

محدودیت مدیریت یک گروه Seqrite Endpoint Security

چطور می توانیم مدیریت اندپوینت یک گروه از کلاینتها را تعیین کنیم؟

امکان کلاس بندی و گروه بندی کلاینتها، بر اساس نظر مدیر امنیت سازمان، و تفکیک مدیریت امنیت کلاینت ها بر اساس شبکه یکی از ویژگی های جدید اندپوینت سکيوریتی سکورایت کوییک هیل می باشد. همچنین امکان تعریف کاربران مدیر اندپوینت بر اساس مدیر (Administrator) و گزارش گیر (Report only) وجود دارد. سطح ادمین به دو صورت زیر قابل سیاستگذاری می باشد:

الف) ادمین ارشد (Super Admin) که امکان مدیریت و گزارش گیری از همه کلاینتها، گروه ها و پالیسی ها را خواهد داشت.

ب) ادمین گروه خاص: امکان محدود کردن تنظیمات فقط برای یک یا چند گروه خاص و فعالیتهای قابل اعمال برای آنها وجود دارد.

به عنوان مثال، یک سازمان دارای دفتر مرکزی و تعداد واحد می باشد. علاقه ای به استفاده از متدهایی مانند Slave/ Secondary Server برای مجزا سازی اندپوینت ها وجود ندارد. می خواهیم همه کلاینتها و گروهها بر روی یک سرور مدیریت شوند. اما هر واحد (شعبه) یک ادمین دارد که مایلیم مدیریت کلاینتهای آن واحد را به ادمین محلی تفویض کنیم. برای این کار فرایند زیر را انجام می دهیم:

۱. وارد کنسول مدیریت تحت وب EPS می شویم:

<https://IP-Server:9108>

۲. از منوی بالای صفحه Admin Settings را انتخاب و منوی Manage User را انتخاب می کنیم.

۳. بر روی دکمه Add User کلیک می کنیم.

Seqrite Endpoint Security 7.4 Total

Welcome Administrator | Admin Settings | Support | Help | Logout

Home Clients Settings Reports

Admin Settings

Server Clients

Change Password
Change Email Address
Notification
SMTP Settings
Manage Devices
Data Loss Prevention
Redirection
Manage Users
Internet Settings
Patch Management
General

Manage Users

In this section, you can create users of Administrator, Group Administrator and Report Viewer level. The Super Admin can edit, delete or disable its subordinate users.

Add User

User	User Type	User Status
Administrator	Super Admin	Enabled

۴. اطلاعات خواسته شده را تکمیل می کنیم:

(۱) نام کاربری برای ادمین جدید که قرار است فقط یک گروه را مدیریت کند.

(۲) و (۳) رمز عبور و تکرار رمز عبور برای ادمین گروه

(۴) آدرس ایمیل ادمین

(۵) نوع حساب کاربری که گزینه **Group Administrator** را انتخاب می کنیم.

(۶) برای میزان دسترسی مدیر گروه بر روی کلاینتهای آن گروه، بر روی **Configure** کلیک می کنیم. تنظیمات و اقداماتی که ادمین گروه قادر خواهد بود بر روی گروه خود اعمال کند را تعیین می کنیم.

(۷) با انتخاب گزینه **Enable** وضعیت کاربر را فعال می کنیم.

Add User X

User name: **1**

New Password: **2**

Confirm Password: **3**

Email Address: **4**

Type: **5** **6** [Configure](#)

User Status: **7**

Configure Access Rights X

Select the policy settings from the following which will be accessible to the Group Administrator:

<input checked="" type="checkbox"/>	Settings
<input checked="" type="checkbox"/>	Scan Settings
<input checked="" type="checkbox"/>	Email Settings
<input checked="" type="checkbox"/>	External Drives Settings
<input checked="" type="checkbox"/>	IDS/IPS
<input checked="" type="checkbox"/>	Firewall
<input checked="" type="checkbox"/>	Web Security

بعد از تکمیل فرم ها و Apply کردن، ادمین جدید گروه ساخته می شود.

Manage Users

In this section, you can create users of Administrator, Group Administrator and Report Viewer level. The Super Admin can edit, delete or disable its subordinate users.

Add User

User	User Type	User Status	
Administrator	Super Admin	Enabled	
UnitMan	Group Administrator	Enabled	Edit Delete

۵. اکنون باید گروه یا گروه های موردنظر را به ادمین گروه جدید اختصاص دهیم. برای اینکار از مسیر زیر اقدام می کنیم:

Client > Group Manager

انتخاب گروه مورد نظر و کلیک راست بر روی نام آن و انتخاب گزینه Assign Group Administrator و کلیک بر روی نام ادمین گروه موردنظر.

Welcome Administrator | Admin Settings | Support | Help | Logout

Seqrite Endpoint Security 7.4 Total

Home Clients Settings Reports

Clients

Client Status Client Action Client Deployment Manage Groups Manage Policies Assets

In this section, you can create groups and subgroups to manage endpoints. Right click on any Group or Endpoint to see the operations that you can perform.

Endpoint name/IP Import Export .csv

Endpoint Name	Group	Policy	Domain	IP Address
WIN-EN9EU7HH0E3	Server	stalone	FANOOS	

اکنون ادمین گروه می تواند با مراجعه به مرورگر خود و آدرس کنسول مدیریتی و با نام کاربری و رمزعبور جدید خود لاگین کرده و گروه خود را مدیریت کند.

خاتمه

کوییک هیل به عنوان یکی از محصولات امنیتی معتبر، با دارا بودن موتور و برخی ویژگی‌های امنیتی منحصر بفرد توانسته شرکتها و سازمانهای بزرگ جهانی (مانند شرکت تویوتا) را به خود جلب نماید. سرعت بالای اسکن، قدرت ویروس شناسی بالا، ویژگی‌های پیشگیرانه امنیتی و پشتیبانی عالی، کوییک هیل را به یکی از ۵ آنتی ویروس برتر جهانی تبدیل کرده است.

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

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

راه‌اندازی Update Server رسمی و HoneyPot در ایران (ظرف غسل 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 ویروس شناسی می‌باشد.

برای دریافت اطلاعات بیشتر از جوایز، تاییدیه‌ها، سایر محصولات و توانمندی‌های کوییک هیل به وبسایت <http://quickheal.co.ir> مراجعه و یا با شماره ۰۲۱-۷۷۱۴۲۵۲۶ تماس حاصل فرمایید.