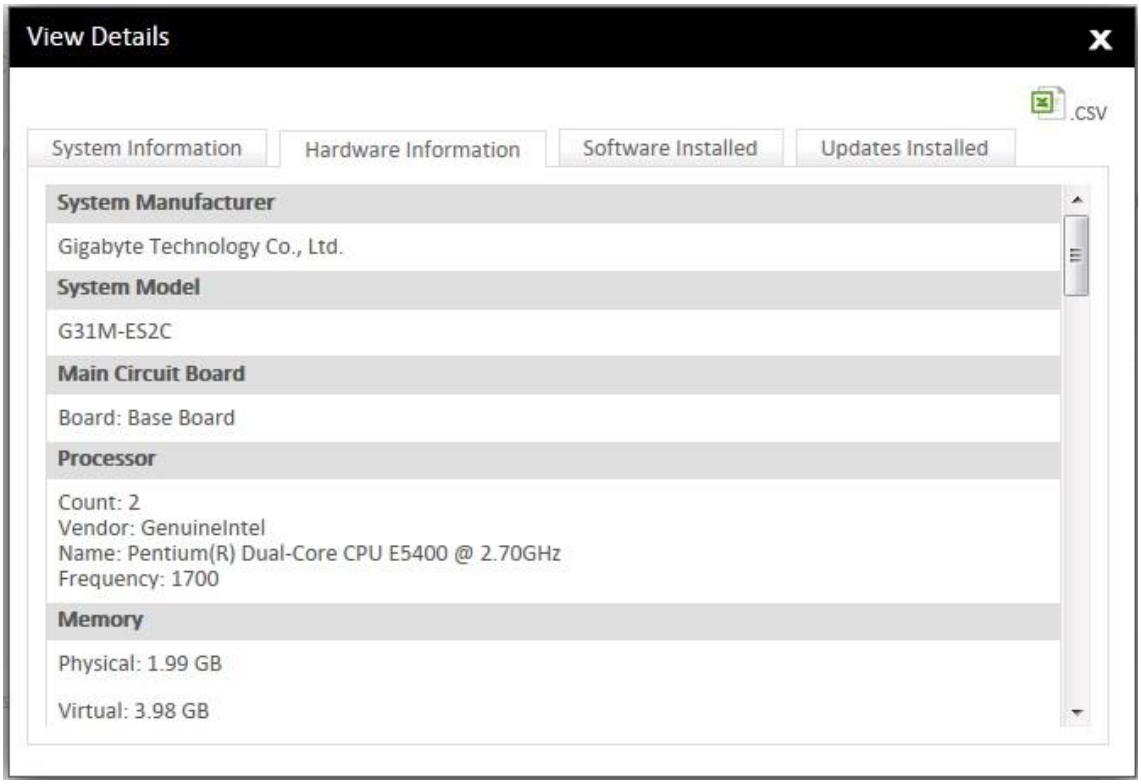
مدیریت دارایی یکی از ویژگی‌های پرکاربرد کوییک‌هیل اندپوینت سکیوریتی ٦ می‌باشد. با استفاده از این امکان، مدیران IT می‌توانند از کلیه سرمایه‌های نرم‌افزاری و سخت‌افزاری سازمان خود مطلع گردند. با استفاده از این ماژول می‌توان اطلاعات جامع سیستمی، سخت‌افزاری، نرم‌افزاری، بروزرسانی همه کلاینت‌ها را به صورت مجتمع و متمرکز از پای کنسول دریافت نمود. نکته دیگر اینکه هرگونه تغییر سخت‌افزاری و نرم‌افزاری بر روی کلاینت‌ها به اطلاع مدیر می‌رسد.



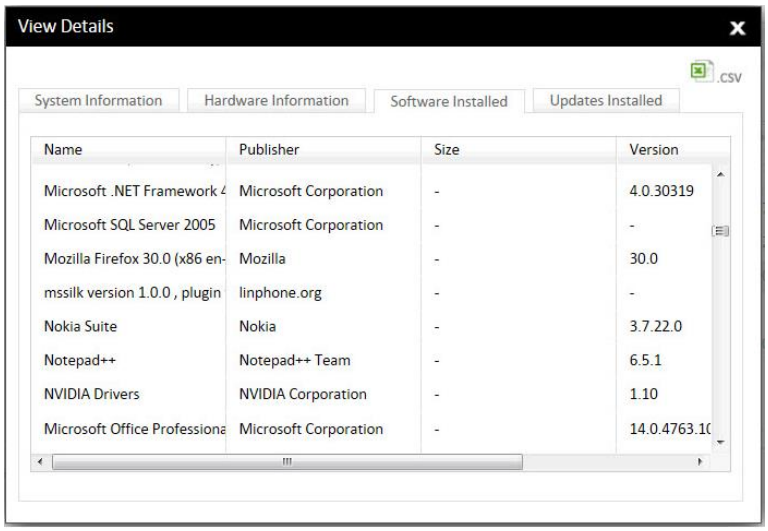
با کلیک بر روی کلاینت موردنظر و فشردن دکمه View Details می‌توانید کلیه اطلاعات کامپیوتر موردنظر را دریافت نمایید.



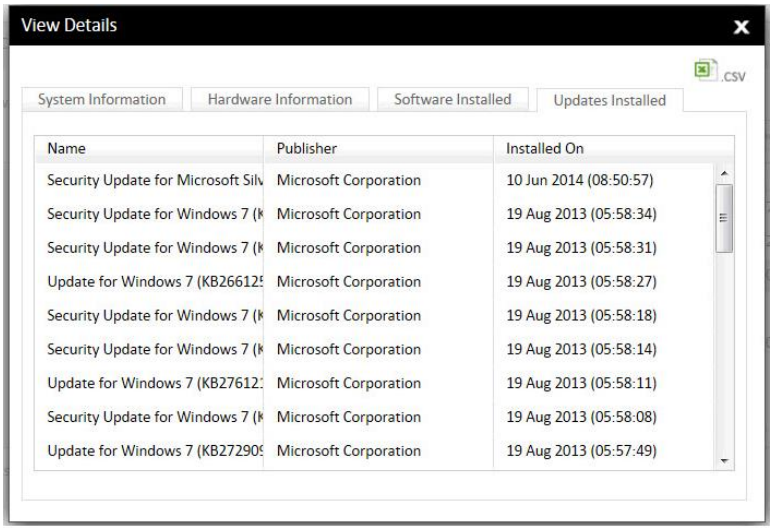
System Information: اطلاعات جامع سیستمی در این بخش قابل ملاحظه می‌باشد. این اطلاعات شامل نام کامپیوتر، دامنه، جزئیات سیستم عامل، حساب‌های کاربری ساخته شده بر روی سیستم، زمان روشن شدن و خاموش شدن قبلی سیستم می‌باشد.



Hardware Information: اطلاعات کامل سخت‌افزاری کلاینت در این بخش قابل مشاهده می‌باشد. این اطلاعات شامل سازنده سیستم، مدل، سریال و مدل مادربورد، اطلاعات CPU، حافظه اصلی RAM، هارد دیسک و میزان ظرفیت و فضای آزاد درایوها، بایوس، مشخصات کارت گرافیک، کارت صدا، اطلاعات کامل کارت شبکه، مانیتور و چاپگرهای متصل به سیستم می‌باشد.



