

راهنمای سریع استفاده از کوئیک هیل اندپوینت سکیوریتی

QuickHeal Endpoint Security 6.4



شرکت فناوری ارتباطات و اطلاعات فانوس

نماینده رسمی محصولات امنیتی کوئیک 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 کوییک هیل در ایران چکیده بیش از ۷ سال تجربه کار با نسخه سازمانی آنتی ویروس کوییک هیل را به صورت کاربردی و ساده، در این جزوه آموزشی گرد آورده است.

در صورت داشتن هر نوع سوال، پیشنهاد یا انتقادی می توانید با شرکت فناوری ارتباطات و اطلاعات فانوس از طریق ایمیل info@qhi.ir تلفن ۰۲۱-۷۷۱۴۲۵۲۶ ، 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 می باشد و حق نسخه برداری برای این شرکت محفوظ است.

فهرست مطالب

۴	نصب کنسول مدیریتی اندپوینت سکیوریتی کوئیک هیل
۱۶	آغاز به کار کنسول مدیریتی متمرکز اندپوینت سکیوریتی کوئیک هیل
۲۱	داشبورد مدیریتی
۲۸	کلاینت‌ها Clients
۳۹	سربرگ Client Settings
۴۴	Email Settings
۴۵	External Drives Settings
۴۶	IDS/IPS
۴۷	Firewall
۵۱	Web Security
۵۳	Application Control
۵۶	Device Control
۶۰	مستثنی کردن ابزار
۶۰	معرفی حافظه USB فلش به لیست Device Control
۶۲	Data Loss Prevention
۶۰	تعریف دیکشنری جدید
۶۲	File Activity Monitor
۶۴	Update Settings
۷۱	Internet Settings
۷۲	General
۷۳	Schedule Settings
۷۳	Client Scan
۷۵	Application Control Schedule Scan
۷۶	Tuneup Schedule Scan
۷۲	Vulnerability Scan
۷۳	Assets
۸۱	Settings
۸۲	Reports
۸۳	Server
۸۴	Manage
۸۷	Admin Settings
۹۵	Client Installation
۹۶	مدیریت لایسنس
۹۸	نصب بروی کلاینت

نصب کنسول مدیریتی اندپوینت سکیوریتی کوپیک هیل

نصب و پیکربندی Seqrite Endpoint Security (SEPS) ساده می باشد. در طول نصب به پیغام ها توجه کرده و مطابق راهنما پیش روید.

۱. پیش نیاز های سیستمی

- پیش از شروع به نصب سکورایت اندپوینت سکیوریتی کوپیک هیل، به موارد زیر توجه کنید:
- پیش از شروع به نصب، آنتی ویروس قبلی نصب شده بر روی سرور و کلاینت ها را حذف کنید. نصب چند آنتی ویروس همزمان بر روی یک سیستم ممکن است موجب اختلال در عملکرد سیستم گردد.
- شبکه با پروتکل TCP/IP می بایست پیکربندی شده و سرور می بایست IP به صورت استاتیک و دستی داشته باشد (نه DHCP).
- گزینه File and printer sharing for Microsoft Networks بر روی کارت شبکه باید فعال باشد.
- برای نصب نیاز به دسترسی سطح کاربری administrator و یا domain administrator دارید.
- برای استفاده از گزینه نصب Login Script، در سیستم عامل های Windows Server 2012 R2 / Windows Server 2012 / Windows 2008 Server R2 / Windows 2008 Server / Windows 2003 Server / Windows 2000 Server / Windows 2000 Server Advanced Server باید به صورت صحیح با سرویس های اکتیو دایرکتوری پیکربندی شوند.

الف) پیش نیازهای سیستمی برای سرور SEPS

نیازمندیهای سیستمی برای سرور سکورایت اندپوینت سکیوریتی به شرح زیر می باشد:

نیازمندی های عمومی:

مشخصات کامپیوتری که سرور اندپوینت بر روی آن نصب می شود باید حداقل های جدول زیر را داشته باشد:

بخش	نیازمندی ها
Processor	1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium or higher
RAM	2 GB – 4 GB
Hard disk space	5200 MB

Web Browser	• Internet Explorer 7, 8, 9, 10, or 11 • Google Chrome 45, 46, or 47 • Mozilla Firefox 38, 39, or 40
Display	1024 x 768

برای کلاینت بیش از ۵۰۰ کاربر کوئیک هیل توصیه می کند:

- A dedicated Web server (IIS)
- Minimum 2 GHz processor or higher
- 4GB RAM or higher

نیازمندی های سیستم عامل:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP 32-bit SP3, 64-bit SP1 and SP2 / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)

نیازمندی های نرم افزاری:

سرور اندپوینت سکیوریتی سکورایت نیاز به وب سرور IIS و نیز .NET Framework 4.0 دارد.

وب سرور	نیازمندی ها
IIS	IIS Version 10 on Windows 10
	IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2

	IIS Version 8.0 on Windows 8 and Windows Server 2012
	IIS Version 7.5 on Windows 7 and Windows Server 2008 R2
	IIS Version 7.0 on Windows Vista and Windows Server 2008
	IIS Version 6.0 on Windows Server 2003
	IIS Version 5.1 on Windows XP SP3

همچنین کامپوننت های زیر می بایست در IIS نصب گردد:

- IIS Management Console •
- Default Document •
- Static Content •
- CGI •
- ASP.NET 4.0 or later versions •

پیش نیاز جاوا (Java Runtime Environment (JRE))

اگر بخواهید کوئیک هیل را بر روی کلاینت ها از طریق وب نصب کنید (یکی از ۶ روش نصب)، و یا ابزار جدید را برای استثنا شدن از طریق وب اضافه کنید نیاز به محیط اجرایی جاوا می باشد.

نسخه سیستم عامل	نیازمندی	JRE
32-bit	32-bit	JRE 7, JRE 8
64-bit	32-bit	32-bit JRE 7, 32-bit JRE 8
	64-bit	64-bit JRE 7, 64-bit JRE 8

ب) پیش نیازهای سیستمی برای کلاینتهای SEPS

برای نصب کوئیک هیل بر روی کلاینتها نیاز به فراهم شدن نیازمندیهای زیر می باشد:

نیازمندی های عمومی:

مشخصات کامپیوتری که کلاینت اندپوینت بر روی آن نصب می شود باید حداقل های جدول زیر را

داشته باشد:

بخش	نیازمندی ها
Processor	1 GHz 32-bit (x86) or 64-bit (x64) for Windows Vista or later
RAM	1 GB
Hard disk space	3200 MB
Web Browser	Internet Explorer 5.5 or later

نیازمندی های سیستم عامل:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)

- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise / Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server

نیازمندی های سیستمی برای Mac OS:

برای نصب اندپوینت سکیوریتی بر روی کلاینت MacOS نیاز به حداقل های سخت افزاری و نرم افزاری زیر می باشد:

وب سرور	نیازمندی ها
MAC OS	Mac OS OS X, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11
Processor	Intel or compatible
RAM	512 MB
Hard disk space	1200 MB

نیازمندی های سیستمی برای Linux OS:

برای نصب اندپوینت سکیوریتی بر روی کلاینت لینوکس نیاز به حداقل های سخت افزاری و نرم افزاری زیر می باشد:

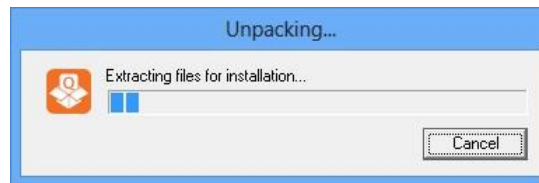
اجزا	نسخه لینوکس	نیازمندی ها
Linux OS	32-bit	• BOSS 6 • Fedora 14, 19 • openSUSE 11.4, 12.2, 12.3 • Ubuntu 10.10, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, and 15.04
	64-bit	• Fedora 14, 18, 19 • openSUSE 12.2 • Ubuntu 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, and 15.04 • CentOS 6.3
Processor		Intel or compatible
RAM		512 MB
Memory		300 MHz or higher
Hard disk space		1200 MB

ج) نصب سرور اندپوینت سکیوریتی

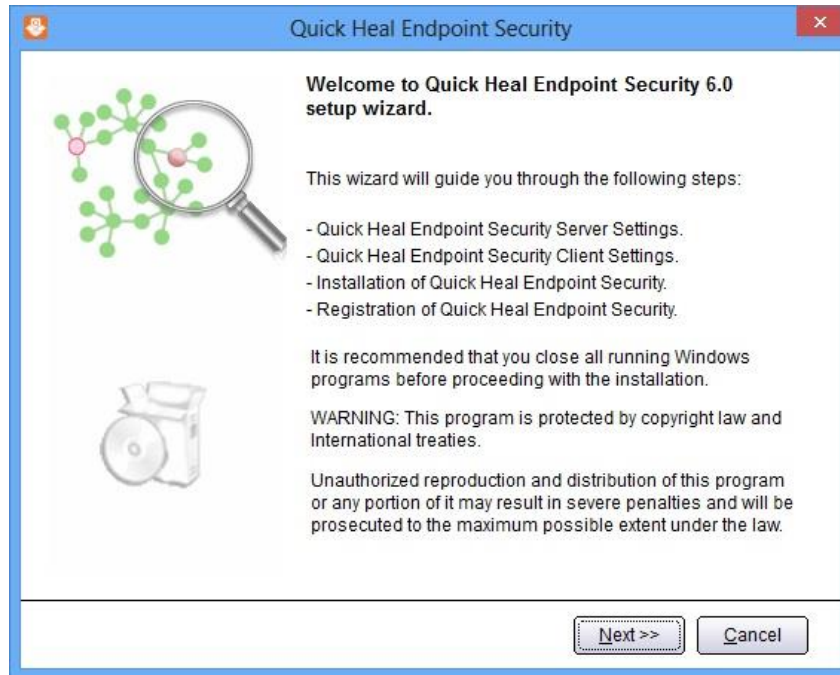
برای نصب نسخه تحت شبکه کوئیک هیل با عنوان اندپوینت سکیوریتی مراحل زیر را دنبال نمایید:



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



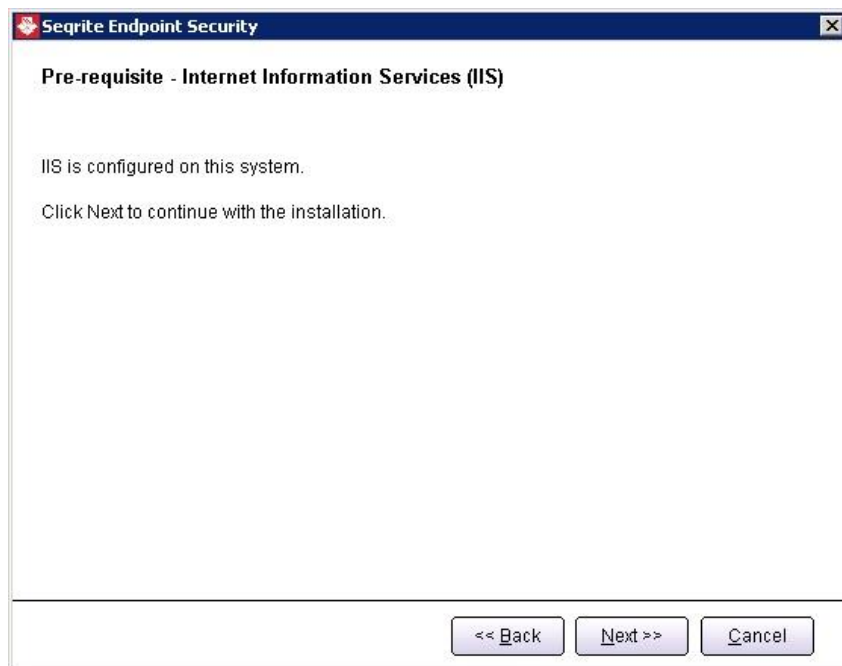
چند لحظه تأمل فرمایید تا فرایند استخراج فایل فشرده نصب تکمیل گردد.



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



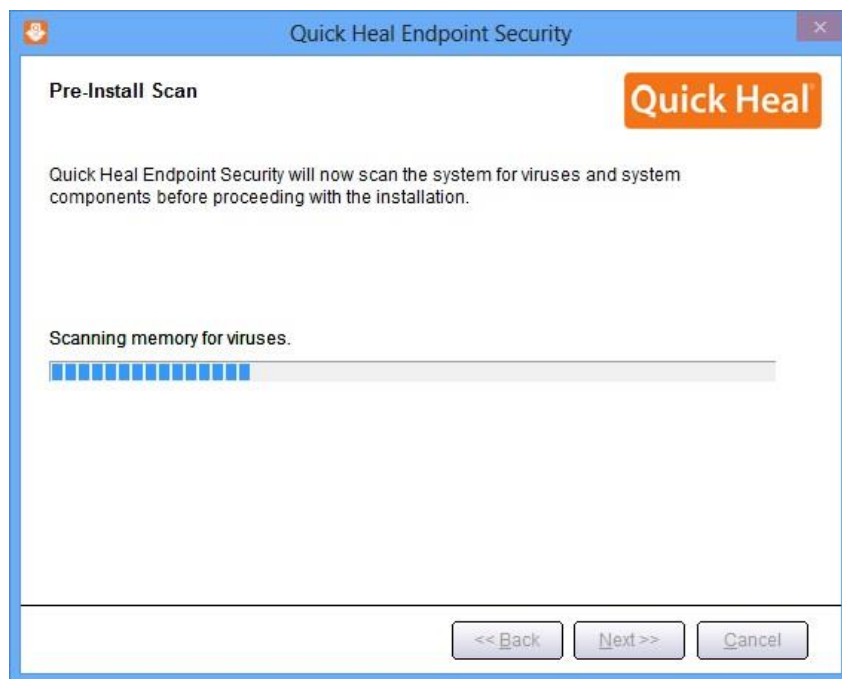
پس از قرائت توافقنامه حفظ قوانین کی‌رایت باید گزینه **I Agree** را انتخاب و بر روی **Next** کلیک نمایید.



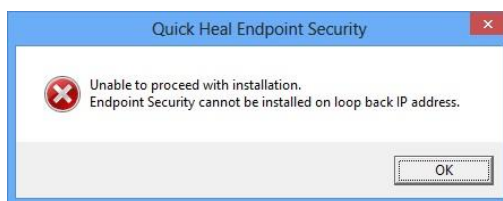
در صورتی که IIS و .Net Framework 4.0 به درستی نصب و پیکربندی شده باشند، این صفحه نمایش داده می‌شود. [در صورتی که مایلید از IIS استفاده نمایید و IIS Server بر روی سیستم شما نصب نیست، باید از مسیر Control Panel/Add or Remove Programs/Add or Remove Components/ Internet Information Services(IIS) نصب انجام گیرد. سپس برنامه مجدداً اجرا گردد.]



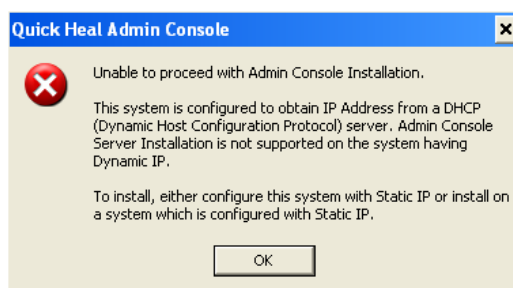
در این مرحله باید مسیر نصب برنامه تعیین شود که می‌توان همان مسیر پیش فرض را انتخاب و **Next** را فشرد.



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 می‌کند، این پیغام نمایش داده خواهد شد. برای رفع این مشکل یک IP استاتیک به کارت شبکه اختصاص دهید.

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 می باشد، در صورتی که پورت های فوق در شبکه شما استفاده می شوند، آنها را تغییر دهید، در غیر این صورت پیش فرض را تایید نموده و بر روی **Next** کلیک نمایید.

برای تایید اطلاعات فوق، بر روی دکمه **Yes** کلیک نمایید.

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

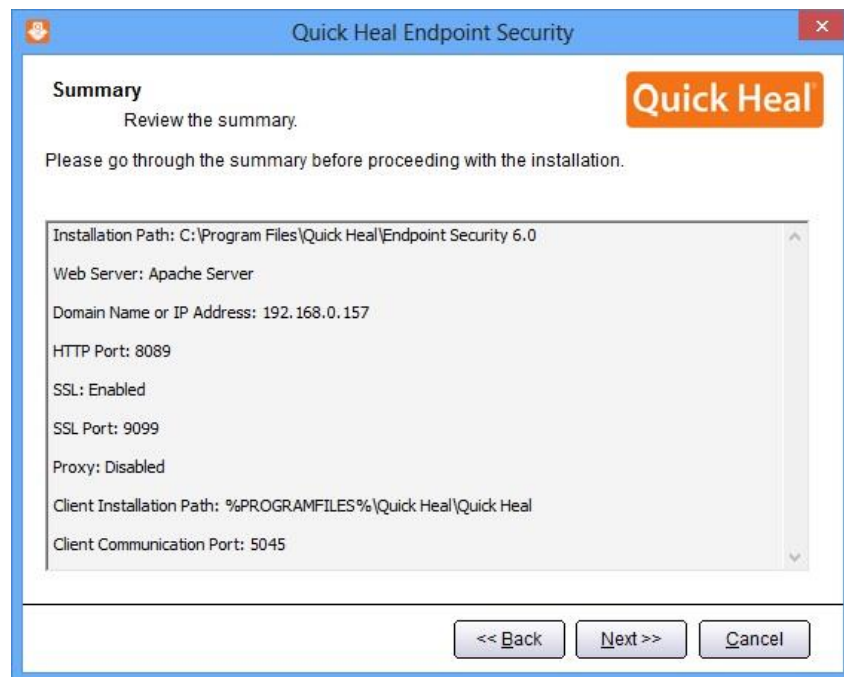
این صفحه تعیین پورت مربوط به ارتباط کلاینت ها با سرور اندپوینت آنتی ویروس است. در صورتی که پورت های فوق آزاد می باشند، پیش فرض را انتخاب و **Next** را بفشارید.



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



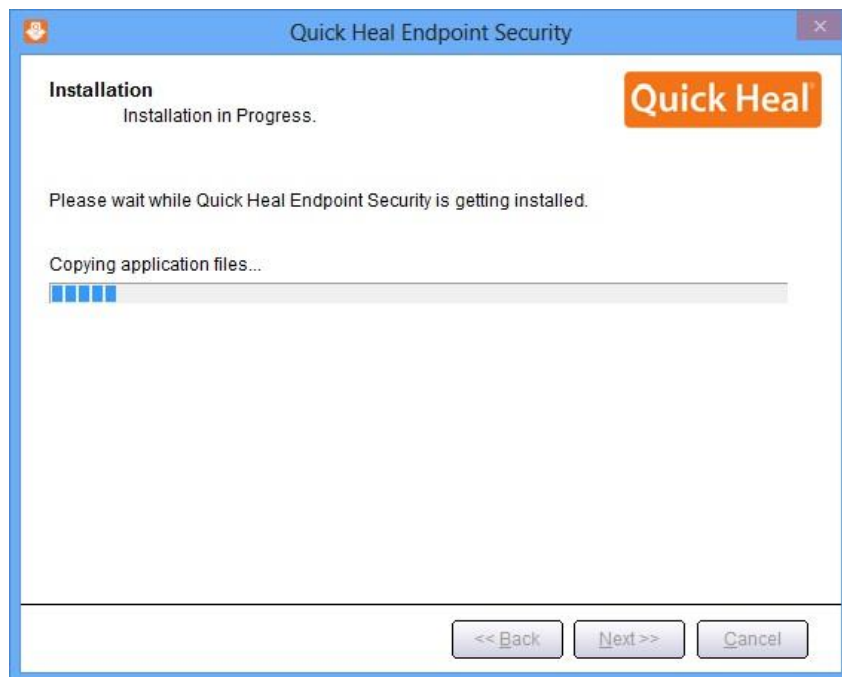
تعیین رمز عبور برای نرم افزار مدیریت سرور و دسترسی به تنظیمات کلاینت از سوی کاربر که به صورت متفاوت باید وارد شود.



