

# Quick Heal Endpoint Security 5.3 New Features and Enhancement

معرفی ویژگی‌های جدید

در

**کوئیک هیل اندپوینت سکیوریتی ۵.۳**

پشتیبانی و فروش در ایران:

شرکت فناوری ارتباطات و اطلاعات فانوس

نماینده رسمی محصولات امنیت سازمانی کوئیک‌هیل در ایران

Web: [Quickheal.co.ir](http://Quickheal.co.ir)

Tel: 021-77142526

Email: [info@qhi.ir](mailto:info@qhi.ir)

Support: [support.quickheal.co.ir](http://support.quickheal.co.ir)

## ویژگی‌ها و بهینه‌سازی‌های جدید:

### ۱. نیازمندی‌های سیستم

نیازمندی‌های سمت سرور

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

### حداقل نیازمندی‌های سیستم کنسول

- 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium processor or equivalent
- 1 GB of RAM
- 3250 MB of free disk space
- Monitor that supports 1024 x 768 resolutions in 256-color mode
- Internet Explorer Version 7, 8, 9, 10, or **11 جدید**.

### نیازمندی‌های سمت کلاینت

#### Windows Workstations supported

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

#### Mac Workstations supported

Mac OS X 10.6, 10.7, 10.8, **10.9 جدید**

Mac Computer with Intel Processor

## Linux Workstations supported

### 32-Bit:

Redhat 9

Redhat Enterprise Linux 4,5,3,6.0

Fedora 7,12,13, 14

SuSE 7.3, SuSE ES 10, SuSE ES 11

BOSS

Mandrake 9.2

Mandriva 2008

CentOS 5

Ubuntu 7.10, 10.04 LTS, 10.04.1 LTS

### 64-Bit:

Redhat Enterprise Linux 5.3,6.0

Fedora 13, 14

SUSE ES 11

Ubuntu 10.04 LTS, 10.04.1 LTS

### حداقل نیازمندی های سیستمی برای کلاینت ویندوز

256 MB of RAM

1800 MB of free disk space

1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista, Windows 2008

Server and Windows 7

1 GB of RAM for Windows Vista and Windows 7

512 MB of RAM for Windows 2008 and Windows 2008 R2

For Windows 2000 – Service Pack 4 or later

Internet Explorer 5.5 or later

Administrative privilege is required for installation

### حداقل نیازمندی های سیستمی برای کلاینت مک (Mac)

512 MB of RAM

1200 MB free hard disk space

### حداقل نیازمندی های سیستمی برای کلاینت لینوکس

133 MHz or later Intel based (or compatible) processor

128 MB or later RAM

500 MB of free hard disk space

توجه: لیست بروز شده در راهنمای اندپوینت سکيوریتی ۵.۳ ذکر شده است،

## ۲. اسکن آسیب‌پذیری (Vulnerability Scanning):

این ویژگی جدید آسیب‌پذیری‌های سیستم‌عامل‌ها و انواع مختلف برنامه‌های کاربردی مانند ادوبی، موزیلا، اوراکل و... را اسکن می‌کند. ویژگی اسکن آسیب‌پذیری تنها از پلتفرم ویندوز پشتیبانی می‌کند.

## ۳. کلاینت کوییک هیل ۲۰۱۴ در EPS5.3 مجتمع شده است.

تنظیمات زیر نیز در کلاینت‌های ویندوز از سرور QHEPS قابل پیکربندی است:  
الف) تنظیمات سیستم رفتارشناسی: سیستم رفتارشناسی، تهدیدات ناشناخته را تنها با واریسی رفتارهای مشکوک شناسایی می‌کند.

ب) تنظیمات محافظت Safe Mode: محافظت Safe Mode از دسترسی غیرمجاز به سیستم در زمان راه اندازی سیستم در حالت Safe Mode جلوگیری می‌کند.

ج) محافظت پردازش برای آنتی ویروس کوییک هیل در سیستم کلاینت.

د) اسکن زمان بوت (Boot time scan) نیز می‌تواند از روی سرور EPS تنظیم گردد.

ه) تنظیمات امنیت وب‌سایت زیر نیز می‌توانند از روی سرور QHEPS پیکربندی گردند:

۱. پیام اخطار که در زمان مسدود شدن وب‌سایت نمایش داده می‌شود.

۲. فعال کردن گزارش امنیت وب‌سایت

۳. مستثنی کردن زیردامنه‌ها از دسته‌های وب‌سایت مسدود شده.

## ۴. کنترل ابزار برای کلاینت‌های Mac: کنترل ابزار از پلتفرم‌های مک نیز

پشتیبانی می‌کند.

## ۵. بهینه‌سازی کلاینت پکیجر (Client Packager):

الف) امکان ساخت کلاینت پکیجر را به فرمت MSI وجود دارد. این ویژگی در زمان استقرار کلاینت‌ها با استفاده از سیاست‌گذاری‌های گروه اکتیو دایرکتوری کاربرد دارد.

ب) مدیر می‌تواند در زمان ساختن کلاینت پکیجر، گروه و سیاستی که کلاینت پس از نصب در آن قرار خواهد گرفت را انتخاب نماید.

ج) پشتیبانی از نام کامپیوتر یونیکد در کلاینتها افزوده شد. کلاینت های می توانند بر روی کامپیوترهایی که دارای نام با زبان محلی مانند فارسی، کره‌ای، لهستانی و... هستند، نصب گردند.