Software Installed: لیست کامل نرم‌افزارهای نصب شده بر روی کلاینت‌ها به همراه اطلاعات کاملی از نرم‌افزار مربوطه و تاریخ نصب در این بخش قابل مشاهده می‌باشد.

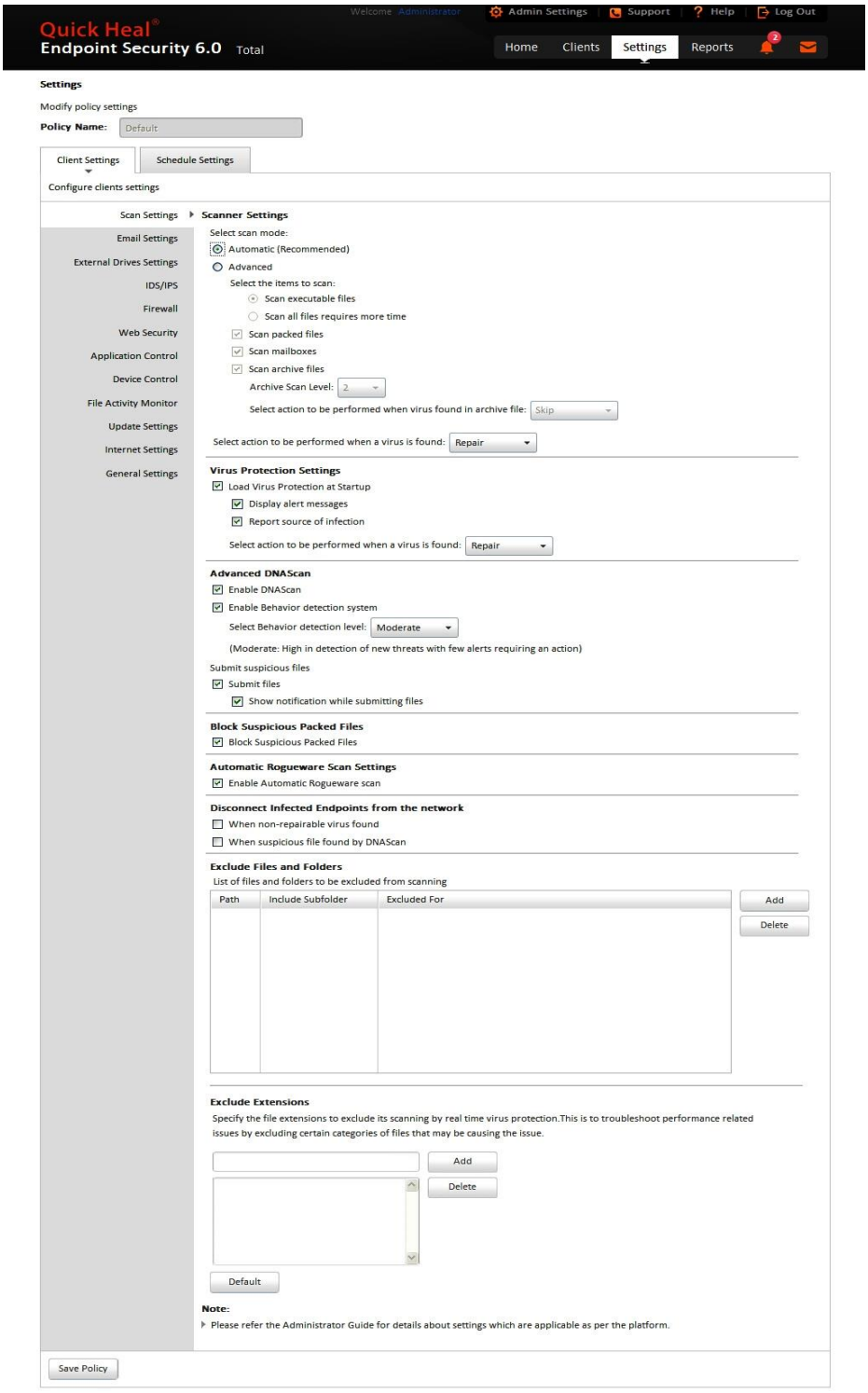


Updates Installed: هرگونه بروزرسانی نرم‌افزاری و سیستم‌عامل در این بخش قابل مشاهده می‌باشد.

نکته: در صورت به وجود آمدن هرگونه مشکل بر روی کلاینتی خاص، می‌توان از طریق مشاهده تاریخ و زمان بروزرسانی، نصب یا حذف نرم‌افزارها و تغییرات سخت‌افزاری، نسبت به عیب‌یابی آن اقدام نمود.

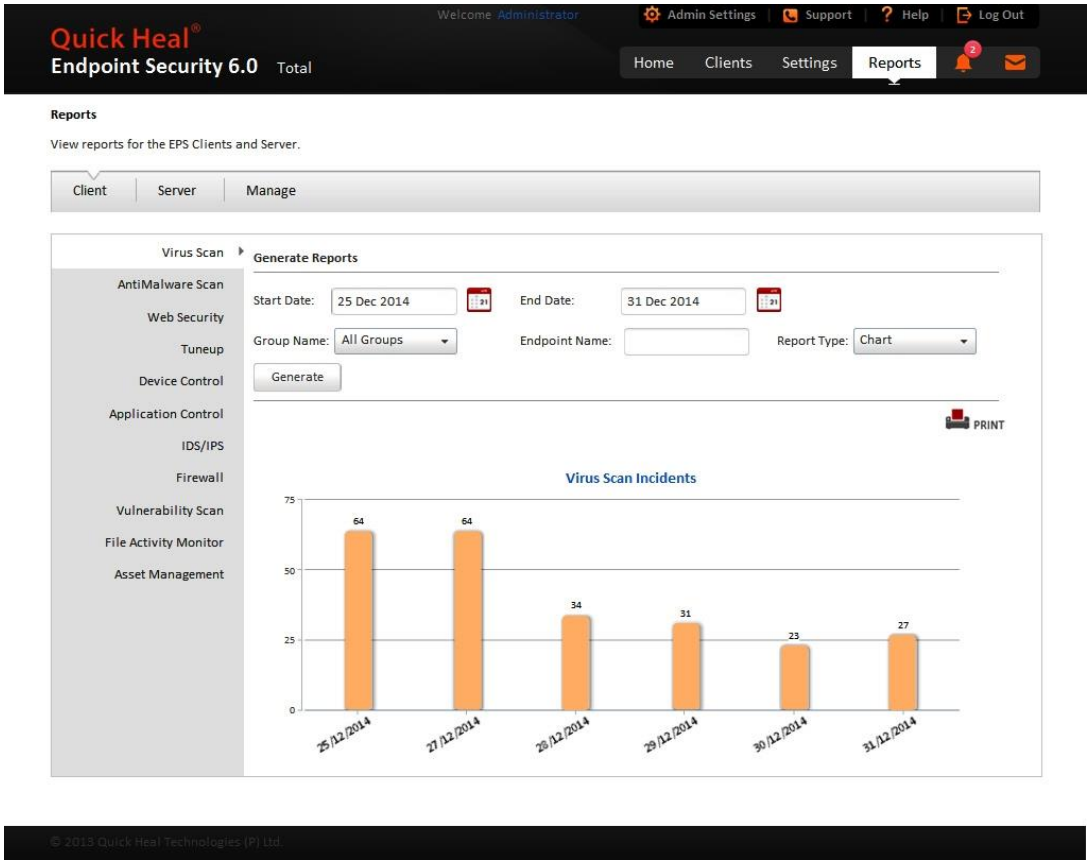
Settings

گزینه های این بخش دقیقاً 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 کلاینت‌ها می‌باشد.