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



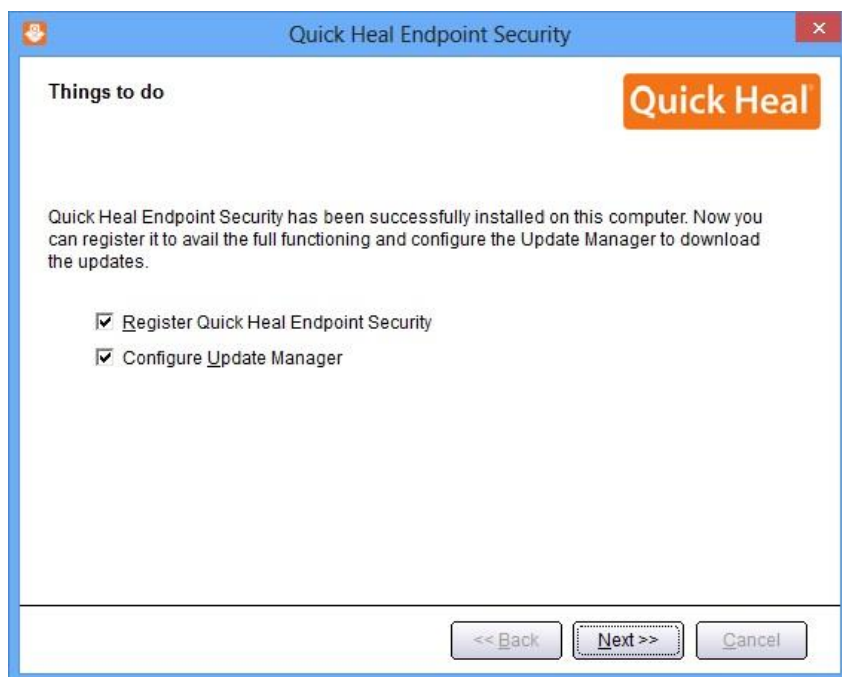
در این صفحه تنظیمات مربوط به پیکربندی IP و پورت نمایش داده می‌شود. در انتها به کاربر پیغامی مبنی بر قطع و وصل موقتی خودکار شبکه در هنگام نصب نمایش داده می‌شود.



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



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



این صفحه به شما اطلاع می‌دهد کوئیک هیل اندپوینت سکیوریتی با موفقیت نصب شده است. تیک بودن **Register** و **Configure** صفحه‌ی رجیستر و ثبت محصول را نمایش داده و گزینه‌ی **Update Manager**، پنجره پیکربندی مدیریت آپدیت را نمایش خواهد داد.



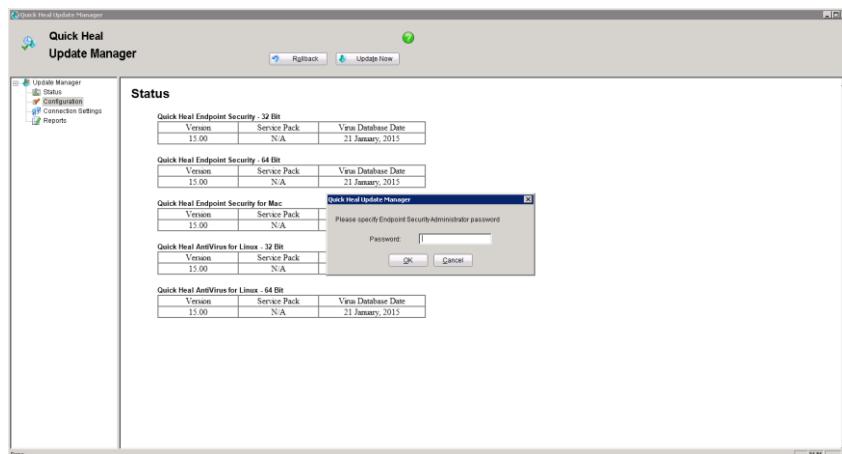
اگر سرور به اینترنت دسترسی نداشته باشد، پنجره فوق نمایش داده می‌شود. ابتدا سرور را به اینترنت متصل کرده و بر روی دکمه **Retry** کلیک کنید. برای رجیستر کردن، سیستم باید به اینترنت متصل باشد. (مراکز حساس که امکان اتصال به اینترنت را ندارند، با نماینده کوئیک هیل در ایران تماس بگیرند)



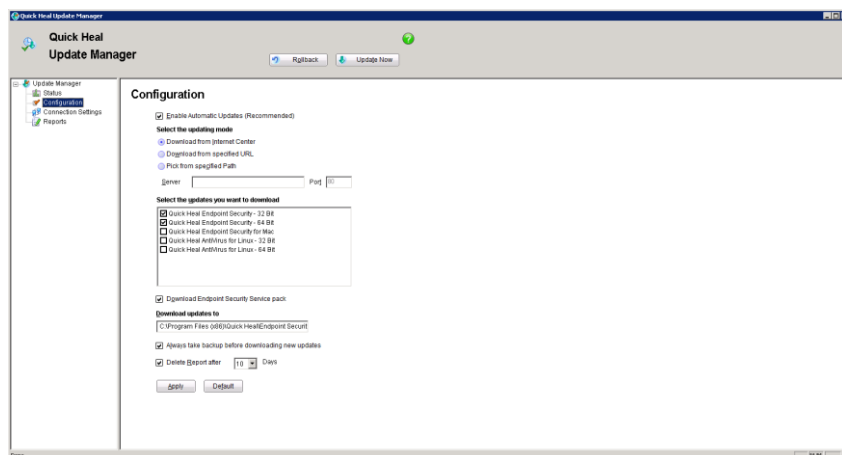
لایسنس یا کلید محصول خود را وارد نمایید. اگر برای اولین بار نصب انجام می‌گیرد پس از وارد کردن لایسنس، در صفحات بعدی اطلاعات زیر را تکمیل کنید:

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.

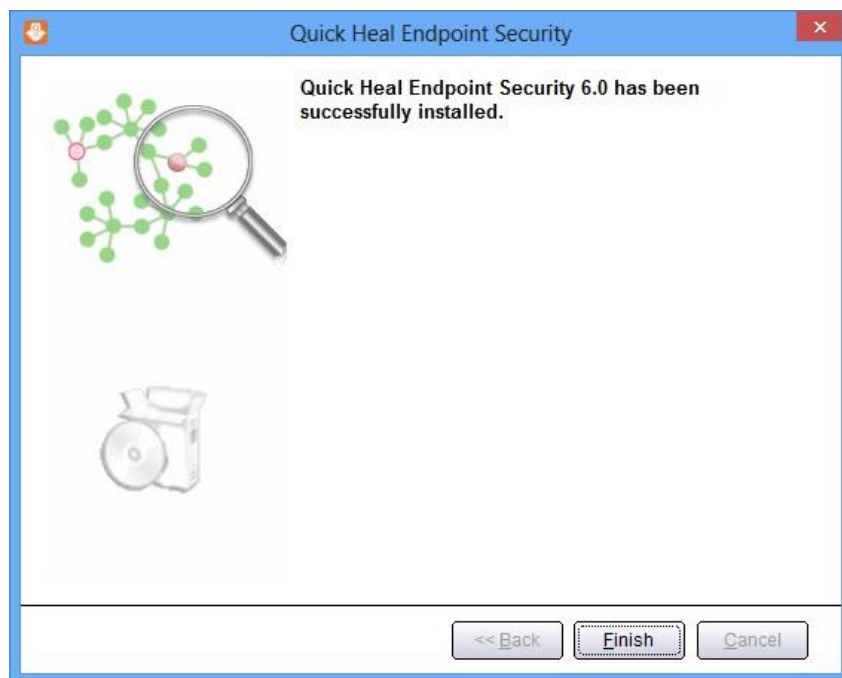


این قسمت مربوط به تنظیمات نرم افزار Update Manager می‌باشد که جهت ورود به تنظیمات می‌بایست رمز عبور نرم افزار اندپوینت وارد شود.



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 کلاینت های موجود در شبکه خود می توانید هر کدام از گزینه ها را انتخاب نمایید.
- انتخاب مسیر ذخیره فایل های آپدیت
- بکاپ گرفتن از آپدیت های قبلی، قبل از گرفتن آپدیت جدید
- حذف گزارش دریافت Update بعد از تعداد روز انتخاب شده
- تغییر کلمه رمز عبور

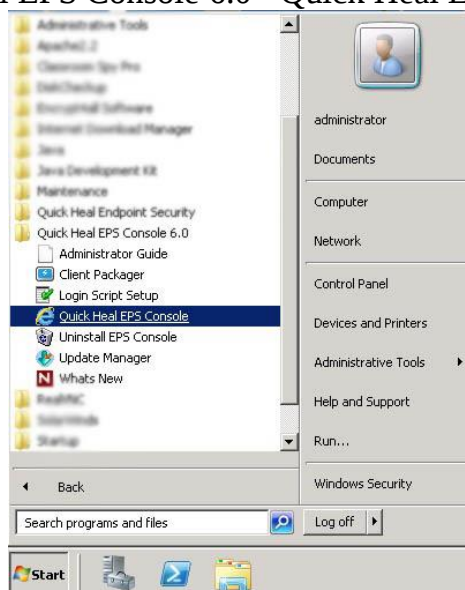


این صفحه نشان می دهد که نصب و فعالسازی با موفقیت به پایان رسید.

آغاز به کار کنسول مدیریتی متمرکز اندپوینت سکیوریتی کوئیک هیل

۱. اجرای کنسول کوئیک هیل اندپوینت سکیوریتی 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.

Quick Heal®
Endpoint Security 6.0

Account Login

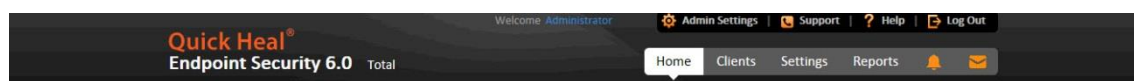
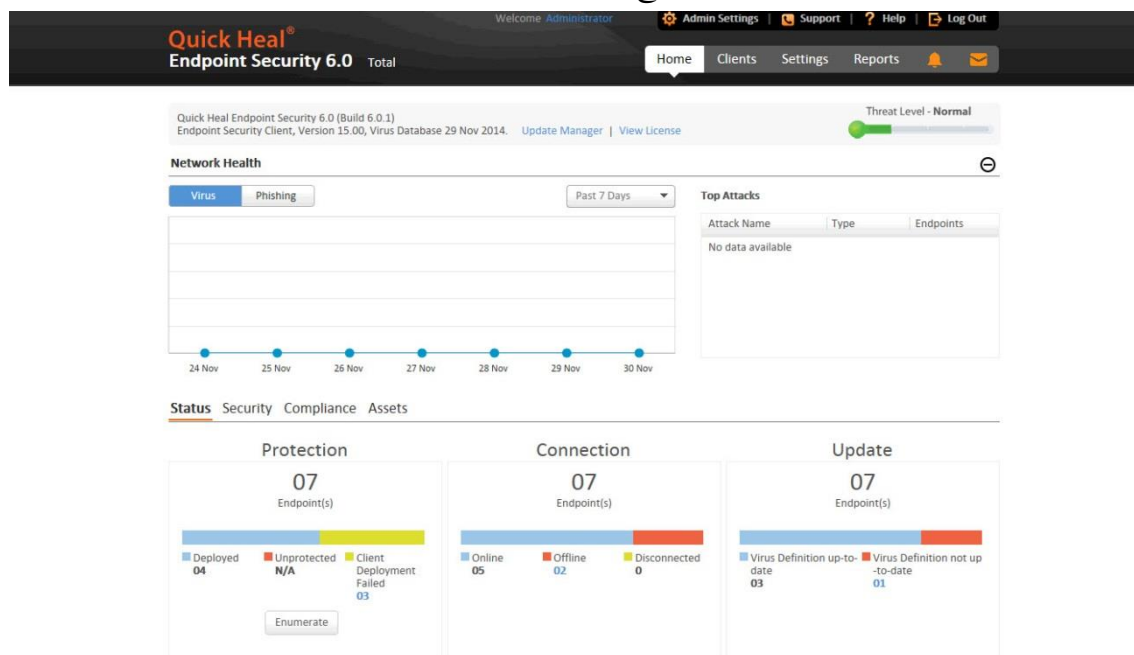
User name

Password

Login

داشبورد مدیریتی

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



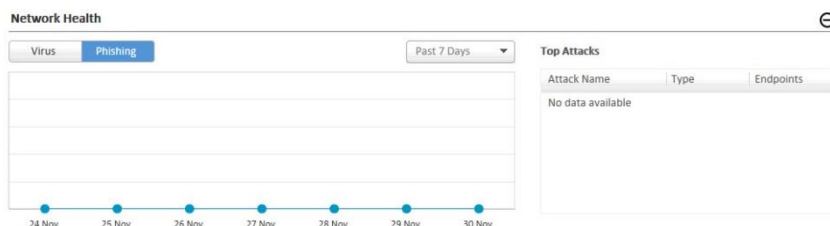
در نوار طوسی رنگ، نام و نسخه محصول به همراه تاریخ بروزرسانی نمایش داده می شود. با کلیک بر روی Update Manager می توانید وضعیت بروزرسانی اندپوینت را مشاهده و یا تنظیمات دلخواه را اعمال نمایید. اطلاعات مربوط به لایسنس از طریق لینک View License در دسترس می باشد. سطح تهدید در شبکه با نمودار رنگی (سبز=عادی،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

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 باز شو View form می‌توانید نمایش را از هفته اخیر (Last Week) به حالت ۲۴ ساعت گذشته، ۱۵ روز اخیر و ۳۰ روز اخیر تغییر دهید. با کلیک بر روی هر یک از گره‌ها 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 امنیتی 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 کوپیک‌هیل 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 کوپیک‌هیل اندپوینت سکیوریتی به صورت نمودار و جامع نمایش داده می‌شود. در سربرگ اول (Status) نمای کلی از وضعیت اندپوینت سکیوریتی 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 کوپیک‌هیل

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

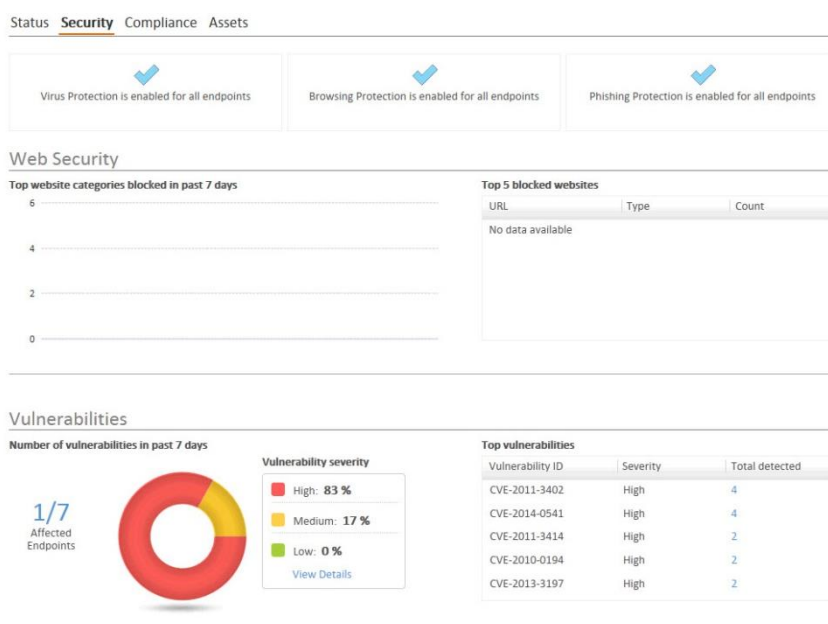
ب) Connection: در این بخش وضعیت کلاینت نشان داده می‌شود. تعداد کل کلاینت‌هایی که کوئیک‌هیل بر روی آنها نصب شده است (Endpoints)، تعداد کلاینت‌هایی که هم اکنون روشن و آنلاین بوده و ارتباط با سرور دارند (Online)، تعداد کلاینت‌هایی که هم اکنون آفلاین، خاموش و یا ارتباط شبکه‌ای با سرور ندارند (Offline)، تعداد کلاینت‌هایی که به علت آلودگی و تیک بودن گزینه مربوط به قطع اتصال شبکه‌ای 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 نشده‌اند (Virus Definition not up-to-date) در این بخش نمایش داده می‌شود.



۴. وضعیت امنیتی سازمان (Security)



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

الف) Security در این بخش می‌توانید اطلاعات کلی از نحوه برقراری امنیت و فعال بودن ماژول‌های امنیتی کلاینت‌های 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.



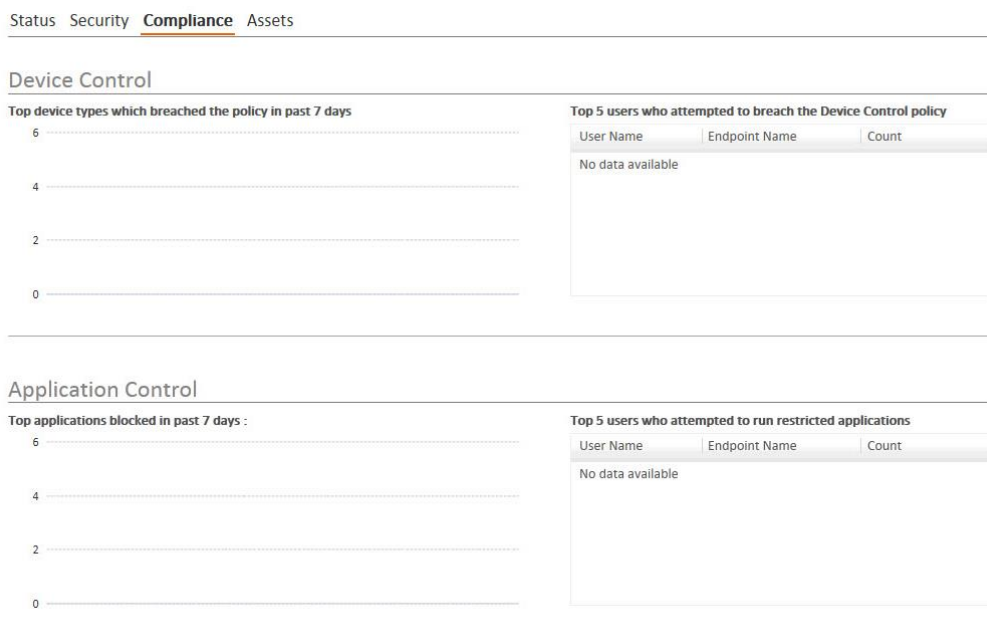
ب) Web Security در این بخش اطلاعات مربوط به امنیت وب نشان داده می‌شود. در این بخش می‌توانید اطلاعات مربوط به تعداد سایت‌های آلوده و نیز مسدود شده توسط مدیر که کاربران قصد مشاهده آنها را داشتند را مشاهده نمایید. در صورتی که مدیر، یک گروه از سایت‌ها و یا آدرس‌های اینترنتی خاصی را مسدود نماید، لیست پربازدیدترین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



ج) Vulnerabilities در این بخش بیشترین آسیب پذیری‌ها و حفره‌های نرم افزاری موجود در شبکه لیست می‌شود. با کلیک بر روی View details می‌توانید 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 دستگاه‌های حافظه‌های 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 دستگاه‌های مسدود شده‌ای 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.