## ۶. بهینه سازی صفحه داشبورد (اول) وب کنسول اندپوینت سکيوریتی:

الف) وضعیت استقرار، آخرین وضعیت کلاینت‌هایی که نصب و استقرار در آنها ناموفق بوده است را نشان می دهد. اگر استقرار یک کلاینت ناموفق بود، یک لینک نمایش جزئیات (View Details) نشان داده خواهد شد که به مدیران کمک می کند تا لیست کاملی از همه کلاینت‌هایی که استقرار بر روی آنها ناموفق بوده به همراه لینک تاریخچه نصب (Installer Log) را مشاهده نمایند. لینک View Installer Log کمک می کند تا دلیل نصب ناموفق کلاینت مشخص گردد.

ب) اگر تعداد کلاینت های نصب شده از تعداد کلاینت قابل پشتیبانی -براساس لایسنس خریداری شده- بیشتر گردد، پیام خطاری نمایش داده خواهد شد.

ج) بخش راهنما (Help) و پشتیبانی (Support) افزوده شد.

د) نمودارهای حلقه ای برای بالاترین آسیب‌پذیری ها (Top Vulnerabilities) و دقت آسیب‌پذیری (Vulnerability Severity) افزوده شد.

## ۷. بهینه سازی کنترل برنامه (Application control):

کنترل برنامه از برنامه های بیشتری پشتیبانی می کند. برخی نسخه های جدید برنامه ها و طبقه‌بندی‌های جدید برنامه ها مانند نرم‌افزارهای پشتیبان‌گیری (Backup Softwares)، نرم‌افزارهای آموزشی (Educational Softwares)، متفرقه (Miscellaneous)، نرم‌افزارهای امنیتی (Security Softwares) و نرم‌افزارهای بهینه‌سازی (Tuning Software) به لیست پیش‌فرض برنامه ها افزوده شدند.

## ۸. بهینه سازی‌های دیگر:

الف) تنها گروه های انتخاب شده می توانند صادر گردند از Client Status -> Clients and Clients ->

Manage Groups. این ویژگی به مدیران کمک می‌کند تا اطلاعات گروه‌های انتخاب شده را صادر و ذخیره نمایند. (در نسخه‌های قبلی QHEPS انتخاب هر گروه، همه گروه‌های آن صفحه صادر می‌شدند.)

ب) دکمه Browse در Update Manager > Configuration > Pick from specified Path افزوده شد. این دکمه به مدیران کمک می‌کند تا مسیر بروزرسانی را مرور و انتخاب نمایند.

ج) تعداد ۲۰ رکورد در هر صفحه گزارش کنسول وب QHEPS در Reports > Tabular reports view و Reports > Server > Event Logs نمایش داده می‌شود.

د) پروتکل‌های امنیتی SSL/TLS برای اطلاع‌رسانی‌های ایمیل (Email notifications) افزوده شده است. بنابراین مدیران می‌توانند از سرورهای SMTP که از احراز هویت SSL و TLS (مانند gmail) استفاده می‌کنند، برای دریافت ایمیل اطلاع‌رسانی QHEPS استفاده نمایند.

## اطلاعات کاربری

۱. در زمان نصب QHEPS با استفاده از نام دامنه (Domain Name)، تعداد کاراکترهای نام کامپیوتر نباید بیش از ۱۵ کاراکتر باشد.

۲. همگام‌سازی اکتیو دایرکتوری (AD)

الف) در زمان استقرار کلاینت QHEPS، فایروال ویندوز باید خاموش باشد.

ب) همگام‌سازی تمام کنترلر دامنه در زمان برپایی همگام‌سازی اکتیو دایرکتوری توصیه نمی‌شود. در عوض می‌توانید تنها گروه‌هایی که شامل کامپیوترها می‌باشند را همگام‌سازی کنید.

۳. کنترل ابزار

اگر دستگاه USB مجاز و رمزنگاری شده، فرمت شود، از آن پس دستگاه شما مانند یه دستگاه غیرمجاز شناسایی می‌شود. در این مورد، مدیر باید ابزار مجدداً به Device Control افزوده و سیاست خاص خود را اعمال نماید.

۴. به علت تنظیمات امنیت بالا (High Security) در اینترنت اکسپلورر (IE) سیستم عامل‌های سرور، ممکن است برخی از صفحات وب به خوبی نمایش داده نشوند. توصیه می‌شود برای مشاهده بهتر کنسول وب QHEPS گام‌های زیر را در سیستم عامل‌های ویندوز سرور انجام دهید.

الف) مرورگر IE را باز کنید.

ب) بروید به Tools/Settings > Internet Options > Advanced

ج) تیک چک‌باکس‌های زیر را بردارید:

- Do not save encrypted pages to disk.
- Empty Temporary Internet Files folder when browser is closed.

د) گزینه «Play animations in web pages\*» که در زیر Multimedia Settings

است را تیک کنید.

ه) تنظیمات را اعمال (Apply) کنید.



۵. در سیستم عامل (Windows Small Business Server)، به علت ممکن است به علت تنظیمات (ESC) Enhanced Security Configuration در IE، برخی از صفحات بازشونده (popup) باز نشوند. برای اجازه باز شدن این پنجره‌ها لطفاً تنظیمات زیر را انجام دهید:

الف) Server Manager Tool را اجرا کنید.

ب) بر روی «Configure IE ESC» که در سمت راست Server Manager Tool در بخش Security Information قرار دارد کلیک کنید

ج) گزینه IE ESC را خاموش کنید.

د) تنظیمات را Apply کنید.

۶. برای استفاده از مرورگر سندباکس (Browser Sandbox) باید ویژگی Secure Boot را خاموش کنید. ویژگی Secure Boot را می‌توانید از طریق پیکربندی بایوس (BIOS) سیستم غیرفعال (disable) کنید.