Reports

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



در بخش ***Client***، گزارش‌های مختلف امنیتی قابل تولید است. گزارش‌های مربوط به اسکن ویروس (Virus Scan)، اسکن ضد بدافزار (AntiMalware Scan)، امنیت وب (Web Security)، بهینه‌سازی (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

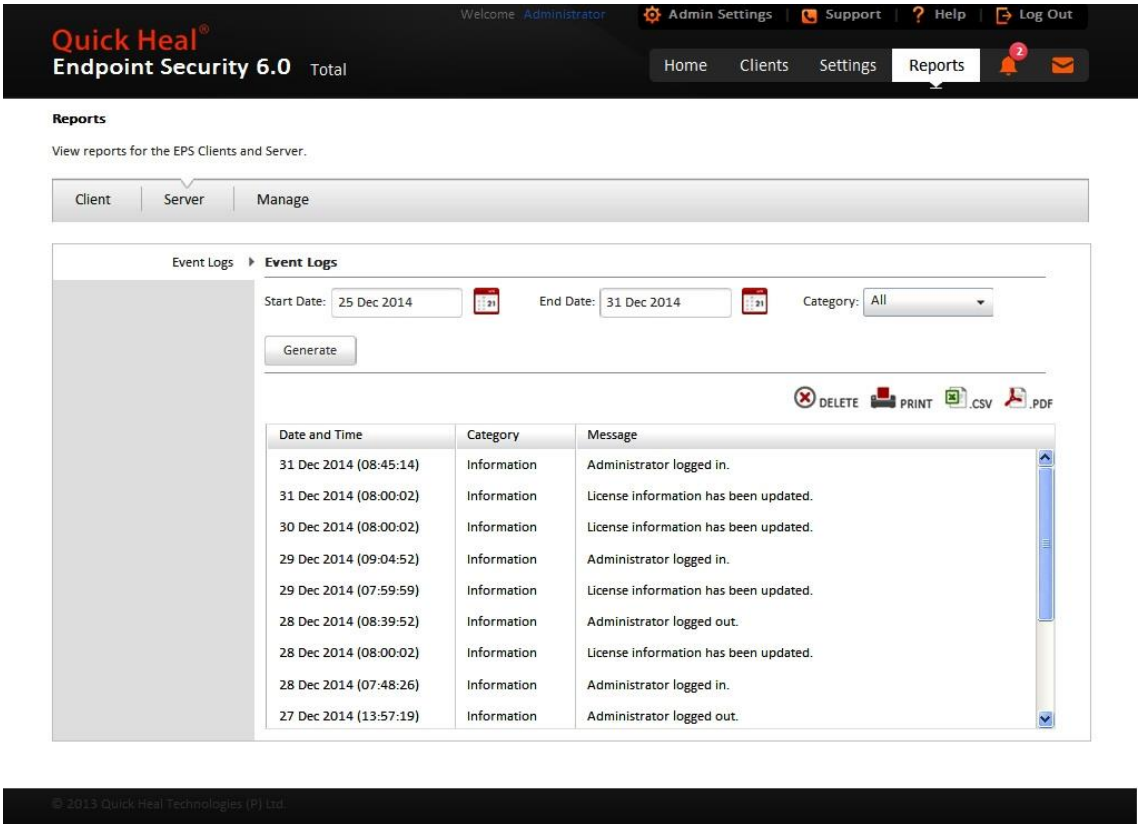
Group Name: نام گروه

Computer Name: نام کامپیوتر که می‌تواند خالی باشد.

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

Server

بخش دوم گزارش‌ها Server می‌باشد. در این بخش، گزارش‌های مربوط به سرور اندپوینت‌سکیوریتی قابل مشاهده، خروجی و چاپ است.



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

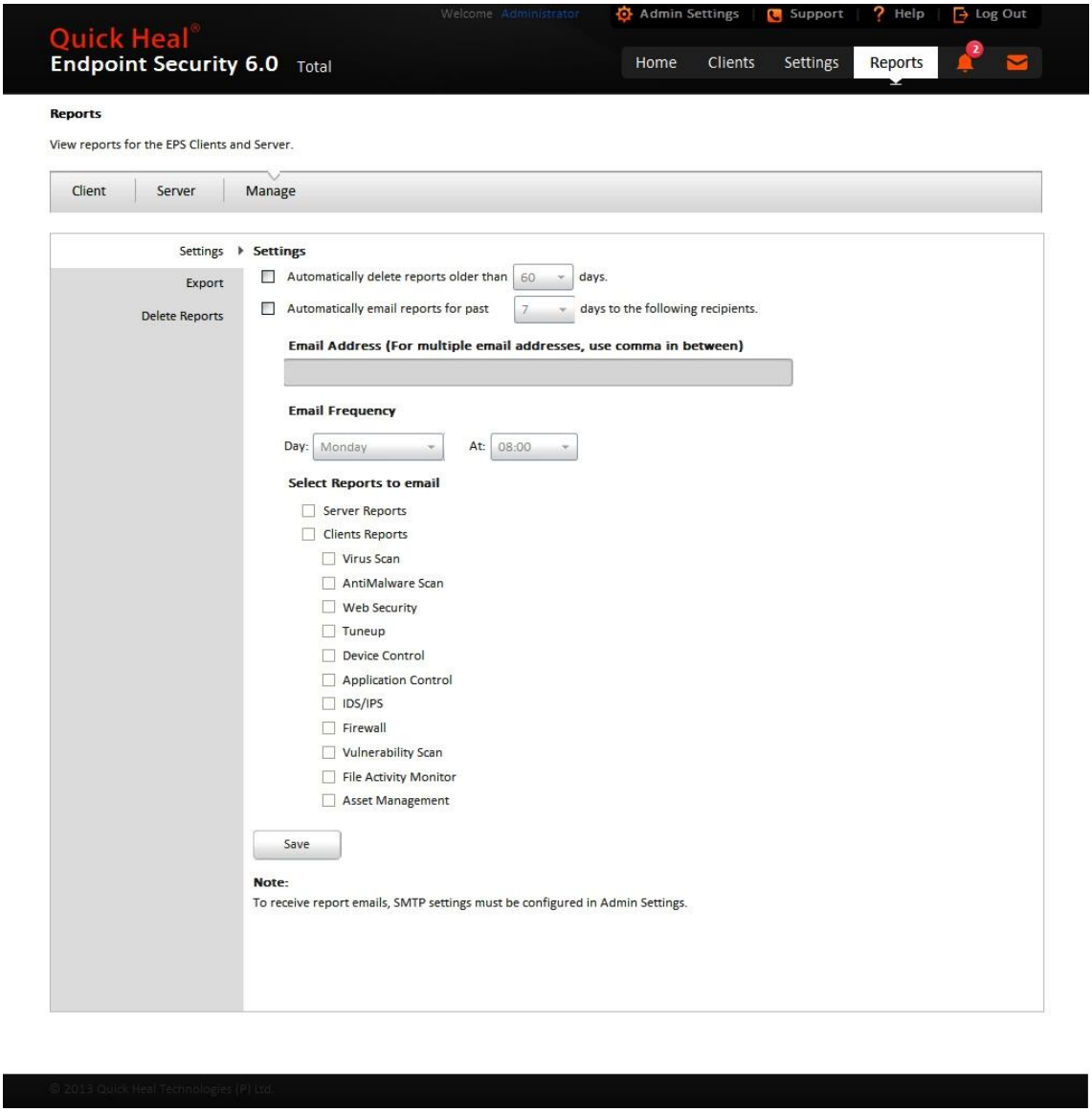
.CSV با کلیک بر روی این دکمه، خروجی CSV می‌دهد.