Application Control

Top applications blocked in past 7 days :

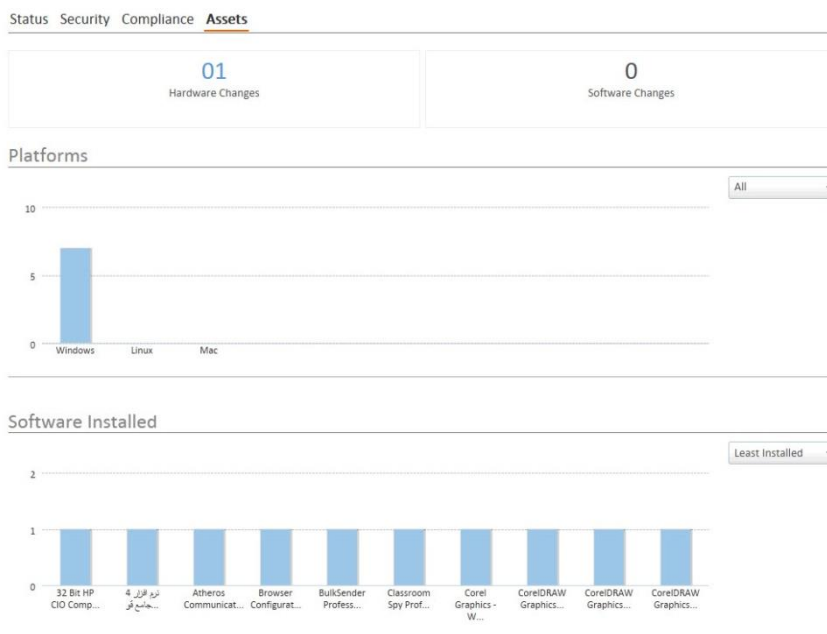


Top 5 users who attempted to run restricted applications

User Name	Endpoint Name	Count
No data available		

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:

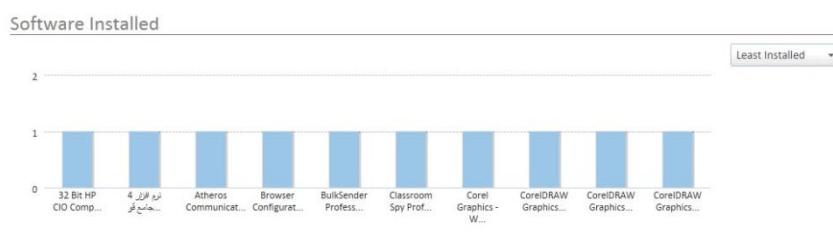


الف) Assets در آغاز این سربرگ، هرگونه تغییرات سخت‌افزاری (Hardware Changes) و نرم‌افزاری (Software Changes) صورت پذیرفته بر روی کلاینت‌ها لیست می‌شوند. با کلیک بر روی تعداد تغییر می‌توانید از اطلاعات کلاینت‌ها و تغییر صورت پذیرفته بر روی آنها مطلع گردید.



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.



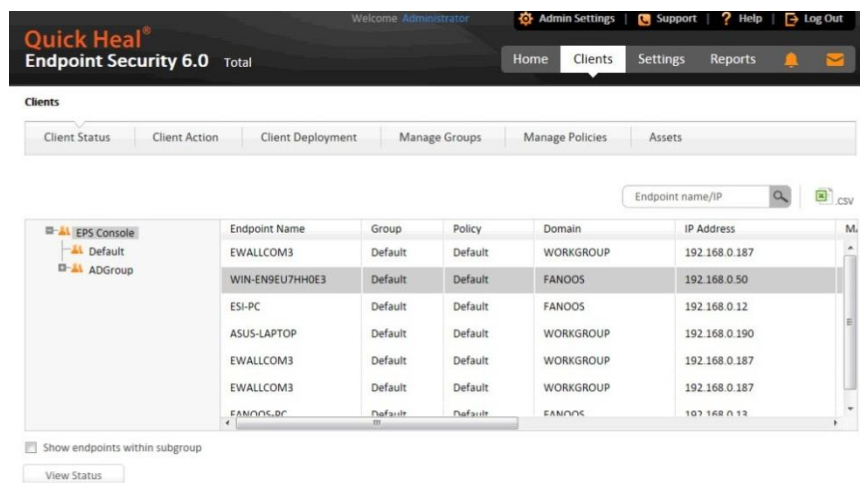
ج) Software Installed: در این بخش، لیست آخرین نرم‌افزارهای نصب شده بر روی کلاینت‌ها به همراه نمودار فراوانی مربوطه نمایش داده می‌شود.

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 می باشد. در بخش کلاینت، پیکربندی های آنتی ویروس کلاینت ها قابل اعمال می باشد.

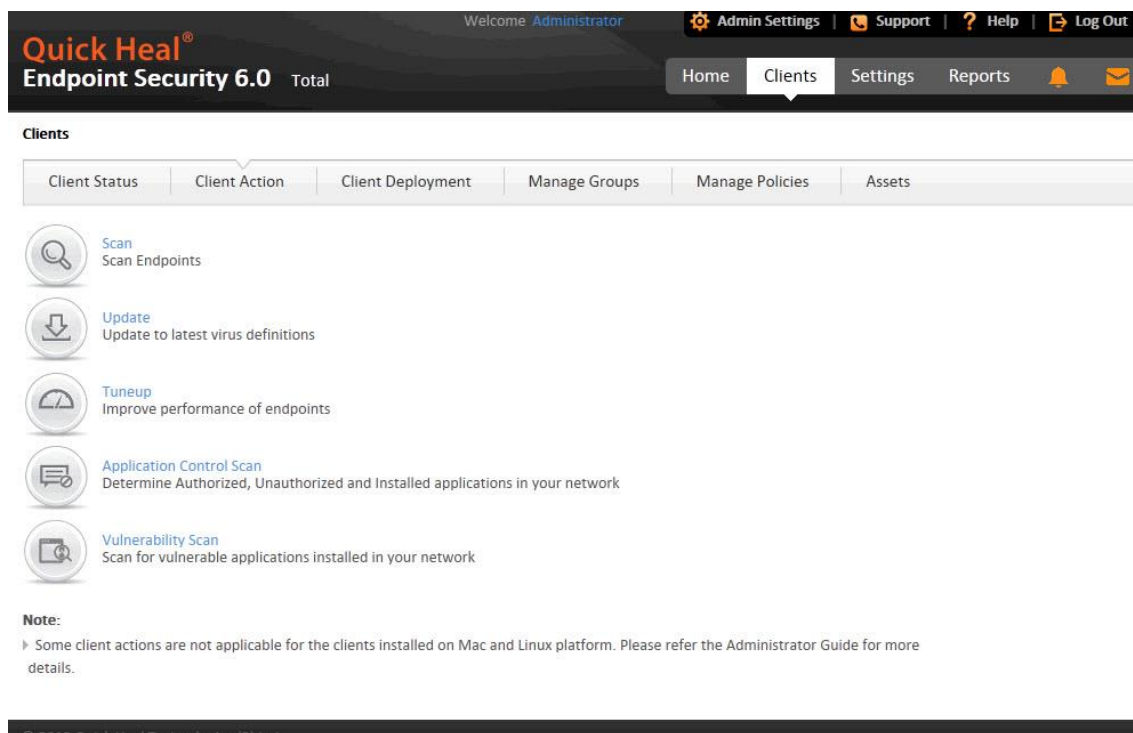
الف) Client Status



این سربرگ وضعیت کلاینت ها را نشان می دهد. در این صفحه می توانید کلاینت همه گروه ها و گروه های خاص را مشاهده نمایید. با کلیک بر روی نام گروه در درختواره سمت چپ می توانید اطلاعات کامپیوترهای موجود در آن گروه را ببینید. گروه پیش فرض Default می باشد. 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 ایجننت (Product Version)، تاریخ بروزرسانی (Virus Database Date) و تاریخ آخرین اسکن (Last Scan Date) در این بخش ارائه می شود. با کلیک بر روی عنوان هر گزینه براساس آن پارامتر مرتب سازی انجام می گیرد. با انتخاب یک کلاینت و کلیک بر روی دکمه View Status، اطلاعات کاملی از کلاینت مربوطه ارائه می گردد. با تیک کردن گزینه Show computers within subgroup همه ی کلاینت های عضو زیرگروه انتخابی لیست می گردند.

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.

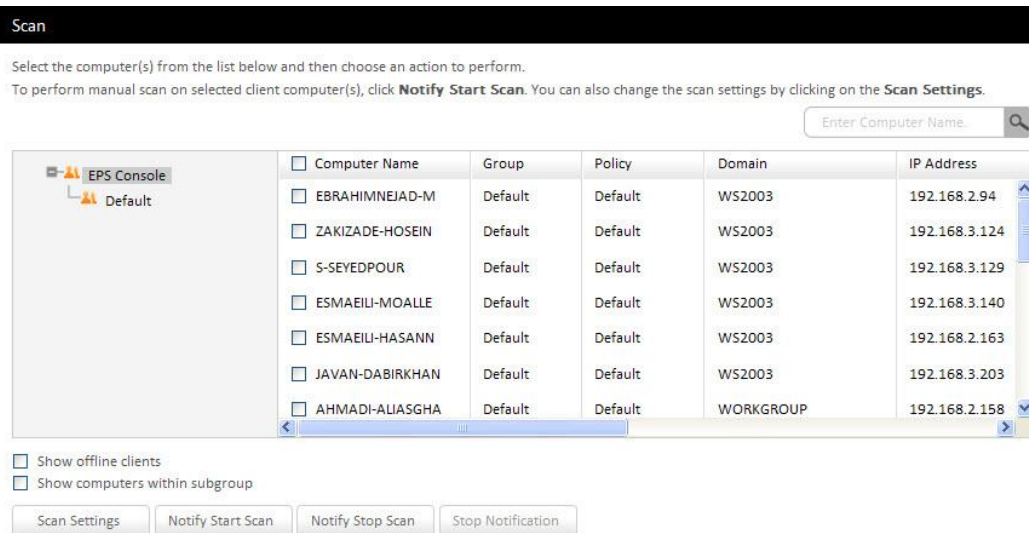
پوشش و تولید گزارش از برنامه‌های نصب شده بر روی یک کلاینت و اعمال محدودیت اجرا در صورت اعمال سیاست‌گذاری از راه دور ممکن می‌باشد.

پس از نصب کوئیک‌هیل بر روی 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 دکمه **Notification** کلیک کنید تا ارسال دستور، متوقف گردد.

Update

Update

Select the computer(s) from the list below and then choose an action to perform.
To update Quick Heal on selected clients click **Notify Update Now**.

☐	Computer Name	Group	Policy	Domain	IP Address
☐	EBRAHIMNEJAD-M	Default	Default	WS2003	192.168.2.94
☐	ZAKIZADE-HOSEIN	Default	Default	WS2003	192.168.3.124
☐	S-SEYEDPOUR	Default	Default	WS2003	192.168.3.129
☐	ESMAEILI-MOALLE	Default	Default	WS2003	192.168.3.140
☐	ESMAEILI-HASANN	Default	Default	WS2003	192.168.2.163
☐	JAVAN-DABIRKHAN	Default	Default	WS2003	192.168.3.203
☐	AHMADI-ALIASHGA	Default	Default	WORKGROUP	192.168.2.158

☐ Select computers with out-of-date Quick Heal
☐ Show computers within subgroup

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.

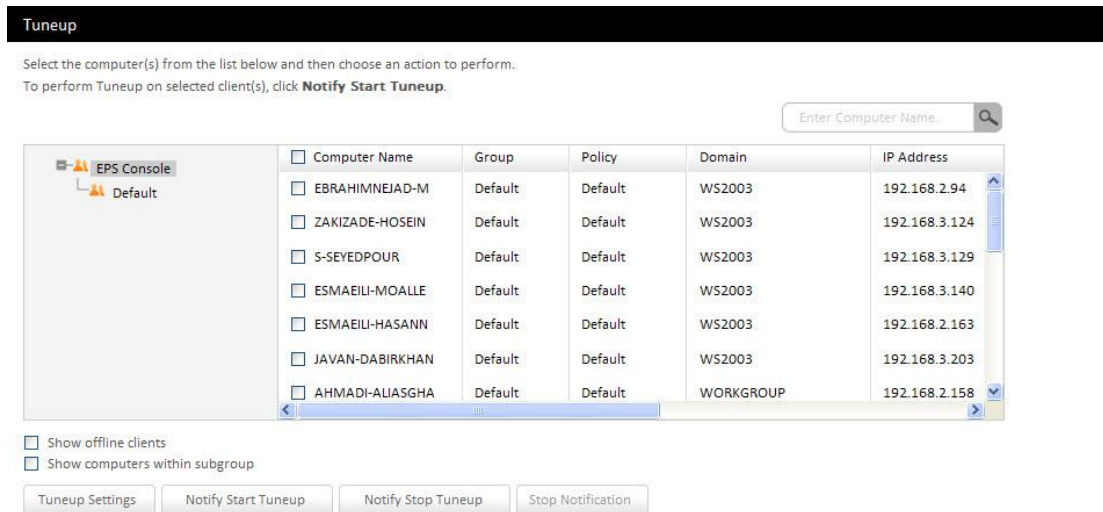
Notify Update Now: با انتخاب کلاینت‌هایی که مایلید بروز گردند، و کلیک بر روی این دکمه،

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 بر روی 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 می‌توانید اقدام به اسکن اپلیکیشن و برنامه‌های نصب شده بر روی کلاینت یا کلاینت‌های مورد نظر نموده و گزارش آن را در بخش **Report** مشاهده فرمایید.

Application Control Scan

Select the computer(s) from the list below and then choose an action to perform.
To perform Application Control Scan on selected client(s), click **Notify Start Scan**.

Enter Computer Name.

☐	Computer Name	Group	Policy	Domain	IP Address
☐	EBRAHIMNEJAD-M	Default	Default	WS2003	192.168.2.94
☐	ZAKIZADE-HOSEIN	Default	Default	WS2003	192.168.3.124
☐	S-SEYEDPOUR	Default	Default	WS2003	192.168.3.129
☐	ESMAEILI-MOALLE	Default	Default	WS2003	192.168.3.140
☐	ESMAEILI-HASANN	Default	Default	WS2003	192.168.2.163
☐	JAVAN-DABIRKHAN	Default	Default	WS2003	192.168.3.203
☐	AHMADI-ALIASHGHA	Default	Default	WORKGROUP	192.168.2.158

☐ Show offline clients
☐ Show computers within subgroup

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

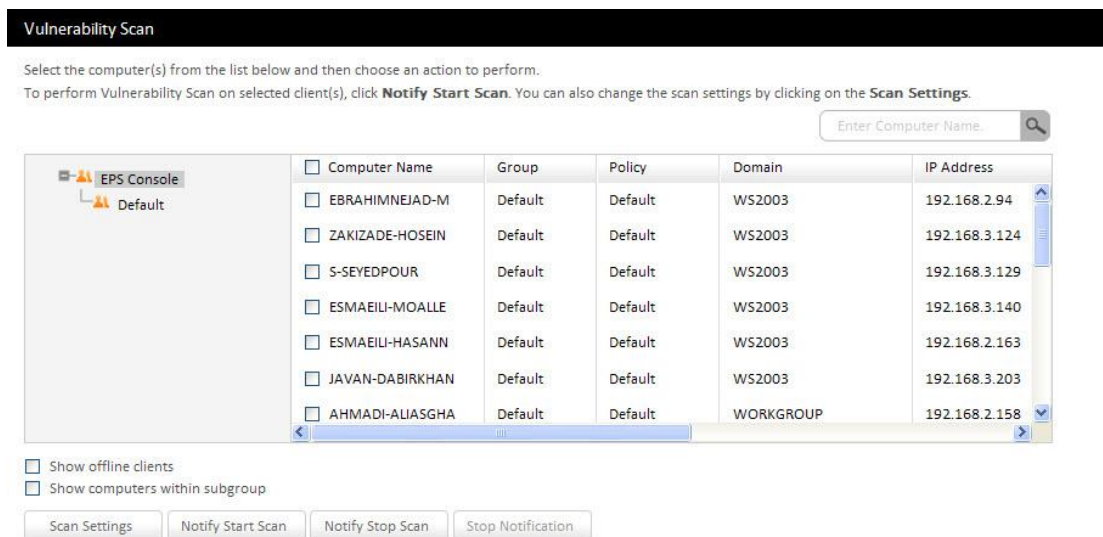
Notify Start Scan: ارسال دستور شروع به کار اسکن برنامه‌ها به کلاینت/کلاینت‌های انتخابی.

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

Stop Notification: توقف فرایند ارسال دستور به کلاینت.

Vulnerability Scan

گزارش کاملی از آسیب‌پذیری‌های سیستم عامل میکروسافت ویندوز و برنامه‌های نصب شده بر روی کلاینت از شرکت‌های مختلف نرم‌افزاری جهان مانند Oracle، Mozilla، Apple، Adobe ارائه می‌دهد. با این ویژگی می‌توانید به راحتی وضعیت امنیتی رایانه‌های شبکه خود را بررسی و وصله‌های مورد نیاز را دریافت نمایید.