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 و تعیین تعداد روز، گزارش‌ها پس از مدت زمان مذکور حذف می‌گردند.

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

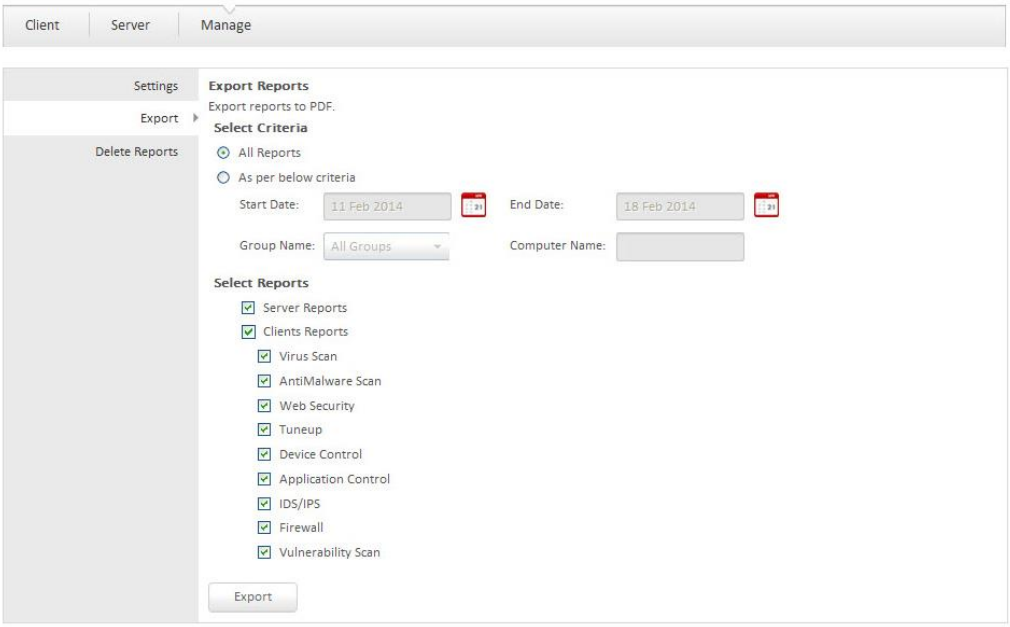
Email Address: آدرس ایمیل مقصد را در این بخش وارد می‌کنید. با کاما (,) می‌توانید چندین ایمیل را از هم جدا کنید.

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 ،Control ،Application Control ،IDS/IPS ،Firewall و Vulnerability Scan

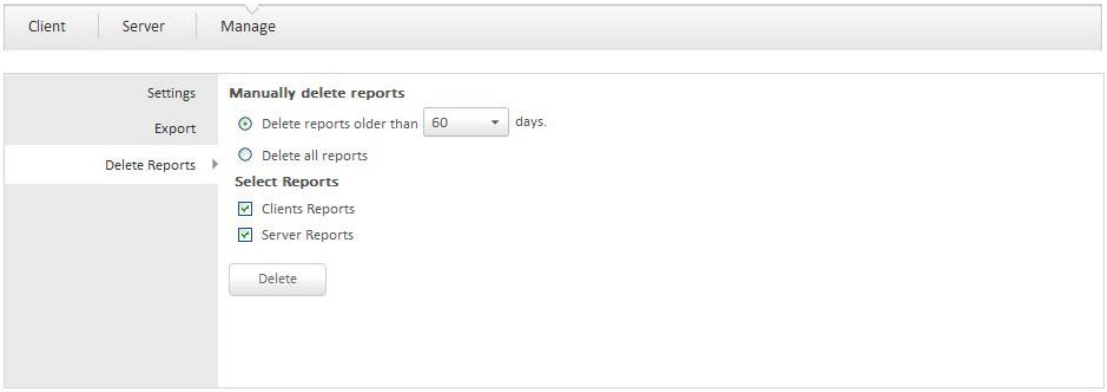
Export

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



Delete Reports

در این 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 کلاینت‌ها حذف گردند.

Server Reports: گزارش های سرور حذف گردند.

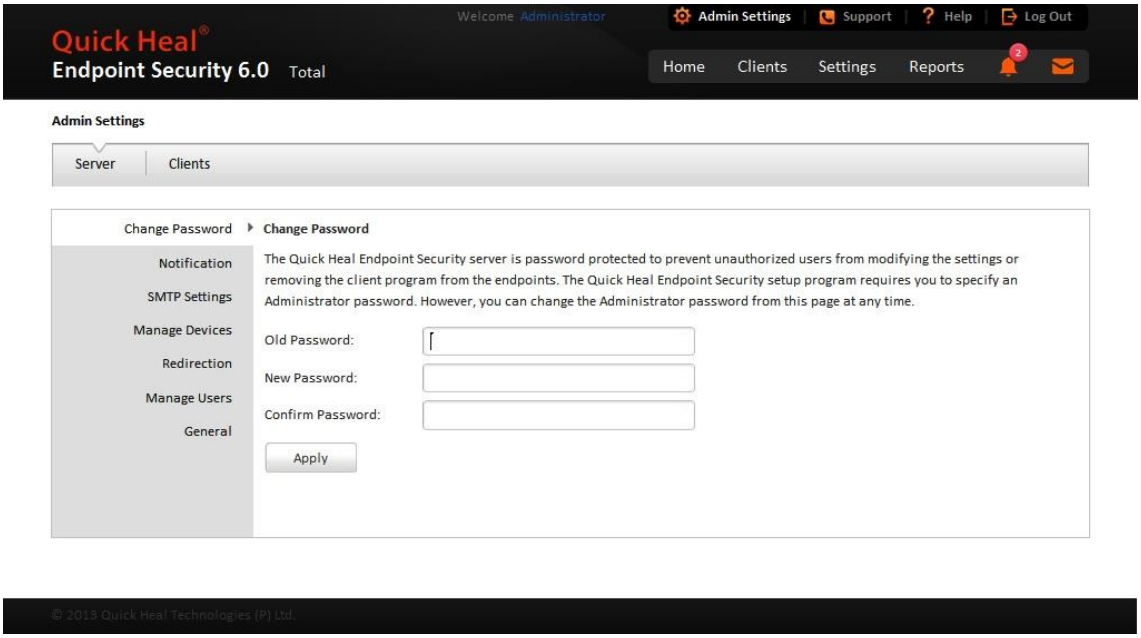
Delete: با انتخاب موارد فوق و کلیک بر روی این دکمه گزارش ها حذف می‌گردند.

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...)

Admin Settings

در این بخش تنظیمات مدیریتی ادمین اندپوینت‌سکیوریتی کوییک‌هیل قرار دارند.

Change Password



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

Old Password: رمزعبور قبلی را وارد کنید.