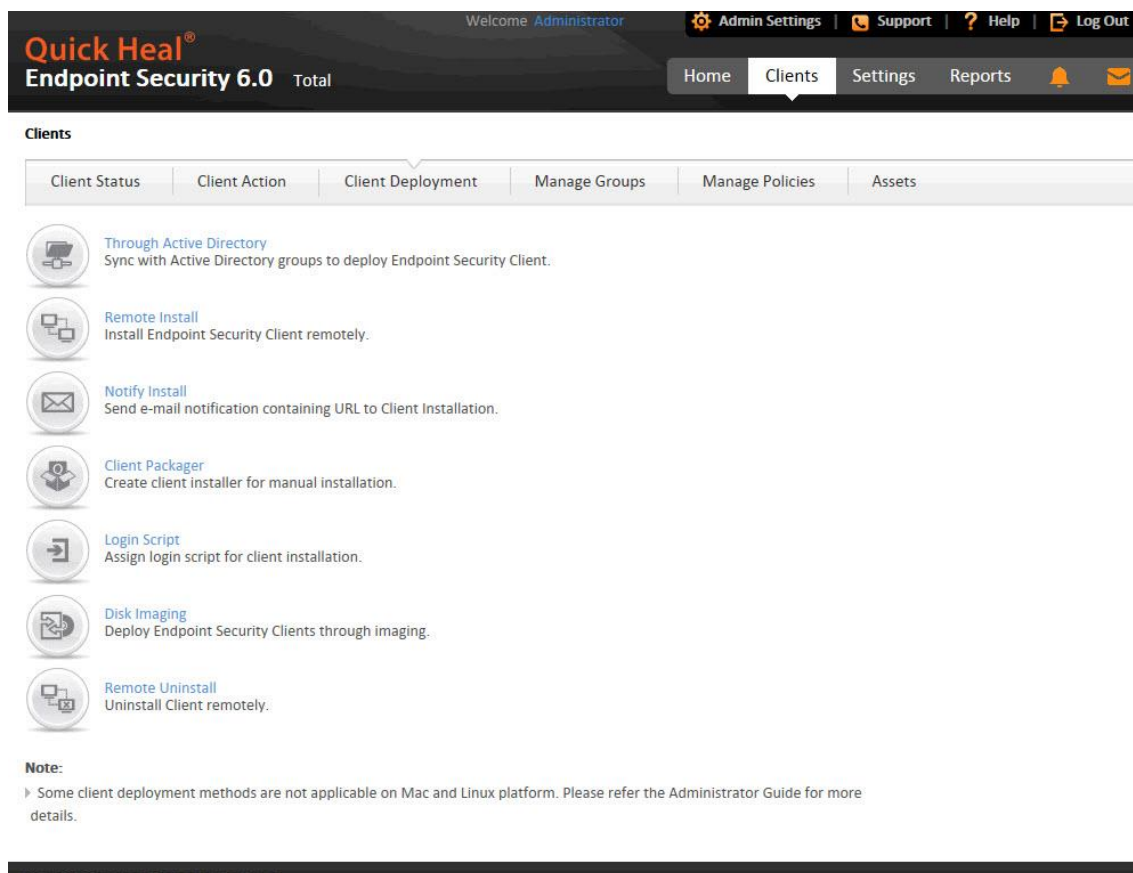


با کلیک بر روی **Scan Settings** می‌توانید تعیین کنید که آسیب‌پذیری‌های میکروسافت و شرکت‌های دیگر یا فقط آسیب‌پذیری‌های میکروسافت و یا تنها آسیب‌پذیری‌های شرکت‌های دیگر مورد بررسی و کاوش قرار گیرند.

- ✓ با انتخاب کلاینت مورد نظر و کلیک بر روی دکمه **Notify Start Scan** دستور اجرای اسکن آسیب‌پذیری و تهیه گزارش ارسال می‌گردد.
- ✓ برای ارسال دستور توقف فرایند اسکن آسیب‌پذیری 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.



اندپوینت سکیوریتی کوپیک هیل از ۶ روش نصب و یک روش حذف پشتیبانی می‌کند. متناسب با پیکربندی شبکه و مطابق سلیقه خود می‌توانید یکی از این ۶ روش نصب را استفاده می‌کنیم.

۱. **Through Active Directory**: با استفاده از این ویژگی می‌توانید نصب Client Agent

کوپیک هیل 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 ۳۹ راهنمای اندپوینت سکیوریتی ۶،۴ موجود است.

۲. **Remote Install**: امکان نصب کلاینت ایجنت کوپیک هیل از راه دور در این قسمت پیش بینی

شده است. راهنمای کامل‌تر در صفحه‌ی ۴۲ نمای اندپوینت سکیوریتی ۶،۴ موجود است.

۳. **Notify Install**: در صورت تمایل می‌توانید با استفاده از این روش یک ایمیل اطلاع رسانی جهت

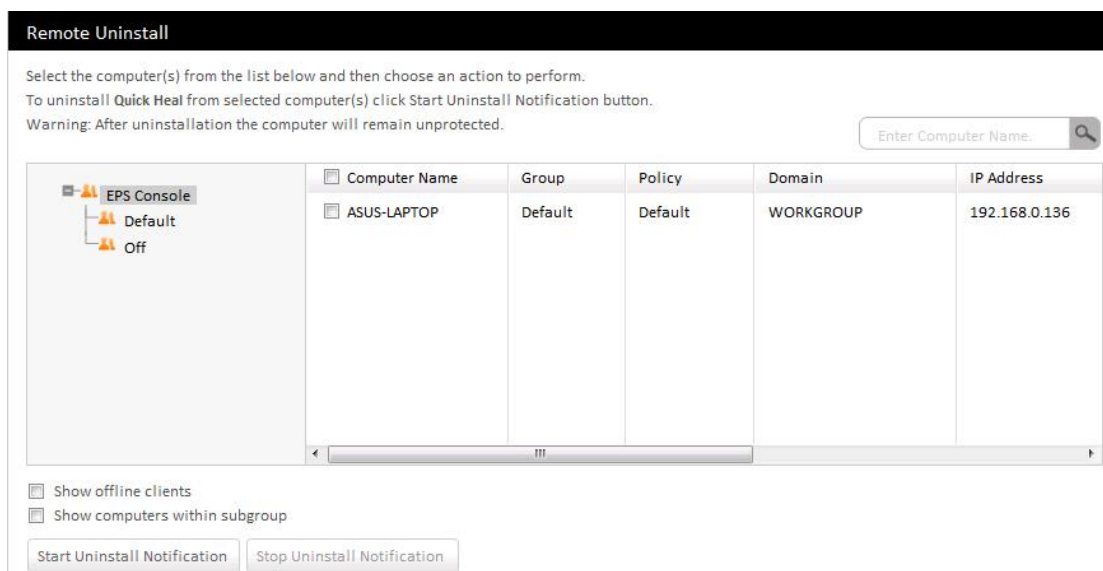
نصب کوپیک هیل به کاربران شبکه ارسال نمایید. این ایمیل شامل لینک نصب کوپیک هیل می‌باشد. در ضمن می‌توانید این لینک (<https://SERVER-IP:9099/qhscan6/install.htm>) را از طریق IE بر روی هر کلاینت بدون ارسال ایمیل، اجرا نموده و اقدام به نصب از راه دور کوپیک هیل نمایید.

۴. **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.

۵. **Login Script**: این روش تنها در شبکه‌های مبتنی بر دامنه قابل اجرا می‌باشد. در این روش یک فایل **QHEPS.BAT** ساخته می‌شود. کوپیک هیل به محض لاگین شدن کلاینت‌ها به سرور دامنه نصب می‌گردد. توضیحات بیشتر در صفحه ۴۱ راهنما.

۶. **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 برنامه‌های 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 ایمج نمایید. از این پس به محض نصب ایمج، کوپیک هیل هم به صورت خودکار نصب و اکتیو می‌گردد.

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



Start Uninstall 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.

Endpoint name/IP

Import Export .csv

Endpoint Name	Group	Policy	Domain	IP Address
EWALLCOM3	Default	Default	WORKGROUP	192.168.0.187
WIN-EN9EU7HH0E3	Default	Default	FANOOS	192.168.0.50
ESI-PC	Default	Default	FANOOS	192.168.0.12
ASUS-LAPTOP	Default	Default	WORKGROUP	192.168.0.190
EWALLCOM3	Default	Default	WORKGROUP	192.168.0.187
☒ EWALLCOM3	Default	Default	WORKGROUP	192.168.0.187
FANOOS-PC	Default	Default	FANOOS	192.168.0.13

☐ Show endpoints within subgroup

برای گروه بندی و اعمال سیاست گذاری مورد نظر بر روی هر گروه، از این سربرگ استفاده می‌شود. درختواره سمت چپ، گروه‌ها و زیرگروه‌ها 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 بر روی 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 بر روی نام گروه، گزینه‌های 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.

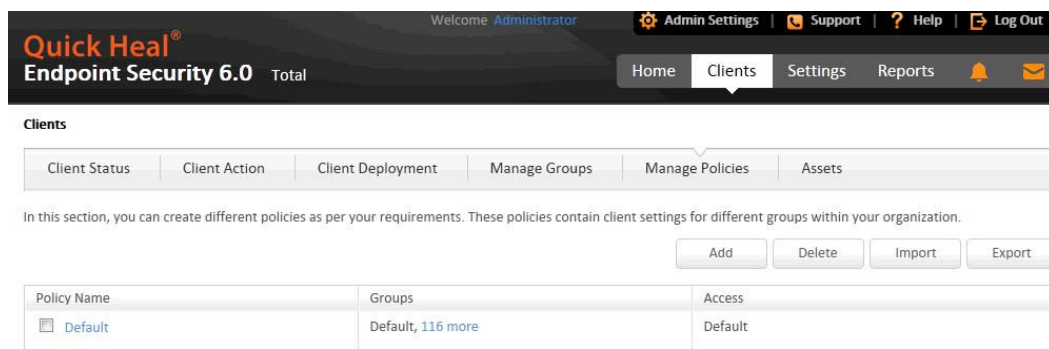
Import from Active Directory: در صورتی که می‌خواهید لیست کلاینت‌ها را از اکتیودایرکتوری

وارد نمایید، از این گزینه استفاده می‌کنید.

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

ه) سربرگ Manage Policy

این بخش مدیریت سیاست گذاری کلاینت ها را برعهده دارد.



در این بخش تعاریف مربوط به سیاست گذاری آنتی ویروس کلاینت ها صورت می پذیرد. همه تنظیمات آنتی ویروس کوئیک هیل کلاینت های شبکه در این بخش قابل تعریف می باشد. با کلیک بر روی اسم هر پالیسی می توانید آن را ویرایش نمایید.

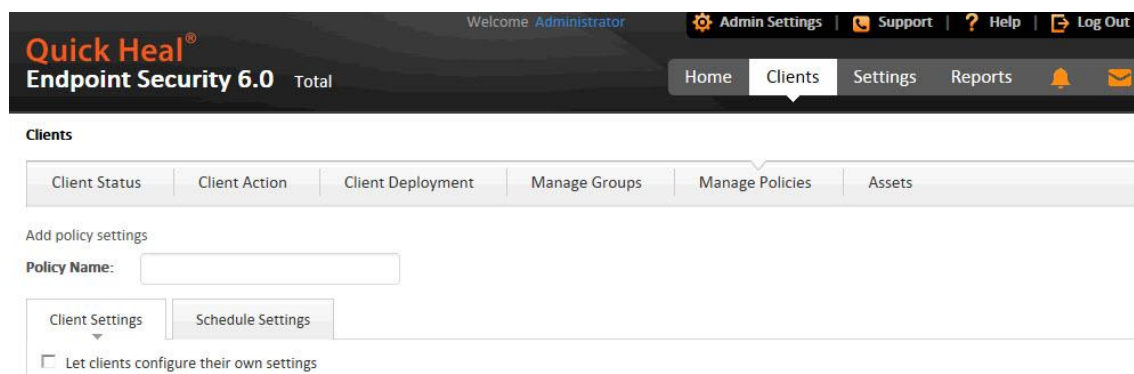
Add: افزودن سیاست گذاری.

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 می خواهید ایجاد نمایید را وارد نمایید.

این صفحه دارای دو سربرگ **Client Settings** (تنظیمات کلاینت) و **Schedule Settings**

(تنظیمات زمانبندی) می باشد.

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 بخش‌های 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** می باشد که بیانگر این مطلب است که هنگام یافتن یک ویروس، آن را تعمیر کند. گزینه های دیگر می تواند حذف (**Delete**)، صرف نظر (**Skip**) باشد.

Virus Protection Settings

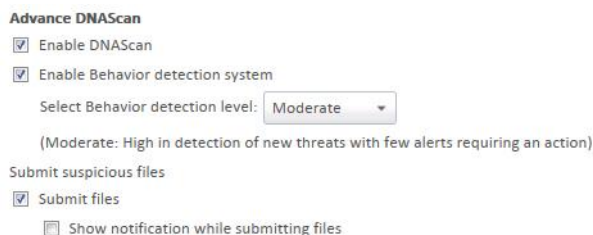


Load Virus Protection at Startup: اگر این گزینه تیک باشد، در هنگام راه اندازی به صورت خودکار آنتی ویروس در سیستم کلاینت بارگذاری و اجرا می گردد.

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

Select action to be performed when a virus is found: در صورت پیدا شدن ویروس توسط محافظت بلادرنگ کوئیک هیل، آنرا تعمیر (**Repair**)، حذف (**Delete**) و یا از آن صرف نظر (**Skip**) می کند.

Advance DNAScan



در این بخش تنظیمات مربوط به اسکن پیشرفته مبتنی بر نقشه ژنوم انسانی (**DNAScan**) که وظیفه اسکن ویروس های ناشناخته را دارد، قابل پیکربندی می باشد. در واقع کوئیک هیل مجهز به لابراتوار مجازی بر روی همه کلاینت های خود بوده که مانند یک سرور سنسور عمل می کند.

Enable DNAScan: با تیک بودن این گزینه دی.ان.ای اسکن کوئیک هیل فعال می گردد.

Enable Behavior detection system: علاوه بر **DNAScan** کوئیک هیل، مجهز به هوش مصنوعی سیستم شناسایی بدافزار بر اساس رفتار (رفتارشناسی) می باشد که مانع حمله ویروس های جدید به سیستم می گردد. با تیک بودن این گزینه این سیستم فعال می گردد.

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

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

Show notification while submitting files: اگر این گزینه تیک باشد، در هنگام ارسال

فایل‌های مشکوک، پیغام به کاربر نشان داده می‌شود.

Block Suspicious Packed Files

☒ Block Suspicious Packed Files

Automatic Rogueware Scan Settings

☒ Enable Automatic Rogueware scan

Disconnect Infected Clients from the network

☐ When non-repairable virus found

☐ When suspicious file found by DNAScan

Exclude File and Folders

List of files and folders to be excluded from scanning

Path	Include Subfolder	Excluded For

Add

Delete

Block Suspicious Packed Files: تک بودن این گزینه موجب می‌شود که فایل‌های 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 می گردند.

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

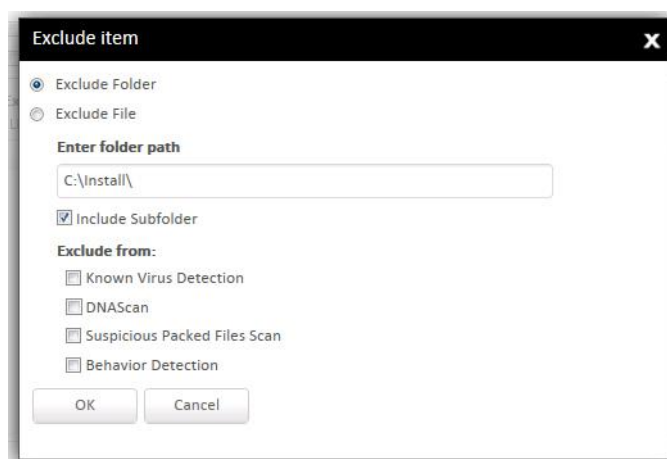
توسط DNAScan کوئیک هیل پیدا شود، ارتباط کلاینت مشکوک از شبکه قطع می گردد.

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، می توانید فایل یا پوشه را از ویروسیابی شدن استثناء نمایید. پس از افزودن (Add کردن) آن فولدر یا فایل و افزوده شدن در لیست مربوطه، کلاint های عضو آن پالسی، فایل یا فولدر موردنظر را اسکن نمی کنند.

پس از کلیک بر روی دکمه Add پنجره ای نمایش داده می شود که می توانید تنظیمات مربوط به استثناء

شدن را در آن درج نمایید.



اگر می‌خواهید پوشه‌ای 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 زیرپوشه‌هایی باشد، تیک بودن این گزینه، آن زیرپوشه‌ها را نیز از اسکن مستثنی می‌کند.

Exclude from: در این بخش موارد استثناء مشخص می‌گردد.

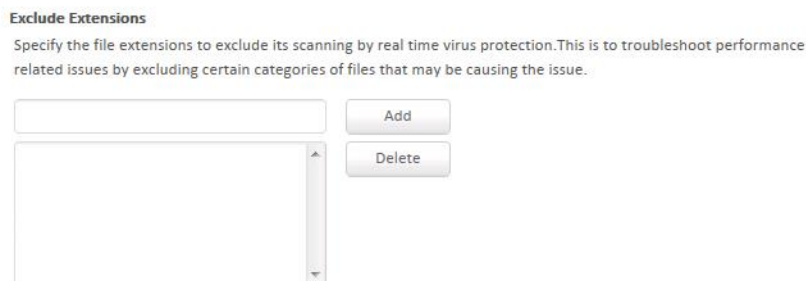
Known Virus Detection: با تیک بودن این گزینه، همه ویروس‌های شناخته شده، از اسکن استثناء می‌گردند.

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

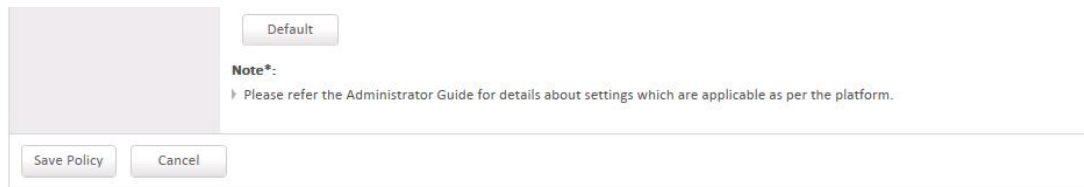
Suspicious Packed Files Scan: استثناء شدن از اسکن فایل‌های بسته‌ای مشکوک.

Behavior Detection: استثناء شدن از انجین رفتارشناسی کوپیک هیل.

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 پیام 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 هرزنانه 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 ایمیل‌ها را می‌توانید تعیین نمایید که

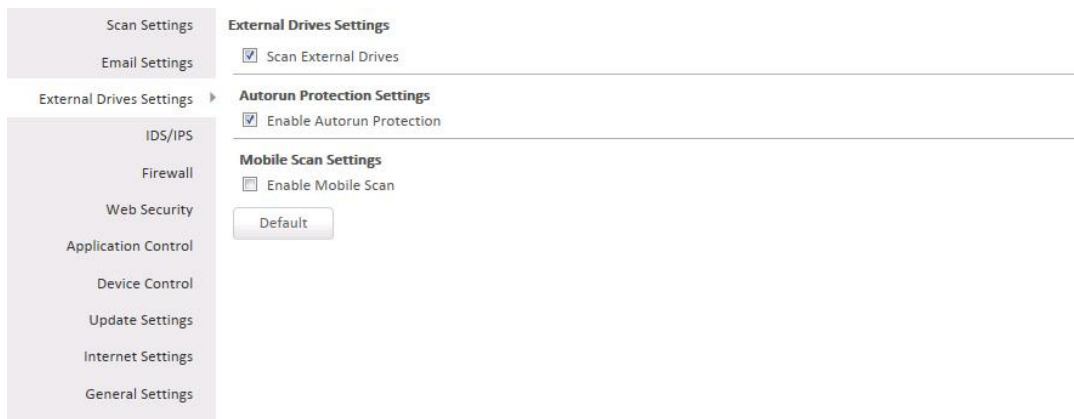
از آنتی اسپم مستثنی شده و همواره به عنوان ایمیل سالم وارد کلاینت کاربر گردد.

Enable black list: با تیک کردن این گزینه لیست سیاهی از ایمیل‌ها را می‌توانید تعیین نمایید که

آنتی اسپم همواره آنها را به عنوان ایمیل مخرب و هرزنانه در نظر می‌گیرد.