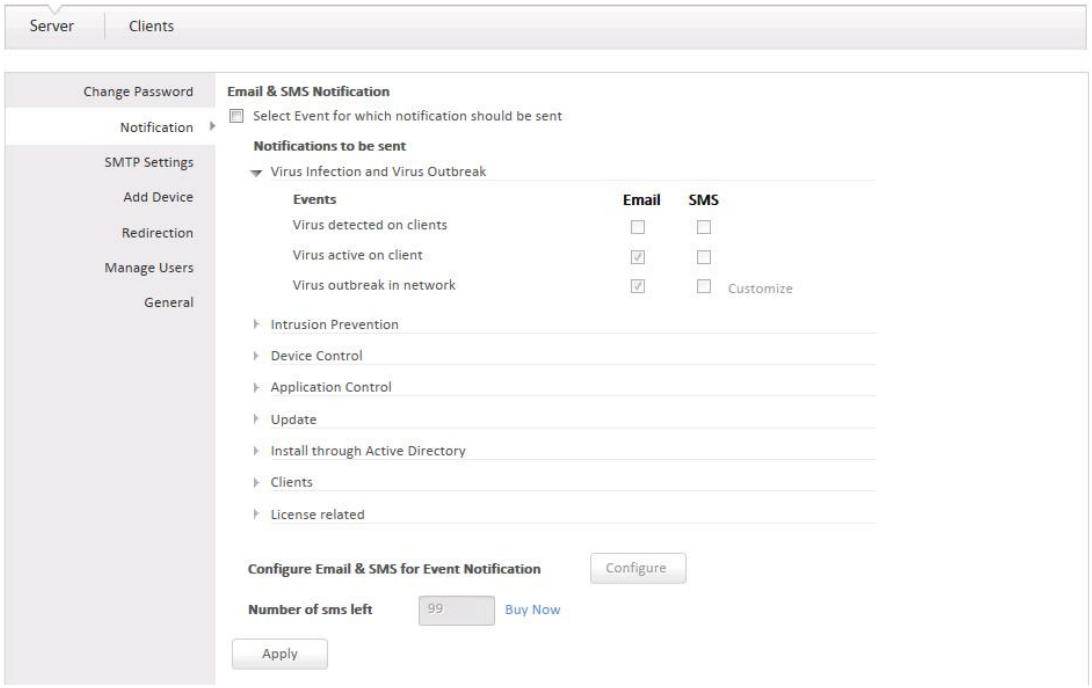
New Password: رمزعبور جدید را وارد کنید.

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 می‌توانند 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 می‌تواند 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 می‌توانید 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 صورت بروز رویداد پویش پورت (Port Scanning) بر روی کلاینت، به اطلاع مدیر برسد.

DDOS Attack detected on client: در صورت 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 می‌باشد.

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

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

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

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 می‌رسد.

Clients are not updated to latest virus definitions: در صورتی که کلاینت‌ها بروزرسانی نشده باشند، به اطلاع مدیر می‌رسد.

Update Manager virus definition date is older: در صورتی که تاریخ بروزرسانی آپدیت منیجر (Update Manager) قدیمی باشد، به اطلاع مدیر می‌رسد.

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

Synchronization with Active Directory failed: در صورتی که همگام سازی با اکتیودایرکتوری با شکست روبرو شد، به اطلاع مدیر می‌رسد.

Clients: اطلاع رسانی مربوط به کلاینت‌ها در این بخش قابل پیکربندی می‌باشد.

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

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

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

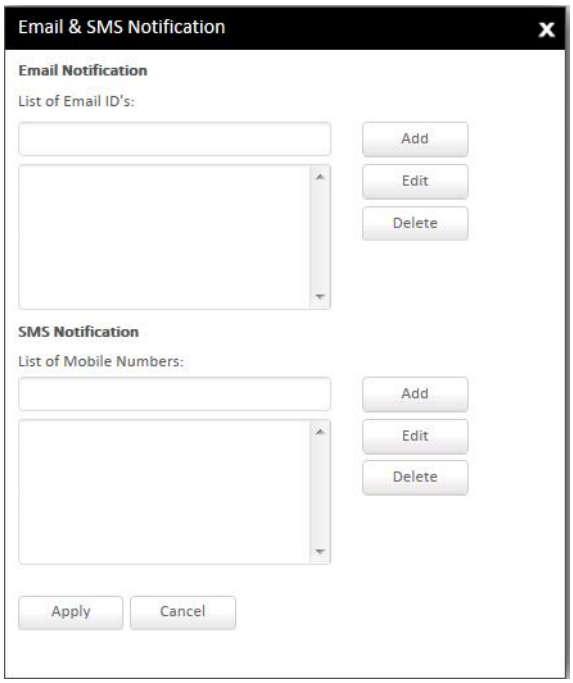
License related: اطلاع رسانی مربوط به لایسنس در این بخش قابل پیکربندی می‌باشد.

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

License is about to expire: در صورتی که 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.

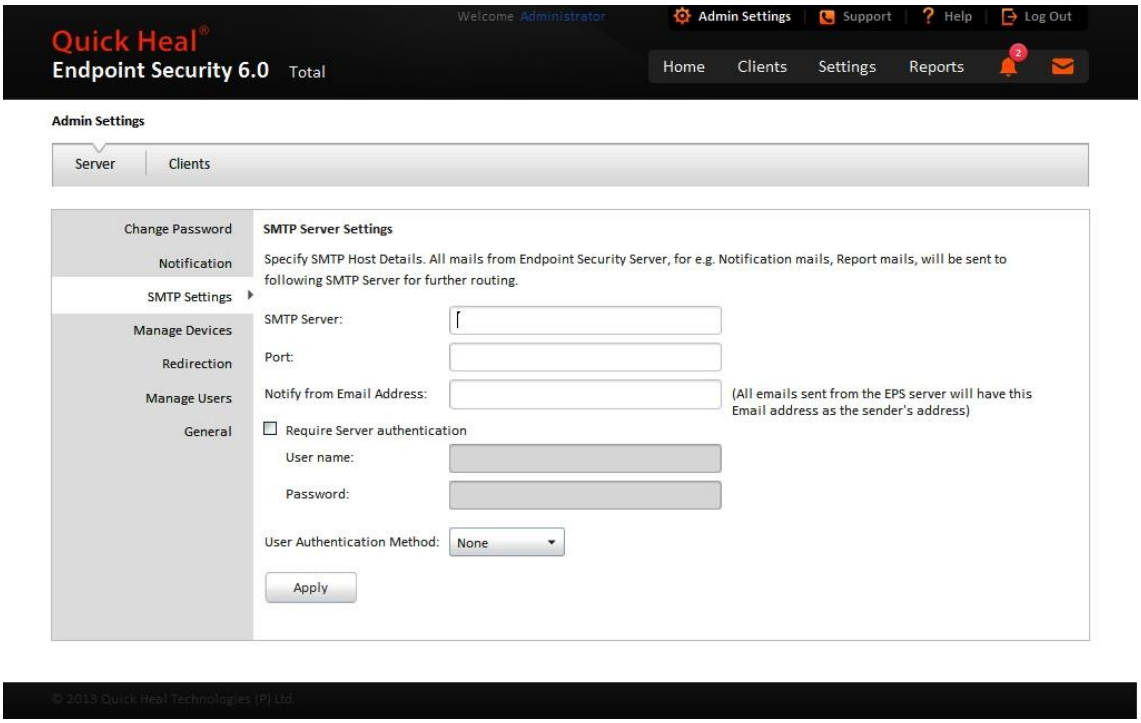
Configure Email & SMS for Event Notification: در این قسمت ایمیل و SMS خود را برای اطلاع‌رسانی پیکربندی می‌کنید. با کلیک بر روی دکمه Configure پنجره زیر باز می‌شود.