External Drives Settings

این بخش شامل تنظیمات مربوط به اسکن دستگاه های خارجی می باشد.



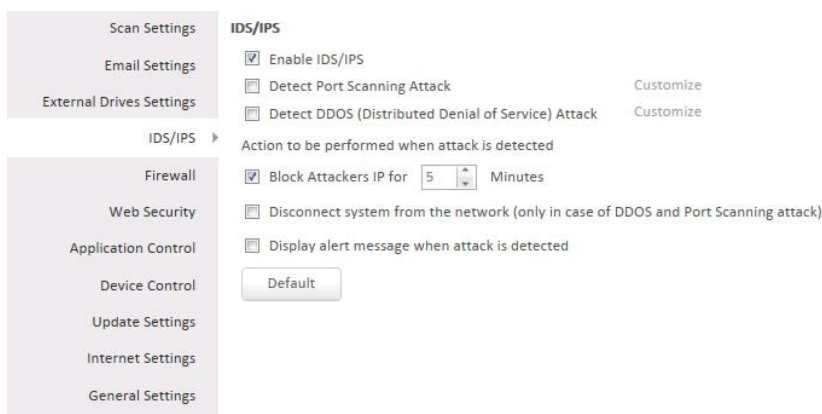
Scan External Drives: در صورتی که این گزینه تیک باشد، به محض اتصال فلش یا حافظه های USB، کوپیک هیل به صورت خودکار اقدام به اسکن آنها می کند.

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

Enable Mobile Scan: در صورت تیک بودن این گزینه، ویژگی اسکن موبایل PC2Mobile به کلاینت های عضو گروه مرتبط با این پالیسی فعال می گردد. این ویژگی انحصاری کمک می کند تا کوپیک هیل 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 کوپیک هیل 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 آدرس‌های IP و پورت‌های 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 آدرس‌های 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 کوپیک هیل 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.

Firewall

☒ Enable Firewall

Level

- ☐ Block all (Block all Inbound & Outbound traffic)
- ☐ High (Block all Inbound & Outbound traffic excluding exception)
- ☐ Medium (Block all Inbound & allow all Outbound traffic excluding exception)
- ☒ Low (Allow all Inbound & Outbound traffic excluding exception)

☐ Display alert message when firewall violation occurs

☐ Enable firewall reports

Enabling this option will generate reports for all blocked connections. If the firewall policy is set as 'Block All' or 'High' then firewall will block all connections and will generate many reports. In this case you may observe increase in network traffic.

Exceptions

Exception Name	Protocol	Direction	Action
☒ Allow File Sharing over UDP - Inbound	UDP	Inbound	Allow
☒ Allow File Sharing over UDP - Outbound	UDP	Outbound	Allow
☒ Allow File Sharing over TCP - Inbound	TCP	Inbound	Allow
☒ Allow File Sharing over TCP - Outbound	TCP	Outbound	Allow
☒ Allow access to file shares TCP - Inbound	TCP	Inbound	Allow
☒ Allow access to file shares TCP - Outbound	TCP	Outbound	Allow

Buttons: Add, Delete, Import, Export, Move Up, Move Down

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 استثناءها را مجاز می‌کند.

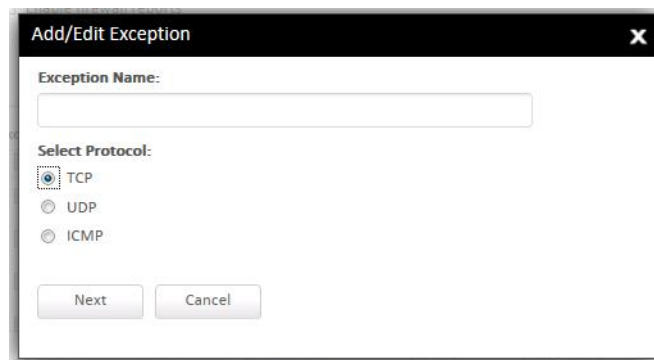
Display alert message when firewall violation occurs: اگر این گزینه فعال باشد، در هنگام حملات، فایروال پیغام خطر مناسب به کاربران نشان می‌دهد.

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

Exceptions: استثنای 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...

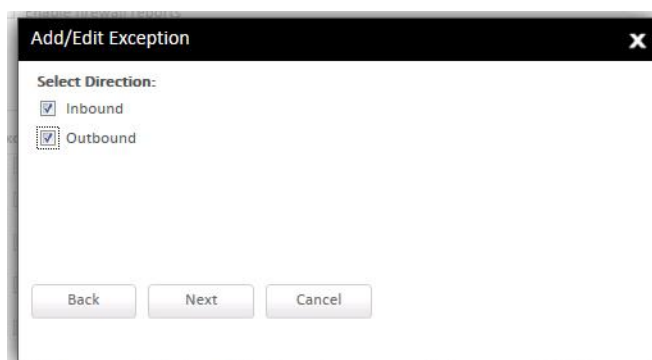
در جدول استثنای نام استثناء (Exception Name)، پروتکل (Protocol) که می‌تواند TCP/UDP/ICMP باشد، جهت (Direction) که می‌تواند ورودی (Inbound) یا خروجی (Outbound) باشد، اقدام مربوطه (Action) که می‌تواند مجاز (Allow) یا غیرمجاز (Deny) و وضعیت (Status) که می‌تواند فعال (On) یا خاموش (Off) باشد قابل مشاهده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

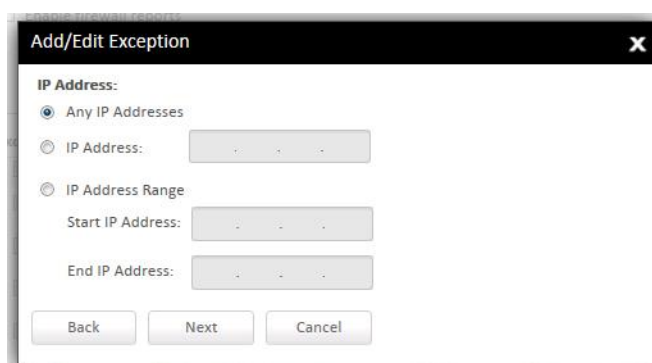


Exception Name: نام یا شرحی برای استثناء وارد نمایید.

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.

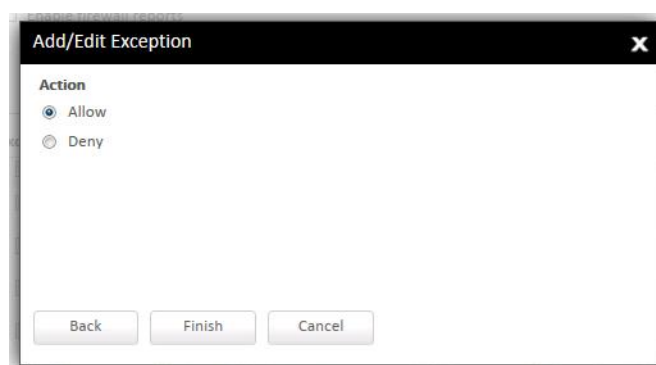


TCP/UDP Ports: در این بخش پورتهایی را که قانون فایروال باید بر روی آنها اعمال شود، مشخص نمایید.

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 ۴۴۳ 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 رول‌هایی 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 رول‌ها گرفته و آنها را بر روی کنسول‌های 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 سایت ها و مسدود یا مجاز کردن سایت های خاص در این بخش قرار دارند.

Web Security

☒ Browsing Protection

☒ Phishing Protection

To exclude URLs from browsing and phishing protection, Click on Exclusion Exclusion

☒ Display alert message when website is blocked

Web Categories

☐ Restrict access to particular categories of Websites

Category	Status
Advertisements and Pop-Ups	Allow
Alcohol and Tobacco	Deny
Anonymizers	Deny
Arts	Allow
Business	Allow
Computers and Technology	Allow
Chat	Allow

Block specified websites

☐ Restrict access to particular Websites

List of restricted Websites/URLs

URL	Block Subdomain

Add
Delete
Delete All

☒ Enable Web Security reports

Enabling this option will generate reports for all blocked websites. In this case you may observe large number of reports depending upon the web usage.

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

Phishing Protection: تیک بودن این گزینه موجب می گردد تا سایت های کلاهبردانه و فیشینگ مسدود شوند.

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

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

Web Categories

در این بخش دسته بندی سایت ها قابل مدیریت می باشد. می توانید دسته خاصی از وبسایت ها (مثلاً بازی) را برای کاربران مسدود نمایید. همچنین امکان مسدود کردن و باز کردن یک سایت خاص نیز مهیا می باشد.

Restrict access to particular categories of Websites

دسترسی به دسته بندی خاصی از وبسایت ها را محدود نمایید. نشان در ستون Status نشان دهنده مجاز بودن و نمایانگر غیرمجاز بودن آن دسته بندی است. با کلیک بر روی این دکمه می توانید وضعیت را به مجاز و غیرمجاز تغییر دهید.

Exclusion

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

Block specified websites

در این بخش می توانید سایت های موردنظرتان را - خارج از اینکه عضو کدام دسته قرار دارند - مسدود نمایید.

Restrict access to particular Websites

تعریف شده در این بخش مسدود می گردد. با فشردن دکمه **Add**، پنجره ای زیر برای وارد کردن آدرس سایت موردنظر جهت مسدود شدن نمایش داده می شود:

Enter URL

آدرس سایتی را که می خواهید از دسترسی کاربران خارج شود، در این بخش وارد

نمایید. (مثلاً yahoo.com)

Also Block Subdomains

در صورتی که می خواهید همه زیردامنه های یک سایت نیز از

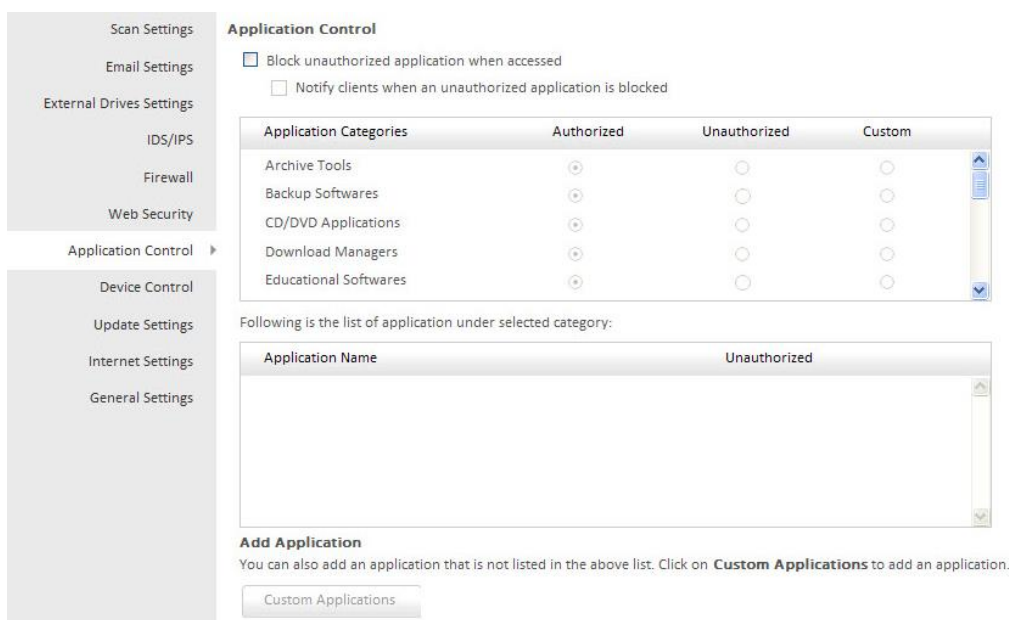
دسترس خارج شوند، این گزینه را تیک نمایید. (مثلاً mail.yahoo.com)

Enable Web Security reports

برای مشاهده سایت های مسدود شده دریافت نمایید، این گزینه را فعال کنید.

Application Control

یکی از ویژگی‌های کوپیک هیل اندپوینت سکیوریتی، کنترل برنامه‌ها (Application Control) می‌باشد. این ویژگی امکان مسدود کردن برنامه‌های کاربران را به صورت کامل فراهم می‌آورد. به عنوان مثال مدیر سیستم می‌تواند دسترسی به برنامه‌های دانلود اینترنتی (مانند IDM) یا بازی یا Babylon و یا برخی نرم افزارهای خاص سفارشی را مسدود نماید. یکی از ویژگی‌های این قابلیت، امکان تعریف فایل خاص می‌باشد. بدین معنی که اگر کاربران از نسخه‌های 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 کوپیک هیل ویژگی معرفی برنامه سفارشی (Custom Applications) را ارائه داده است که می‌توانید فایل .exe خود را به کوپیک هیل معرفی نمایید تا آن را از دسترس خارج نماید.



Block unauthorized application when accessed: برای فعال کردن قابلیت کنترل برنامه‌ها

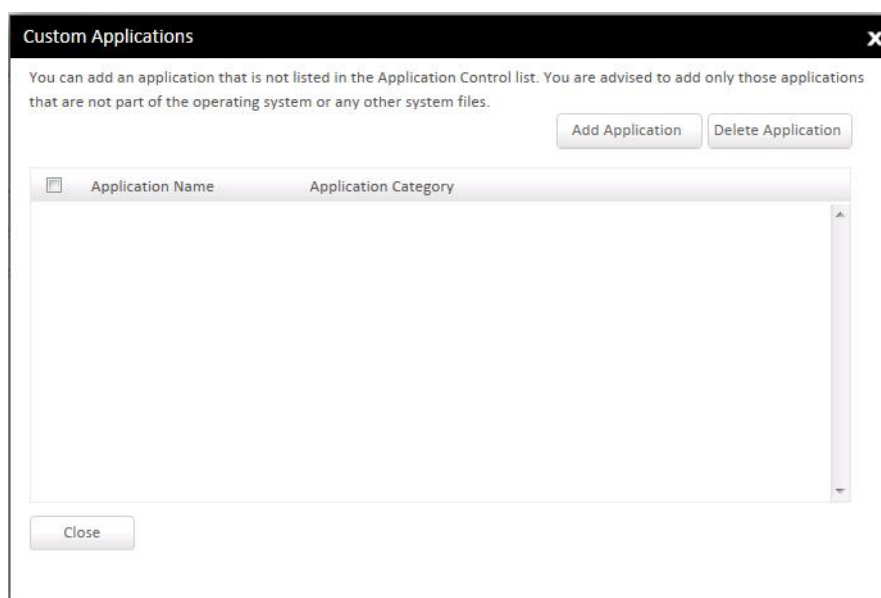
این گزینه باید تیک باشد. با فعال بودن این قابلیت، اجرای برنامه‌های غیرمجاز (unauthorized) برای کاربران ناممکن می‌گردد.

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 Unauthorized، Authorized 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 کوئیک‌هیل 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 کوئیک‌هیل ارسال نمایید. در فرم بالای این گزینه، علت افزودن برنامه را به کوئیک‌هیل توضیح می‌دهید. (این بخش قابل صرف نظر می‌باشد)

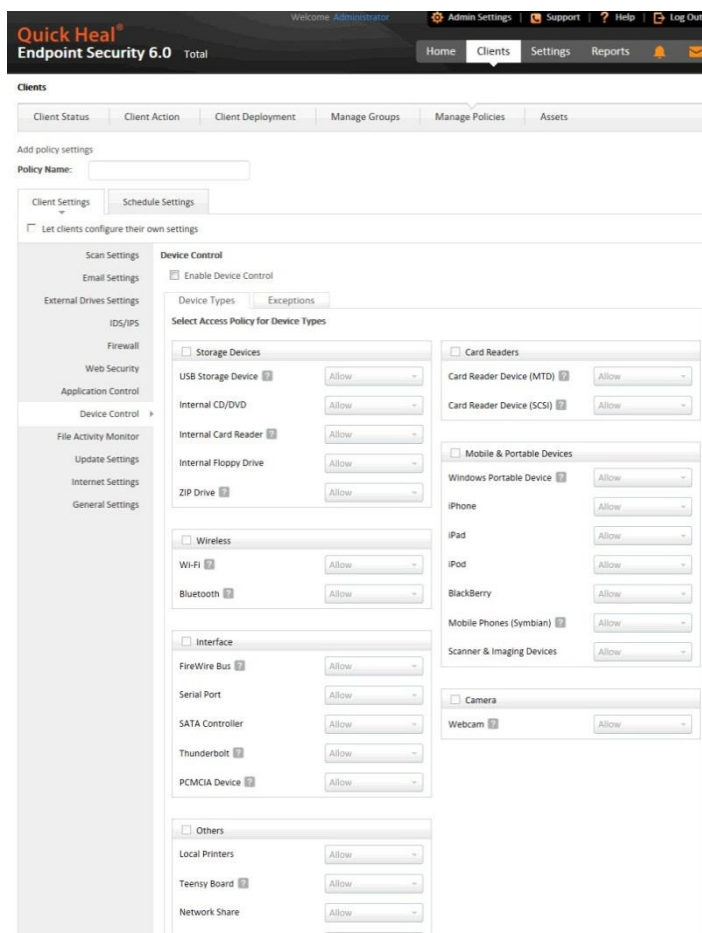
Add Application: برنامه را به لیست گروه با زدن این دکمه اضافه کنید. پس از تایید و خروج از افزودن برنامه کاربردی سفارشی، می‌توانید گروهی را که برنامه به آن اضافه شده (مثلاً **Others**)، غیرمجاز نمایید. همچنین می‌توانید آن گروه را در حالت **Custom** قرار داده و در باکس دومی فقط برنامه موردنظرتان را غیرمجاز کنید.

Device Control

در این بخش می‌توانید بیش از ۲۵ نوع مختلف از ابزارها و دستگاه‌های 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-Rom های داخلی (Internal CD/DVD)، کارت‌خوان‌های حافظه داخلی (Internal Card Reader)، دایره‌های فلاپی داخلی (Internal Floppy Drive) و دایره‌های 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)

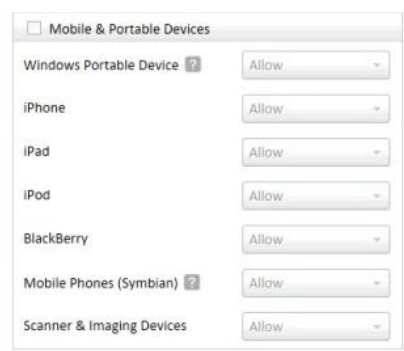
همه‌ی کلاینت‌ها یا گروهی از آنها در این بخش قابل مدیریت و کنترل می‌باشند. اگر می‌خواهید در صورت در دسترس بودن شبکه کابلی، وایرلس کلاینت را غیرفعال نمایید، گزینه Blocked if wired connection is available را در بخش Wi-Fi انتخاب نمایید. امکان مسدود کردن کامل (Block)، و یا مجاز کردن (Allow) نیز وجود دارد.



ب) Interface در این بخش انواع اینترفیس‌های کامپیوترها قابل مدیریت می‌باشد. اینترفیس‌ها شامل Serial، FireWire Bus، SATA Controller، Thunderbolt، PCMCIA Device و Port 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: دستگاه‌های جانبی دیگر مانند چاپگرهای محلی (Local Printers)، سیستم‌های میکروکنترلر مبتنی بر USB (Teensy Board)، اشتراک‌گذاری شبکه (Network Share) و حتی دستگاه‌های ناشناخته (Unknown Device) در این بخش قابل مدیریت می‌باشند.