با وارد کردن شناسه ایمیل وشماره موبایل و زدن دکمه Add می‌توانید 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.

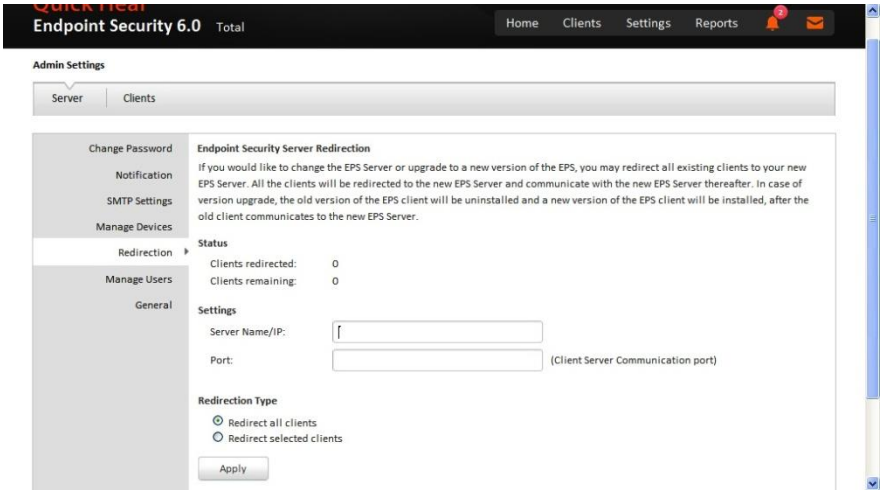
Require Server authentication: در صورتی که سرور SMTP نیاز به احراز هویت دارد، این گزینه را تیک کنید.

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 می‌تواند 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 کلاینت‌ها می‌باشد. همچنین در صورت تمایل می‌توانید، 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 می‌کنید. سپس آدرس IP و یا نام سرور -بسته به روش نصب- و آدرس پورت سرور جدید اندپوینت را در نسخه قبلی اندپوینت وارد می‌کنید. به صورت خودکار همه کلاینت‌ها 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 کلاینت‌ها نصب می‌شود.

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

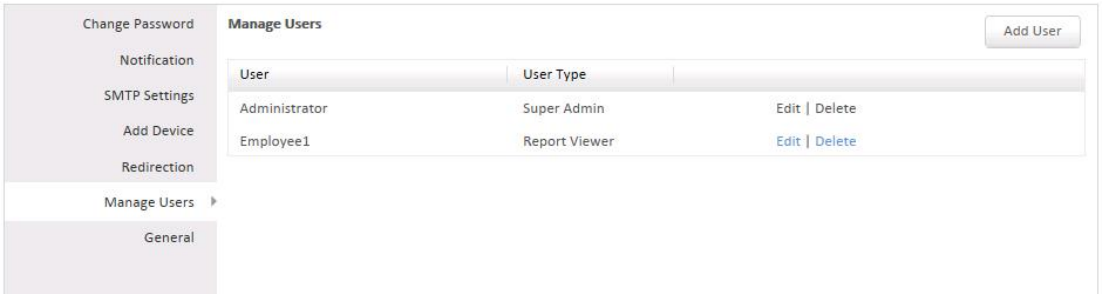
Server Name/IP: نام سرور یا IP اندپوینت جدید را وارد می‌کنید. (در صورتی که اندپوینت جدید را بر روی همان سرور قبلی نصب کردید، آدرس IP یا نام همین کامپیوتر را وارد کنید)

Port: آدرس پورت اندپوینت جدید را در این بخش وارد کنید، آدرس پورت همان آدرسی است که کلاینت‌ها با سرور ارتباط برقرار می‌کنند (مثلاً پورت پیش فرض در Quick Heal Endpoint Security 6.0، آدرس ٥٠٤٤ می‌باشد.)

نکته: برای انتقال کلاینت‌ها به سرور جدید، ابتدا نسخه جدید اندپوینت را اکتیو کرده، سپس وارد کنسول قبلی شده و آدرس IP (مثلا 192.168.0.2) و شماره پورت (مثلا 5044) اندپوینت جدید را در بخش Redirection وارد نمایید.

Manage Users

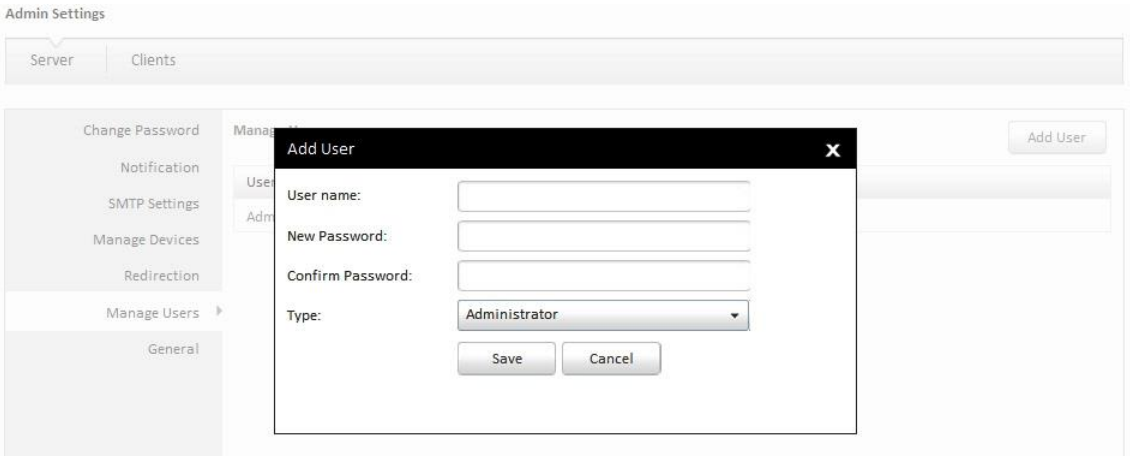
در این بخش، کاربران استفاده کننده از کنسول اندپوینت‌سکیوریتی، قابل مدیریت می‌باشند.



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.

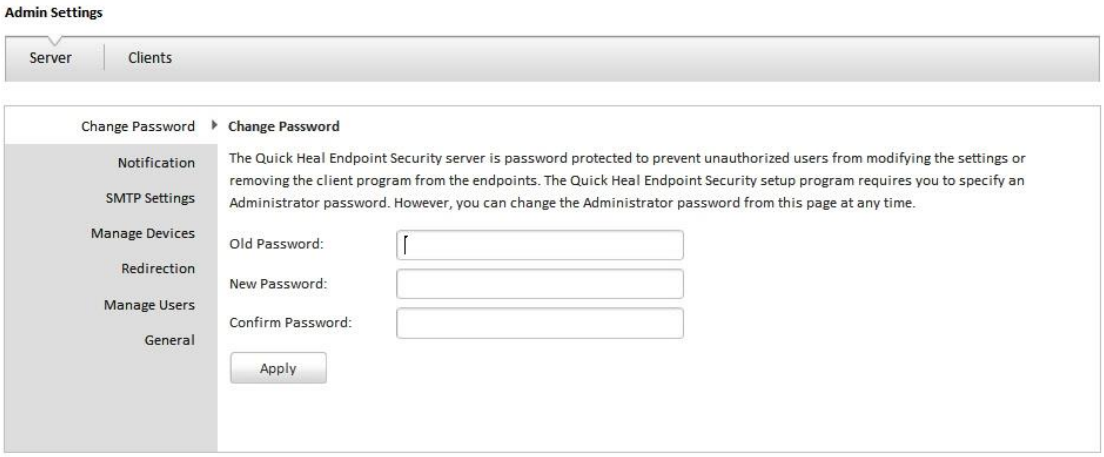
New Password: رمز عبور در این فیلد وارد می‌شود.