گزینه‌های 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 دستگاه‌های 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، تمامی 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 دستگاه‌های معرفی شده، دستگاه جانبی خود را Add و سطح دسترسی موردنظر (Allow) را برای آن تعیین نمایید.

Device Control

☒ Enable Device Control

Device Types Exceptions

Exceptions in the Device Control policy

Add

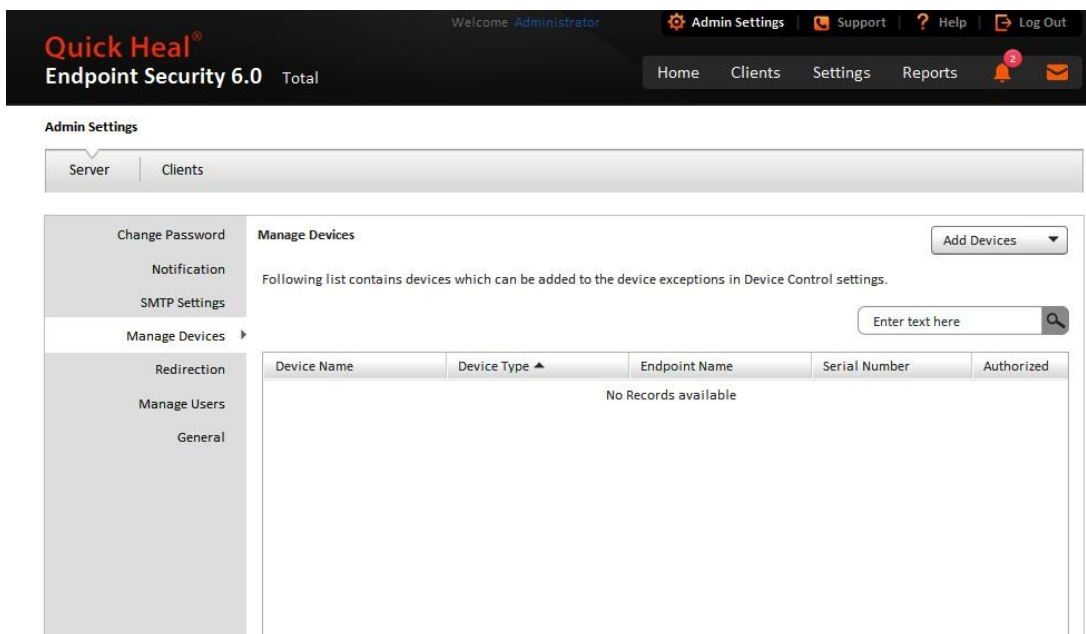
Device Name	Device Type ▲	Endpoint Name	Serial Number	Access
No Records available				

Note:

► Please refer the Administrator Guide for details about settings which are applicable as per the platform.

معرفی حافظه USB فلش به لیست Device Control

در این بخش می‌توانید دیوایس‌ها (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 اندپوینت سکیوریتی معرفی کنید.

Add Device

Serial Number:

Manufacturer:

Size: 4 GB

Device Name:

☐ Make this device accessible only within your corporate network.

Enabling this option will make this device inaccessible to all other system(s) that do not have Endpoint Security Client installed. This helps to prevent data loss as users cannot access the device on any other system outside your corporate network.

Note:

1. You can add only one device at a time. If you have multiple USB Devices connected to the system then remove all USB Devices and attach only one USB Device which you want to add.
2. If you are unable to add devices through the web console, you may also use the Device Control Tool to add devices. This tool is available at the location given below on the EPS server.
Path of Device Control Tool: <installation folder>\Admin\dcconfig.exe
3. In case if you are accessing the web console on Windows Vista, then please turn off 'Protected mode' option in Internet Explorer.

OK

Cancel

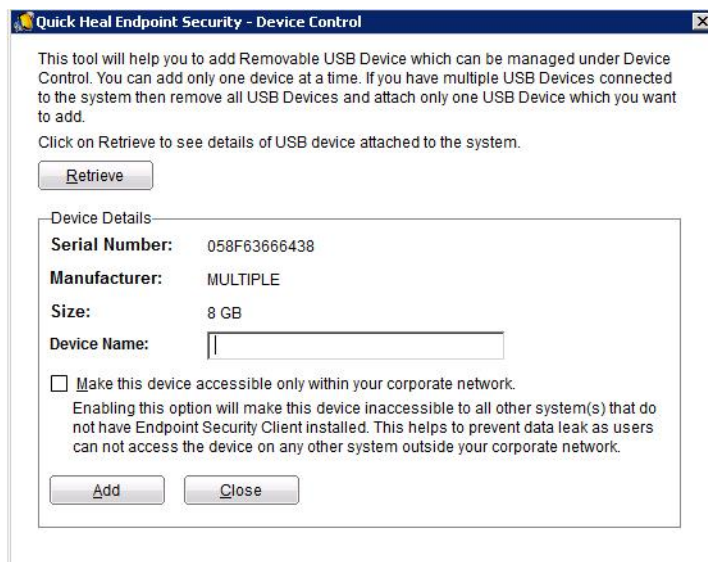
:Make this device accessible only within your corporate network

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 می باشد که در مسیر نصب

کوپیک هیل در دسترس می باشد:



اجرای برنامه از مسیر:

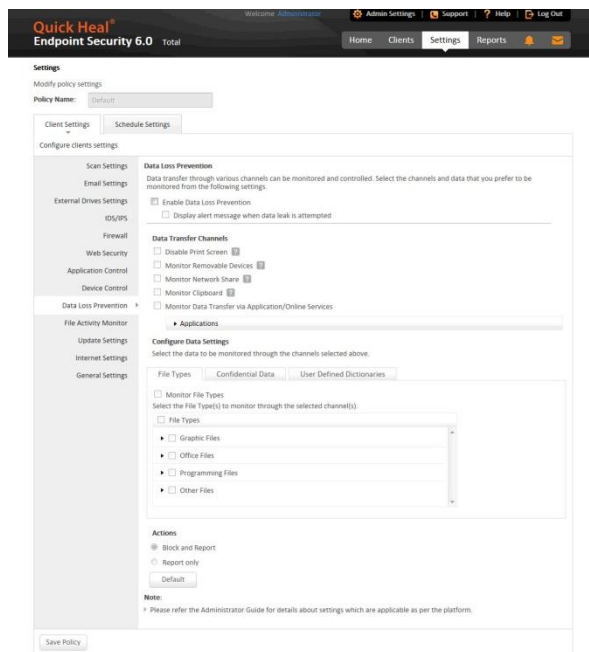
\Quick Heal Installing Path\Admin\dcconfig.exe

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:

Data Loss Prevention

Data transfer through various channels can be monitored and controlled. Select the channels and data that you prefer to be monitored from the following settings.

- ☒ Enable Data Loss Prevention
- ☐ Display alert message when data leak is attempted

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:

Data Transfer Channels

- ☐ Disable Print Screen ?
- ☐ Monitor Removable Devices ?
- ☐ Monitor Network Share ?
- ☐ Monitor Clipboard ?
- ☐ Monitor Data Transfer via Application/Online Services

► Applications

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 جداسدنی (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.

Configure Data Settings (ج): داده‌های محرمانه‌ای که می‌توانند توسط DLP مانیتور گردند در

این بخش تعریف و پیکربندی می‌گردند:

Configure Data Settings
Select the data to be monitored through the channels selected above.

File Types Confidential Data User Defined Dictionaries

☐ Monitor File Types
Select the File Type(s) to monitor through the selected channel(s).

☐ File Types

- ☐ Graphic Files
- ☐ Office Files
- ☐ Programming Files
- ☐ Other Files

Actions

☒ Block and Report

☐ Report only

Default

Note:
Please refer the Administrator Guide for details about settings which are applicable as per the platform.

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.

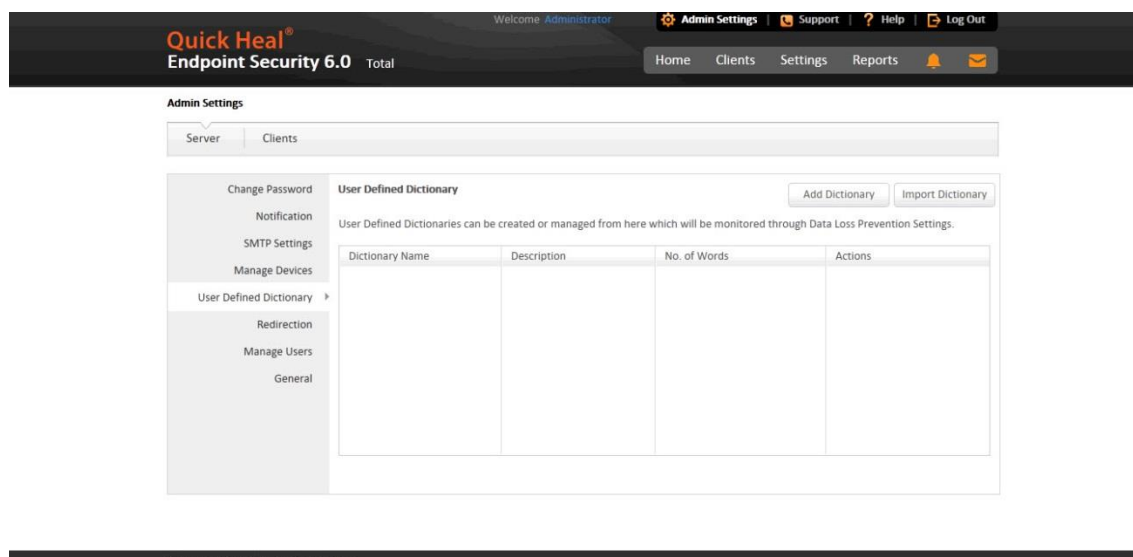
- **Match whole world:** اگر این گزینه تیک باشد، در صورتی که کلمه‌ی تعریف‌شده در دیکشنری دقیقاً برابر با این کلمه باشد تحت رهگیری قرار می‌گیرد. اما اگر این گزینه انتخاب نشود، اگر کلمه در ابتدا، وسط یا انتهای یک کلمه یا عبارت باشد، نیز رهگیری می‌گردد.

- **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 اندپوینت سکیوریتی

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)، درایوهای شبکه و درایوهای محلی (مانند C:\) قابل رصد می‌باشند.

Welcome Administrator | Admin Settings | Support | Help | Log Out

Quick Heal®
Endpoint Security 6.0 Total (Beta)

Home | Clients | Settings | Reports

Client Status | Client Action | Client Deployment | Manage Groups | Manage Policies | Assets

Modify policy settings
Policy Name: Group2_policy

Client Settings | Schedule Settings

☐ Let clients configure their own settings

Scan Settings | Email Settings | External Drives Settings | IDS/IPS | Firewall | Web Security | Application Control | Device Control | Data Loss Prevention | File Activity Monitor | Update Settings | Internet Settings | General Settings

File Activity Monitor

☐ Enable File Activity Monitor

Select File Types and Events to monitor within drives

Monitor	☒ Removable Drives	☐ Network Drives	☐ Local Drives
All Events [Copy, Rename, Delete]	☒	☒	☒
All Files	☐	☒	☒
All File Types	☐	☐	☐
Text Files	☐	☐	☐
doc	☐	☐	☐
docx	☐	☐	☐
odt	☐	☐	☐
rtf	☐	☐	☐
txt	☐	☐	☐
Data Files	☐	☐	☐
Audio Files	☐	☐	☐
Video Files	☐	☐	☐
Image Files	☐	☐	☐
Spreadsheet Files	☐	☐	☐
Database Files	☐	☐	☐
Executable Files	☐	☐	☐
System Files	☐	☐	☐
Compressed Files	☐	☐	☐
Custom Files	☒	☐	☐
Files Without Extensions	☐	☐	☐

Exclusions

%Windir%\Temp\
 ?:\System Volume Information\
 %Windir%\SoftwareDistribution\
 ?:\Users*\AppData\Local\Microsoft\Internet Explorer\
 ?:\Users*\AppData\Local\Microsoft\Windows\Temporary Internet Files\
 %programfiles%\
 %commonfiles%\%1\%2\

Default

Note:
Please refer the Administrator Guide for details about settings which are applicable as per the platform.

Save Policy | Cancel

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 شده‌اند.

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 اندپوینت سکیوریتی در اینجا پیکربندی نمی‌شود.

Enable Automatic Update: در صورت فعال بودن این گزینه بروزرسانی کلاینت‌ها 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 در نظر 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 دکمه‌های 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 کوئیک‌هیل به اینترنت متصل شود تنظیمات پراکسی را در این بخش وارد می‌نمایید.

The screenshot displays the 'Internet Settings' configuration window. On the left, a sidebar lists settings categories: Scan Settings, Email Settings, External Drives Settings, IDS/IPS, Firewall, Web Security, Application Control, Device Control, Update Settings, Internet Settings (selected), and General Settings. The main area is titled 'Internet Settings' and contains the following options:

- ☒ Enable Proxy Settings
- Proxy Type: HTTP Proxy (dropdown menu)
- Proxy Server: 192.168.2.1 (text input)
- Port: 8080 (text input)
- Authentication to connect through firewall or proxy server (label)
- User name: (text input)
- Password: (text input)

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 کوئیک‌هیل 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 کوئیک‌هیل به محافظت خود ادامه می‌دهد.

Enable Self Protection: در صورتی که این گزینه فعال باشد، کوئیک‌هیل 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 برنامه‌ها، بهینه سازی، اسکن آسیب پذیری را زمانبندی نمایید.

The screenshot shows the 'Schedule Settings' window. On the left, there's a sidebar with 'Client Settings' selected. Under 'Client Settings', 'Client Scan' is expanded. The 'Client Scan' section has a checkbox 'Enable Schedule Scan' which is checked. Below it, 'Frequency' is set to 'Daily', 'Start At' is '0 Hrs 0 Mins', 'Repeat Scan' is 'Every 1 Hrs', and 'Notify if client is off-line' is unchecked. The 'Scanner Settings' section has 'How to Scan' set to 'Quick Scan (Scan Drive where Operating System is installed)', 'Select scan mode' set to 'Automatic (Recommended)', and 'Select the items to scan' with 'Scan executable files' selected. Other options like 'Scan all files', 'Scan packed files', 'Scan mailboxes', and 'Scan archives files' are also visible. The 'Antimalware Scan Settings' section has 'Perform Antimalware scan' checked and 'Select action to be performed when malware found' set to 'Clean'.

Client Scan

سربرگ اول این بخش مربوط به زمانبندی اسکن کلاینت می‌باشد. در این بخش می‌توانید تعیین کنید که در دوره‌های زمانی خاص، کوئیک‌هیل 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. دوره‌های 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 برنامه‌ها را زمانبندی نمایید تا در زمان مشخص شروع به اسکن برنامه‌های غیرمجاز (Unauthorized applications)، برنامه‌های مجاز و غیرمجاز (Unauthorized applications and authorized applications)، تمامی برنامه‌های نصب شده (All installed applications) نماید.

The screenshot shows the 'Application Control Schedule Scan' configuration window. On the left is a sidebar with 'Client Scan' selected, containing 'Application Control', 'Tuneup', and 'Vulnerability Scan'. The main area is titled 'Application Control Schedule Scan' and includes the following settings:

- ☐ Enable Schedule Scan
- Frequency:
- Start At: Hrs Mins
- ☐ Repeat Scan
- Every: Hrs
- ☐ Notify if client is off-line

Scan and Report

- ☒ Unauthorized applications
- ☐ Unauthorized and authorized applications
- ☐ All installed applications

Tuneup Schedule Scan

زمانبندی اسکن بهینه سازی در این بخش تعیین می گردد. در بخش اول زمانبندی مشخص می گردد.

تنظیمات بهینه سازی

Disk cleanup: پاکسازی دیسک انجام می گیرد.

Registry cleanup: پاکسازی رجیستری صورت می پذیرد.

Defragment at next boot: در راه اندازی بعدی، فایل های سیستمی و مهم ویندوز دفرگمنت

می شود و موجب افزایش سرعت سیستم می گردد.

Vulnerability Scan

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

Vulnerability Scan

☐ Enable Schedule Scan

Weekday: Monday

Start At: 0 Hrs 0 Mins

☐ Repeat Scan

Every: 1 Weeks

☐ Notify if client is off-line

Scan and Report

Scan for vulnerability against following software vendors:

- ☒ Microsoft applications and other vendor applications
- ☐ Microsoft applications only
- ☐ Other vendor applications only

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

Assets

مدیریت دارایی یکی از ویژگی‌های پرکاربرد کوئیک هیل اندپوینت سکیوریتی ۶ 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.

Quick Heal®
Endpoint Security 6.0 Total (Beta)

Welcome Administrator | Admin Settings | Support | Help | Log Out

Home Clients Settings Reports

Clients

Client Status | Client Action | Client Deployment | Manage Groups | Manage Policies | Assets

In this section, you can view system information, hardware information, etc. of EPS Clients. Please select the client and click on View Details.

Endpoint name/IP

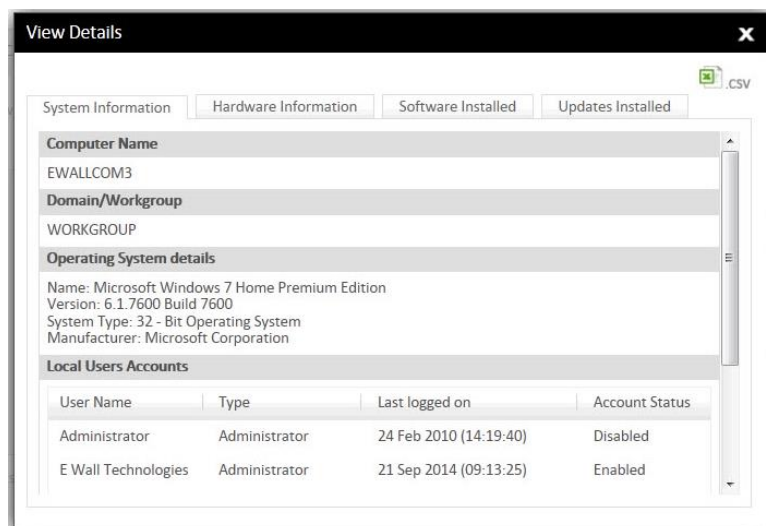
Endpoint Name	Group	Domain	IP Address	Operating System
ASUS-LAPTOP	Default	WORKGROUP	192.168.0.173	Microsoft
ESI-PC	Group2	FANOOS	192.168.0.12	Microsoft
EWALLCOM3	Group2	WORKGROUP	192.168.0.100	Microsoft
NOVIN-4F5007EDC	Default	FANOOS	192.168.0.5	Microsoft
WIN-EN9EU7HH0E3	Group2	FANOOS	192.168.0.50	Microsoft

Show endpoints within subgroup

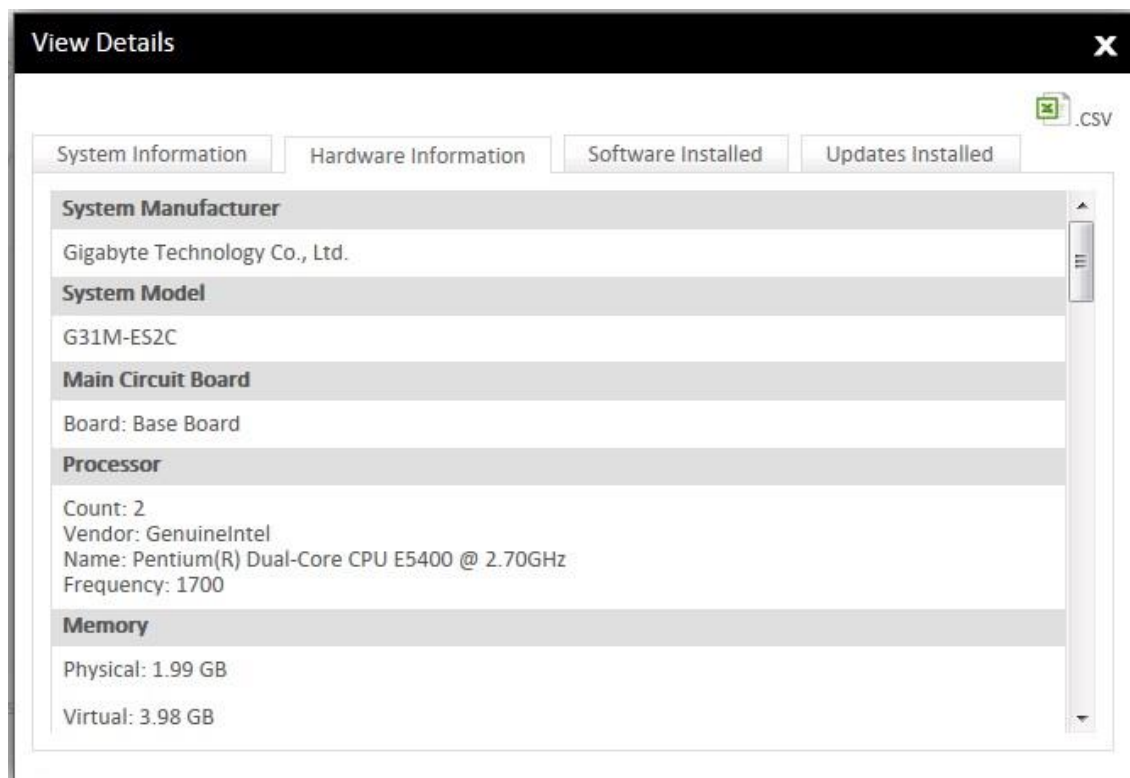
View Details

© 2013 Quick Heal Technologies (P) Ltd

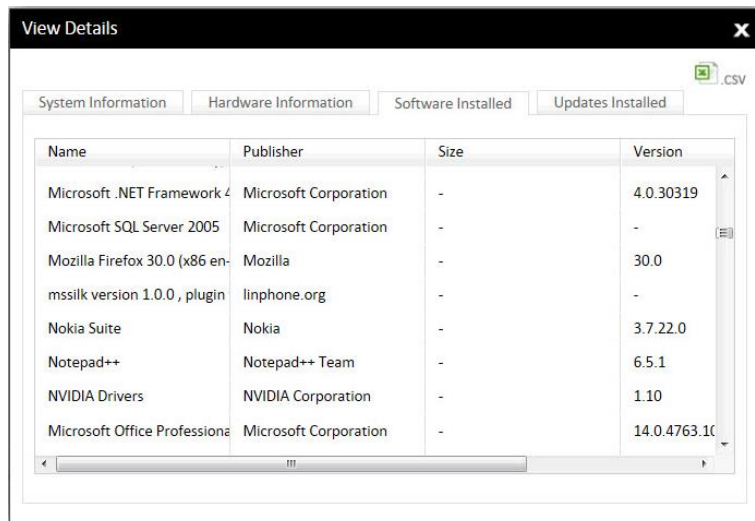
با کلیک بر روی کلاینت موردنظر و فشردن دکمه View Details می‌توانید کلیه اطلاعات کامپیوتر موردنظر را دریافت نمایید.



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.

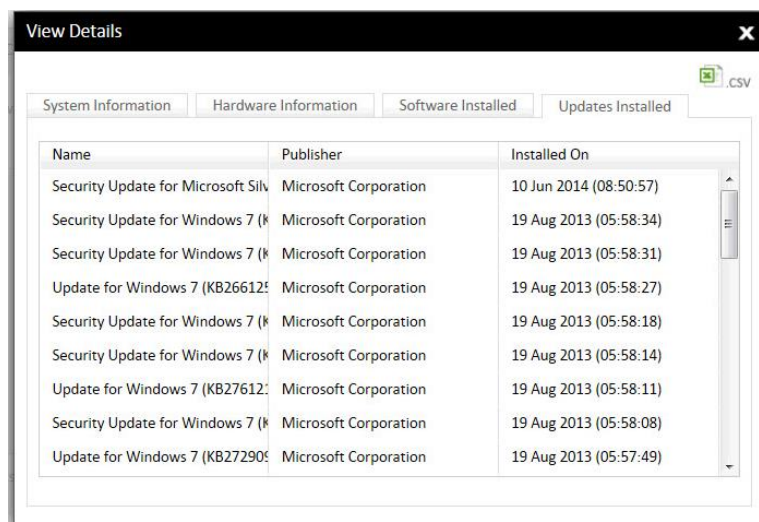


Hardware Information: اطلاعات کامل سخت‌افزاری کلاینت در این بخش قابل مشاهده می‌باشد. این اطلاعات شامل سازنده سیستم، مدل، سریال و مدل مادربرد، اطلاعات CPU، حافظه اصلی RAM، هارد دیسک و میزان ظرفیت و فضای آزاد درایوها، بایوس، مشخصات کارت گرافیک، کارت صدا، اطلاعات کامل کارت شبکه، مانیتور و چاپگرهای متصل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



Name	Publisher	Size	Version
Microsoft .NET Framework 4	Microsoft Corporation	-	4.0.30319
Microsoft SQL Server 2005	Microsoft Corporation	-	-
Mozilla Firefox 30.0 (x86 en-	Mozilla	-	30.0
mssilk version 1.0.0, plugin	linphone.org	-	-
Nokia Suite	Nokia	-	3.7.22.0
Notepad++	Notepad++ Team	-	6.5.1
NVIDIA Drivers	NVIDIA Corporation	-	1.10
Microsoft Office Professional Edition	Microsoft Corporation	-	14.0.4763.10

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



Name	Publisher	Installed On
Security Update for Microsoft Silverlight	Microsoft Corporation	10 Jun 2014 (08:50:57)
Security Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:58:34)
Security Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:58:31)
Update for Windows 7 (KB2661254)	Microsoft Corporation	19 Aug 2013 (05:58:27)
Security Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:58:18)
Security Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:58:14)
Update for Windows 7 (KB2761254)	Microsoft Corporation	19 Aug 2013 (05:58:11)
Security Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:58:08)
Update for Windows 7 (KB2729095)	Microsoft Corporation	19 Aug 2013 (05:57:49)

Updates Installed: هرگونه بروزرسانی نرم افزاری و سیستم عامل 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 نرم افزارها و تغییرات سخت افزاری، نسبت به عیب یابی آن اقدام نمود.

Settings

گزینه های این بخش دقیقاً همانند افزودن یک پالیسی جدید می باشد. با این تفاوت که این تنظیمات بر روی کلاینت هایی که عضو هیچ گروه خاصی نبوده اعمال می گردد. در واقع پالیسی پیش فرض کلاینت ها می باشد.

Quick Heal® Endpoint Security 6.0 Total

Welcome Administrator | Admin Settings | Support | Help | Log Out

Home Clients **Settings** Reports

Settings

Modify policy settings

Policy Name: Default

Client Settings | **Schedule Settings**

Configure clients settings

Scanner Settings

Select scan mode:

☒ Automatic (Recommended)

☐ Advanced

Select the items to scan:

☒ Scan executable files

☐ Scan all files requires more time

☒ Scan packed files

☒ Scan mailboxes

☒ Scan archive files

Archive Scan Level: 2

Select action to be performed when virus found in archive file: Skip

Select action to be performed when a virus is found: Repair

Virus Protection Settings

☒ Load Virus Protection at Startup

☒ Display alert messages

☒ Report source of infection

Select action to be performed when a virus is found: Repair

Advanced DNAScan

☒ Enable DNAScan

☒ Enable Behavior detection system

Select Behavior detection level: Moderate

(Moderate: High in detection of new threats with few alerts requiring an action)

Submit suspicious files

☒ Submit files

☒ Show notification while submitting files

Block Suspicious Packed Files

☒ Block Suspicious Packed Files

Automatic Rogueware Scan Settings

☒ Enable Automatic Rogueware scan

Disconnect Infected Endpoints from the network

☐ When non-repairable virus found

☐ When suspicious file found by DNAScan

Exclude Files and Folders

List of files and folders to be excluded from scanning

Path	Include Subfolder	Excluded For

Add

Delete

Exclude Extensions

Specify the file extensions to exclude its scanning by real time virus protection. This is to troubleshoot performance related issues by excluding certain categories of files that may be causing the issue.

Add

Delete

Default

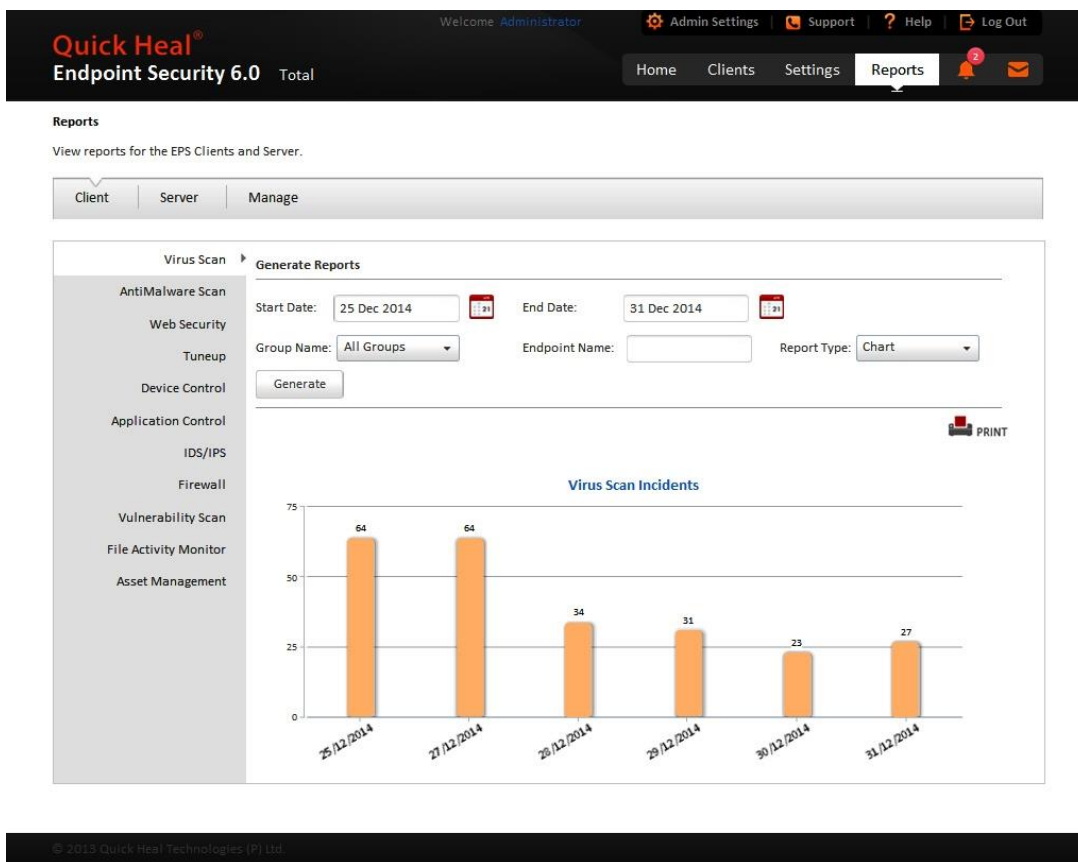
Note:

Please refer the Administrator Guide for details about settings which are applicable as per the platform.

Save Policy

Reports

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



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

Generate Reports: در بخش اول شرایط تولید گزارش تعیین می شود.

Start Date: تاریخ شروع

End Date: تاریخ انتها

Group Name: نام گروه

Computer Name: نام کامپیوتر که می تواند خالی باشد.

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

(Tabular) باشد.

Server

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

Quick Heal®
Endpoint Security 6.0 Total

Welcome Administrator | Admin Settings | Support | Help | Log Out

Home Clients Settings Reports

Reports

View reports for the EPS Clients and Server.

Client Server Manage

Event Logs ▶ Event Logs

Start Date: 25 Dec 2014 End Date: 31 Dec 2014 Category: All

Generate

DELETE PRINT .CSV .PDF

Date and Time	Category	Message
31 Dec 2014 (08:45:14)	Information	Administrator logged in.
31 Dec 2014 (08:00:02)	Information	License information has been updated.
30 Dec 2014 (08:00:02)	Information	License information has been updated.
29 Dec 2014 (09:04:52)	Information	Administrator logged in.
29 Dec 2014 (07:59:59)	Information	License information has been updated.
28 Dec 2014 (08:39:52)	Information	Administrator logged out.
28 Dec 2014 (08:00:02)	Information	License information has been updated.
28 Dec 2014 (07:48:26)	Information	Administrator logged in.
27 Dec 2014 (13:57:19)	Information	Administrator logged out.

© 2013 Quick Heal Technologies (P) Ltd.

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

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

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

: خروجی به صورت pdf صادر می‌شود.

Manage

در این بخش تنظیمات مربوط به گزارش قابل اعمال است.

Quick Heal® Endpoint Security 6.0 Total

Welcome Administrator | Admin Settings | Support | Help | Log Out

Home Clients Settings **Reports**

Reports

View reports for the EPS Clients and Server.

Client Server **Manage**

Settings ▶ Settings

Export
Delete Reports

☐ Automatically delete reports older than 60 days.

☐ Automatically email reports for past 7 days to the following recipients.

Email Address (For multiple email addresses, use comma in between)

Email Frequency

Day: Monday At: 08:00

Select Reports to email

- ☐ Server Reports
- ☐ Clients Reports
 - ☐ Virus Scan
 - ☐ AntiMalware Scan
 - ☐ Web Security
 - ☐ Tuneup
 - ☐ Device Control
 - ☐ Application Control
 - ☐ IDS/IPS
 - ☐ Firewall
 - ☐ Vulnerability Scan
 - ☐ File Activity Monitor
 - ☐ Asset Management

Save

Note:
To receive report emails, SMTP settings must be configured in Admin Settings.

© 2013 Quick Heal Technologies (P) Ltd.

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

اندپوینت سکیوریتی 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 می‌توانید نوع گزارشی که به ایمیل ارسال می‌شود را تعیین نمایید:

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

The screenshot shows the 'Export Reports' section of the software. It includes a sidebar with 'Settings', 'Export', and 'Delete Reports'. The main area is titled 'Export Reports' and 'Export reports to PDF:'. It has two radio buttons for 'Select Criteria': 'All Reports' (selected) and 'As per below criteria'. Below these are fields for 'Start Date' (11 Feb 2014) and 'End Date' (18 Feb 2014), both with calendar icons. There are also fields for 'Group Name' (All Groups) and 'Computer Name'. A 'Select Reports' section lists various report types with checkboxes: Server Reports, Clients Reports, Virus Scan, AntiMalware Scan, Web Security, Tuneup, Device Control, Application Control, IDS/IPS, Firewall, and Vulnerability Scan. All are checked. An 'Export' button is at the bottom.

Delete Reports

در این بخش می‌توانید تنظیمات خود را طوری قرار دهید تا پس از مدتی گزارش‌ها حذف گردند.

The screenshot shows the 'Manually delete reports' section. It has two radio buttons: 'Delete reports older than' (selected) and 'Delete all reports'. The 'Delete reports older than' option has a dropdown menu set to '60' days. Below is a 'Select Reports' section with checkboxes for 'Clients Reports' and 'Server Reports', both of which are checked. A 'Delete' button is at the bottom.

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

Delete all reports: حذف همه گزارش‌ها.

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

Clients Reports: گزارش های کلاینت ها حذف گردند.

Server Reports: گزارش های سرور حذف گردند.

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

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 می باشد، 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 اندپوینت سکیوریتی کوئیک هیل قرار دارند.

Change Password

Quick Heal®
Endpoint Security 6.0 Total

Welcome Administrator | Admin Settings | Support | Help | Log Out

Home Clients Settings Reports

Admin Settings

Server Clients

Change Password

The Quick Heal Endpoint Security server is password protected to prevent unauthorized users from modifying the settings or removing the client program from the endpoints. The Quick Heal Endpoint Security setup program requires you to specify an Administrator password. However, you can change the Administrator password from this page at any time.

Old Password:

New Password:

Confirm Password:

Apply

© 2013 Quick Heal Technologies (P) Ltd.

در این بخش می‌توانید رمز عبور سروری کوئیک هیل اندپوینت سکیوریتی را تعویض کنید.

Old Password: رمز عبور قبلی را وارد کنید.

New Password: رمز عبور جدید را وارد کنید.

Confirm Password: رمز عبور 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 سازی،

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 پوشش 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 اندپوینت سکیوریتی

کوئیک هیل 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

اکتیو دایرکتوری 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 در حال 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.

The screenshot shows a window titled "Email & SMS Notification". It contains two sections: "Email Notification" and "SMS Notification". Each section has a "List of" label, a text input field, and a list box. To the right of each list box are three buttons: "Add", "Edit", and "Delete". At the bottom of the window are "Apply" and "Cancel" buttons.

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

SMTP Server Settings

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

The screenshot shows the 'Admin Settings' page for 'Quick Heal Endpoint Security 6.0'. The 'Server' tab is selected. On the left sidebar, 'SMTP Settings' is highlighted. The main content area is titled 'SMTP Server Settings' and contains the following fields and options:

- SMTP Server:** A text input field.
- Port:** A text input field.
- Notify from Email Address:** A text input field. A note next to it states: '(All emails sent from the EPS server will have this Email address as the sender's address)'.
- Require Server authentication:** A checkbox.
- User name:** A text input field.
- Password:** A text input field.
- User Authentication Method:** A dropdown menu currently set to 'None'.
- Apply:** A button at the bottom.

At the bottom of the page, there is a copyright notice: '© 2019 Quick Heal Technologies (P) Ltd.'.

SMTP Server: سرور SMTP در این فیلد وارد می شود.

Port: آدرس پورت سرور SMTP در این فیلد وارد می شود.

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

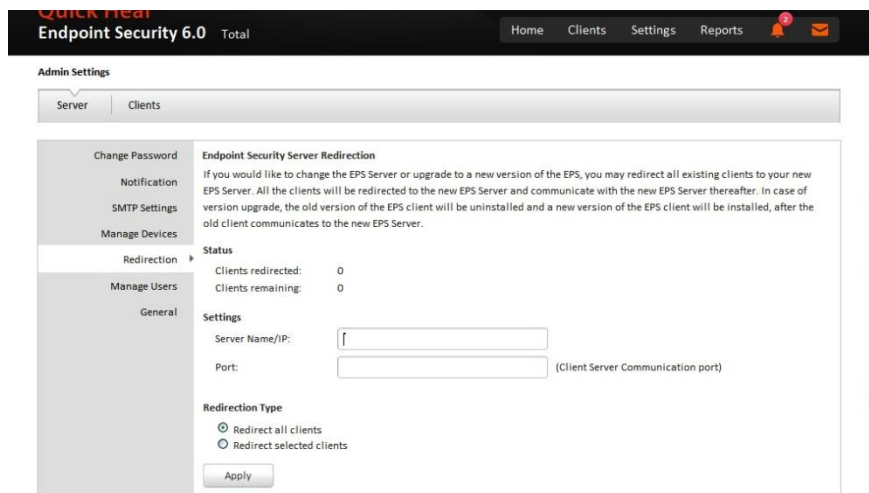
Require Server authentication: در صورتی که سرور SMTP نیاز به احراز هویت دارد، این گزینه را تیک کنید.