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

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

General

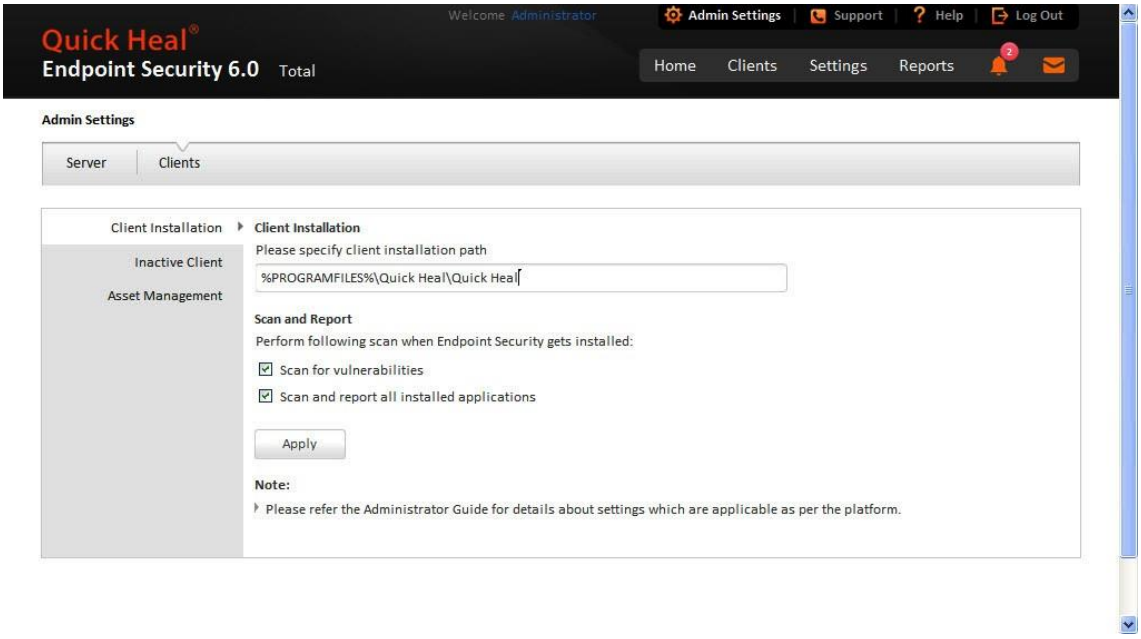
در این بخش می‌توانید زمان اتمام نشست کنسول تحت وب مدیریتی اندپوینت را مشخص کنید.



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 می‌توانید مسیر نصب کلاینت‌ها 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 کلاینت‌ها قابل پیکربندی است.

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

Scan and report all installed applications: پس از اتمام نصب، نرم افزار شروع به اسکن همه برنامه‌های نصب شده و تهیه گزارش از آنها می‌نماید.

Inactive Client Settings: تنظیمات کلاینت‌های 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 آن را حذف شده در نظر گرفته و لایسنس آن را برای نصب بر روی سیستم دیگر آزاد می‌کند.

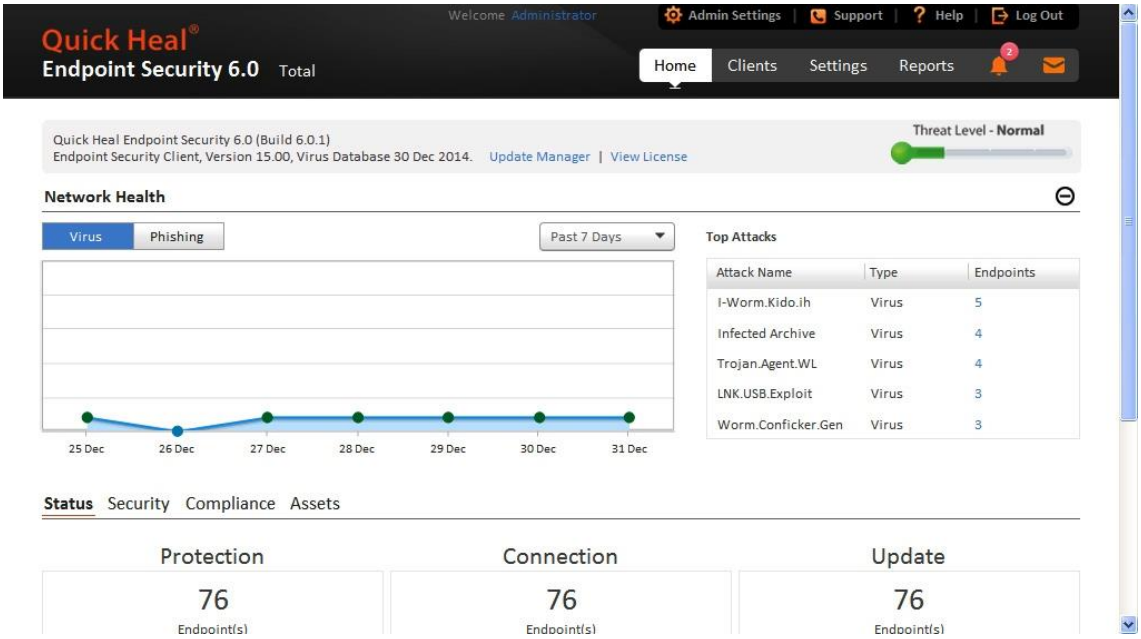
مدیریت لایسنس

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

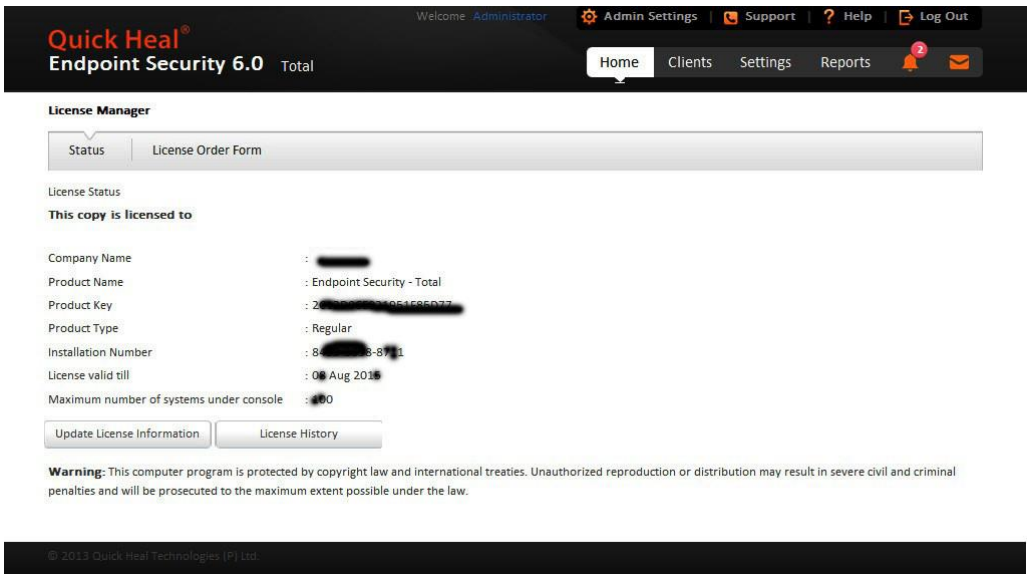
همچنین یکی از قابلیت های کوییک‌هیل در بخش لایسنسینگ، امکان افزودن تعداد کلاینت پس از خرید اولیه است. به عنوان نمونه پس از مدتی تعداد کلاینت‌ها شبکه شما افزایش یافته و نیاز به افزایش تعداد لایسنس مجاز دارید، بدون نیاز به نصب کنسول مجزا، یا خرید لایسنس کامل مجدد، تنها کافی است به تعداد مورد نیاز افزوده 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 کلاینت‌ها میسّر 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 طوسی رنگ ابتدای صفحه نخست بر روی لینک View License کلیک نمایید تا صفحه مربوط به License Manager و سربرگ Status باز شود.



برای اعمال تغییرات و بروزرسانی وضعیت لایسنس، 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 ۲ نمونه از روش های پرکاربرد اشاره می‌کنیم. این روش ها بر روی انواع ساختارهای شبکه (Domain-based و Workgroup) قابل استفاده است.

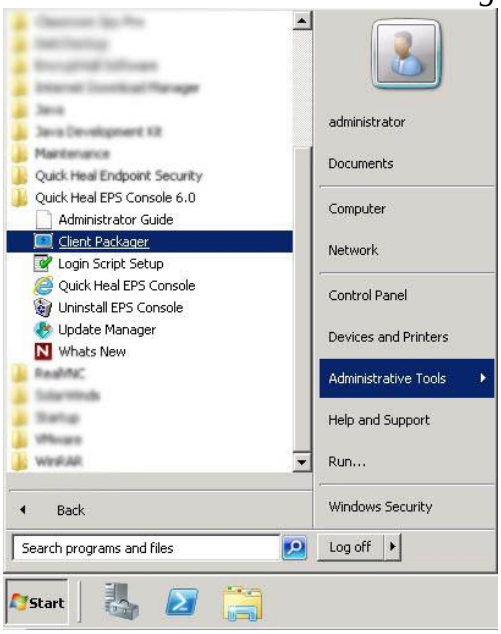
نکته: بعد از نصب و یا آپگرید اندپوینت جدید، کلاینت پکیجر جدید باید ساخته و نصب شود.

الف) استفاده از Client Packager:

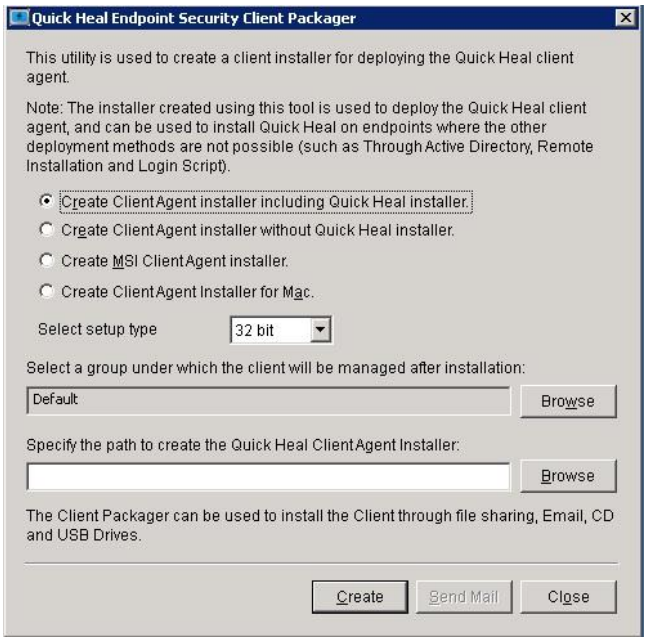
ساده ترین راه، نصب بر روی کلاینت‌ها می‌باشد. یک فایل پکیجر نصب کننده ساخته و آن را بر روی کلاینت‌ها (از طریق به اشتراک گذاری در شبکه و یا فلش) منتقل و اجرا می‌کنید.

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

Start > Quick Heal EPS Console 6.0> 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 و 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.

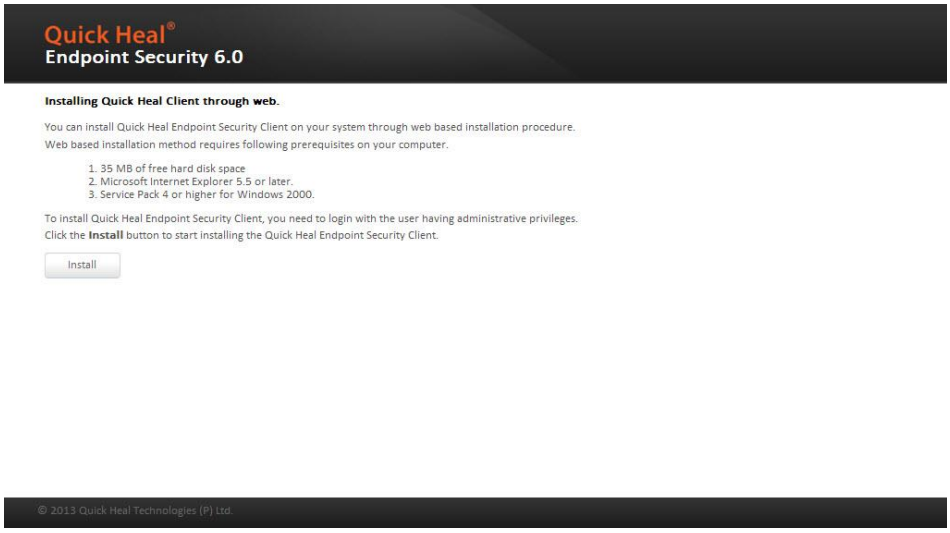
Select a group under which the client will be managed after installation: اگر از قبل گروه و پالیسی در سرور اندپوینت تعریف کرده اید، می‌توانید گروه را در این بخش تعیین کنید تا پکیجر متناسب با آن گروه ساخته شود. همچنین می‌توانید گروه را به صورت Default رها کرده و پس از نصب بر روی کلاینت، آن را عضو گروه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

Specify the path to create the Quick Heal ClientAgent installer: مسیر ساخت کلاینت ایجنت در این قسمت مشخص می‌شود. می‌توانید 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 کلاینت‌ها استفاده از IE، می‌باشد. در این روش آدرس زیر را در اینترنت اکسپلورر کاربر وارد کرده و برروی دکمه Install کلیک می‌کنید:

https://SERVER-IP:PORT/qhscan6/install.htm

مثل:

https://192.168.0.1:9099/qhscan6/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 ۷۷۱۴۲۵۲۶-۰۲۱ تماس حاصل فرمایید.