User name: نام کاربری در این فیلد وارد می شود.

Password: رمز عبور در این فیلد وارد می شود.

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

Redirection



Endpoint Security Server Redirection

یکی از ویژگی های مفید کوئیک هیل اندپوینت سکیوریتی، امکان آپگرید (Upgrade) و تغییر نسخه بدون نیاز به حذف و نصب از روی کلاینت ها می باشد. همچنین در صورت تمایل می توانید، بدون دردسر نصب و حذف از روی کلاینت ها، به راحتی سرور اندپوینت خود را تغییر دهید. در صورت انتشار نسخه جدید (معمولاً سالانه یکبار نسخه جدید منتشر می گردد) نسخه جدید را بر روی سرور جدید و یا در کنار اندپوینت فعلی نصب می کنید. سپس آدرس IP و یا نام سرور بسته به روش نصب - و آدرس پورت سرور جدید اندپوینت را در نسخه قبلی اندپوینت وارد می کنید. به صورت خودکار همه کلاینت ها از سرور اندپوینت جاری به سرور جدید اندپوینت منتقل شده و در صورت نیاز نسخه قبلی خودکار حذف و نسخه جدید کوئیک هیل کلاینت بر روی کلاینت ها نصب می شود. بنابراین تنها نیاز دارید آدرس IP یا نام سرور جدید را در این بخش سرور قدیمی وارد نمایید.

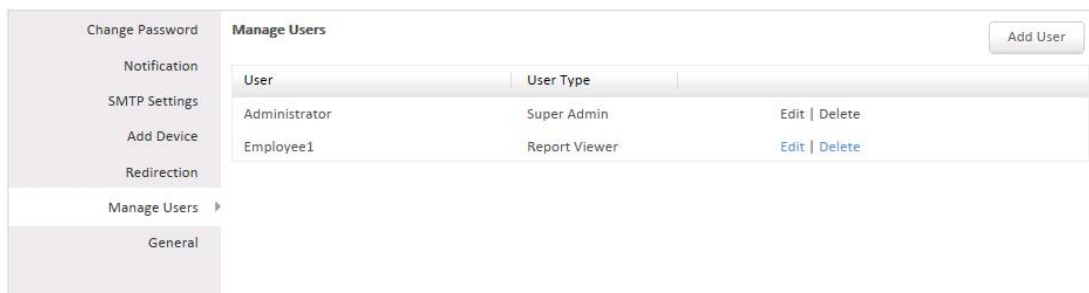
Server Name/IP: نام سرور یا IP اندپوینت جدید را وارد می کنید. (در صورتی که اندپوینت جدید را بر روی همان سرور قبلی نصب کردید، آدرس IP یا نام همین کامپیوتر را وارد کنید)

Port: آدرس پورت اندپوینت جدید را در این بخش وارد کنید، آدرس پورت همان آدرسی است که کلاینت ها با سرور ارتباط برقرار می کنند (مثلاً پورت پیش فرض در Quick Heal Endpoint Security 6.0، آدرس ۵۰۴۴ می باشد).

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

Manage Users

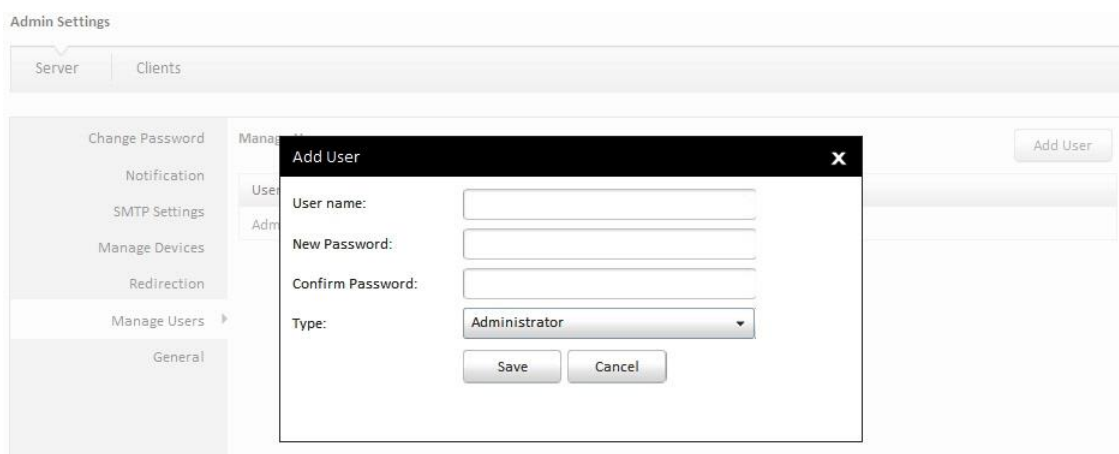
در این بخش، کاربران استفاده کننده از کنسول اندپوینت سکیوریتی، قابل مدیریت می باشند.



مدیر پیش فرض اندپوینت، **Administrator** می باشد 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 می شود.



User name: نام کاربری جدید در این فیلد وارد می شود.

New Password: رمز عبور در این فیلد وارد می شود.

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

Type: در این فیلد نوع دسترسی مشخص می گردد که می تواند 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.

Admin Settings

Server | Clients

Change Password ▶ **Change Password**

Notification

SMTP Settings

Manage Devices

Redirection

Manage Users

General

The Quick Heal Endpoint Security server is password protected to prevent unauthorized users from modifying the settings or removing the client program from the endpoints. The Quick Heal Endpoint Security setup program requires you to specify an Administrator password. However, you can change the Administrator password from this page at any time.

Old Password:

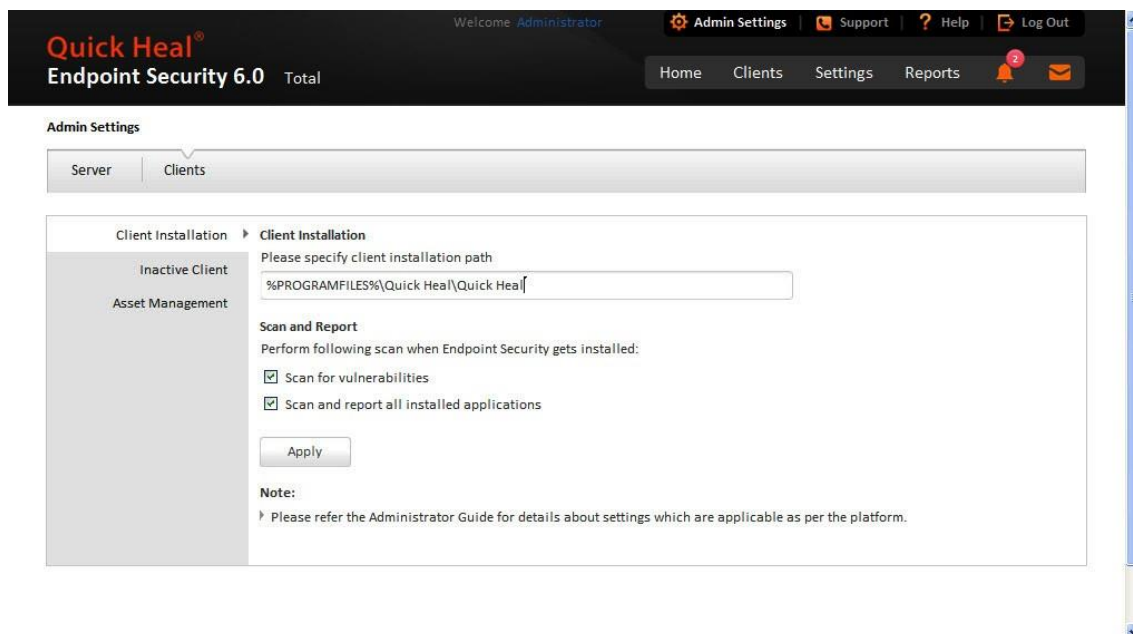
New Password:

Confirm Password:

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،

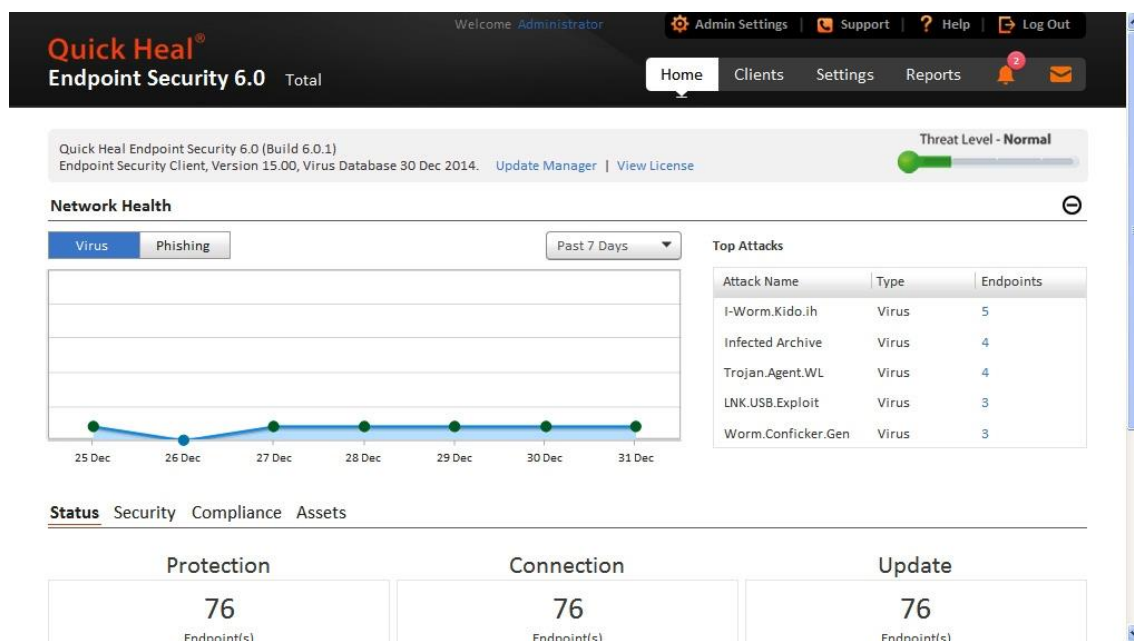
اندپوینت آن را حذف شده در نظر گرفته و لایسنس آن را برای نصب بر روی سیستم دیگر آزاد می‌کند.

مدیریت لایسنس

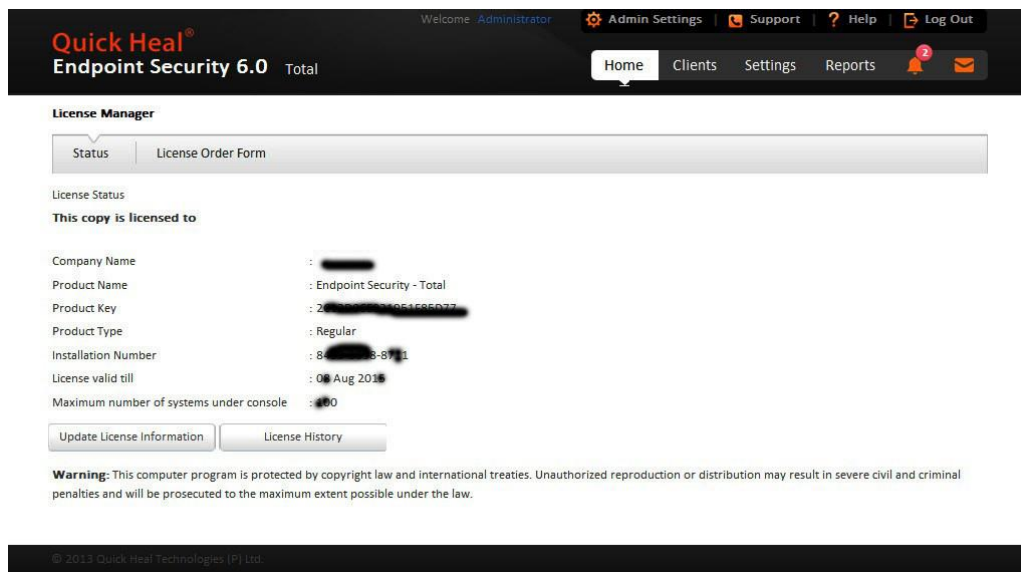
پس از انقضای مدت زمان اعتبار لایسنس و اجرای پروسه مالی سفارش خرید، زمان اعتبار اندپوینت سکیوریتی کوئیک هیل خود را افزایش دهید.

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

همچنین امکان ارتقای نسخه محصول از Quick Heal Endpoint Security Business به نسخه کامل تر Total بدون نیاز به نصب و حذف مجدد کنسول سرور و کلاینت ها میسر می باشد. همه فرایندهای فوق تنها با فشردن یک دکمه صورت می پذیرد.



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

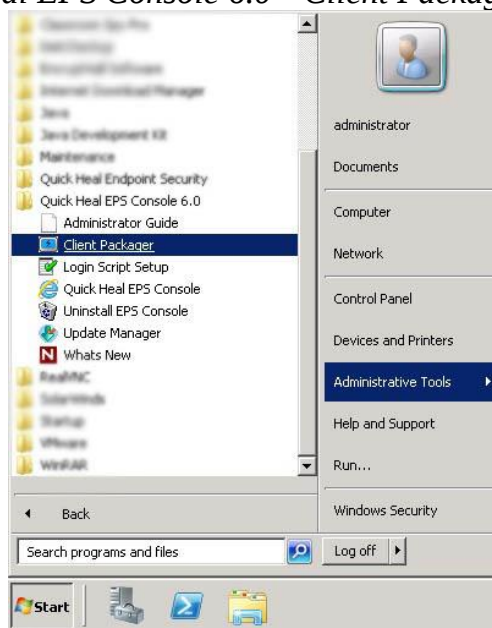
همانطور که در بخش Client Deployment شرح داده شد، ۶ روش مختلف نصب وجود دارد که بسته به سلیقه مدیر و پیکربندی شبکه قابل انتخاب است. در این بخش به ۲ نمونه از روش های پرکاربرد اشاره می کنیم. این روش ها بر روی انواع ساختارهای شبکه (Domain-based و Workgroup) قابل استفاده است.

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

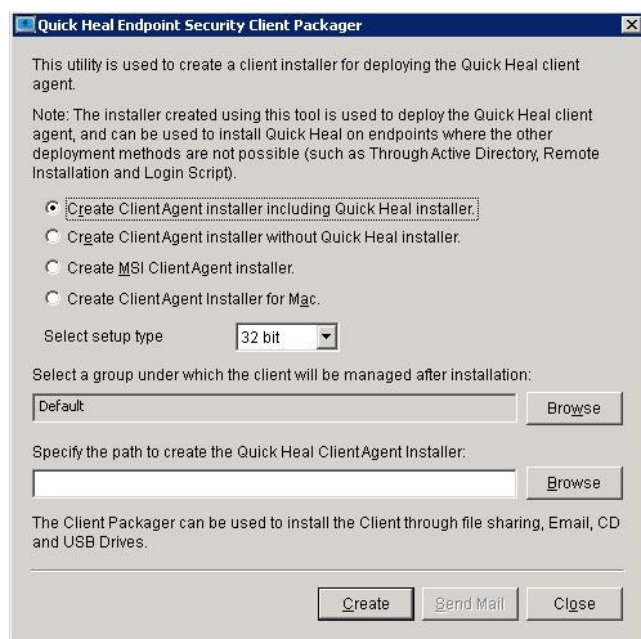
الف) استفاده از Client Packager

ساده ترین راه، نصب بر روی کلاینت ها می باشد. یک فایل پکیجر نصب کننده ساخته و آن را بر روی کلاینت ها (از طریق به اشتراک گذاری در شبکه و یا فلش) منتقل و اجرا می کنید. برای ساختن فایل Client Packager از مسیر زیر سرور استفاده کنید:

Start > Quick Heal EPS Console 6.0> Client Packager



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



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 کوئیک هیل ساخته می شود.

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

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

Select setup type: بسته به نوع معماری کلاینتی، نوع ClientAgent می تواند ۳۲ یا ۶۴ بیتی باشد.

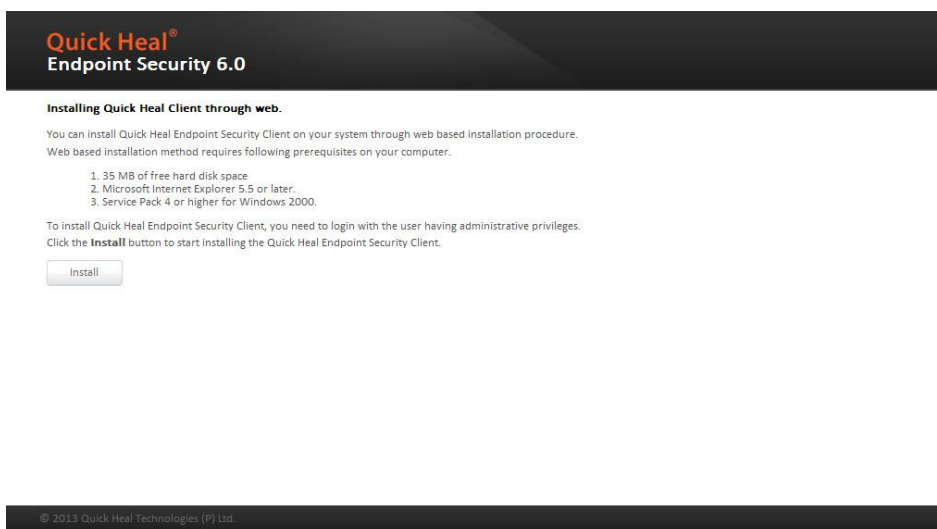
Select a group under which the client will be managed after installation: اگر از قبل گروه و پالیسی در سرور اندپوینت تعریف کرده اید، می توانید گروه را در این بخش تعیین کنید تا پکیجر متناسب با آن گروه ساخته شود. همچنین می توانید گروه را به صورت Default رها کرده و پس از نصب بر روی کلاینت، آن را عضو گروه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

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

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

Send Mail: امکان ارسال کلاینت ایجنت به صورت ایمیل نیز در نظر 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 بر روی 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 بر روی کلاینت انجام می‌پذیرد.

خاتمه

در کنار سه شعار اصلی هوشمندتر، سبک‌تر و سریع‌تر (smarter, lighter, faster) کوپیک‌هیل، که نمایانگر استفاده حداقلی از منابع می‌باشد، رعایت اصول سادگی، کاربرپسند در نصب، راه‌اندازی و مدیریت اندپوینت سکیوریتی کوپیک‌هیل 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 کوپیک‌هیل 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 کوپیک‌هیل می‌گردد.

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