FORTINET

آموزش فورتی آنالایزر

مترجم: اشکان پزشکی

این اثر را تقدیم میکنم به مادر و برادر عزیزم؛

که عالمانه به من آموختند چگونه در عرصه زندگی ایستادگی را تجربه کنم...

چرا این اثر ترجمه شد؟

کمپانی فورتی‌نت یکی از بزرگترین شرکت‌های تولید کننده تجهیزات امنیتی در دنیا است. تنوع محصولات این شرکت شهره عام و خاص است. در هر زمینه‌ای محصولی تولید کرده که از هر نظر مورد تقدیر و تحسین منتقدان و طرفدرانش می‌باشد. تولیدات این شرکت در ایران طرفداران بسیار زیادی داشته و تحریم های آمریکا نتوانسته تاثیری بر میزان محبوبیت این دستگاه‌ها در نزد ادمین های شبکه بگذارد. بیشتر سازمان‌ها و شرکت‌های بزرگ ایرانی از دستگاه‌های این برند استفاده می‌کنند. با توجه به اهمیت لاگ گیری در شبکه‌های کامپیوتری و آنالیز لاگ‌های بدست آمده جهت ردیابی و جلوگیری از تهدیدات امنیتی یکی از تجهیزات مورد استفاده و مشهور برند فورتی نت در ایران دستگاه فورتی آنالایزر می‌باشد. دستگاهی با ساختاری ساده و کارایی فوق العاده است. با کمی جستجو در اینترنت متوجه شدم که هیچ منبع فارسی جهت استفاده برای این دستگاه وجود نداشته و فقط به صورت پراکنده مطالبی خیلی خلاصه از این تجهیز وجود دارد؛ حتی کلاس‌های آموزشی برای کاربری و راه‌اندازی دستگاه وجود ندارد. با حمایت مالی و معنوی شرکت پردیس پارس توانستم کتاب را ترجمه و تجربه لازم در استفاده از دستگاه را بدست بیاورم. به خوانندگان عزیز کتاب توصیه می‌کنم برای درک مطالب بیان شده در کتاب حتماً آشنایی ابتدایی با مفاهیم شبکه‌های کامپیوتری داشته باشند.

امید که ترجمه این کتاب مورد توجه شما دوستداران عزیز واقع گردد.

درباره مترجم:

بنده اشکان پزشکی متولد تهران هستم. تحصیلات دوره کاردانی و کارشناسی خود را در رشته کامپیوتر خوانده و در مقطع فوق لیسانس رشته مدیریت فناوری اطلاعات را انتخاب کردم. بعد از اتمام دانشگاه علاقه زیادی به شبکه‌های کامپیوتری پیدا کرده و با حضور در کلاس های مختلف آموزشی و زیرنظر اساتید بزرگوار این رشته و راهنمایی دوستان توانستم کار خود را آغاز نمایم. ابتدا مدارک مرتبط با مایکروسافت را اخذ نموده و پس از آن در حوزه سیسکو مطالعاتی داشتم. سپس به مجازی سازی علاقه مند شده و در این زمینه درکلاس‌های مختلفی شرکت کرده و کتاب های زیادی مطالعه نمودم. در بحث سرورها مطالعاتی دارم و ...

از همان ابتدا اعتقاد داشتم زمانی که دانشی به اشتراک گذاشته می‌شود مسلما پیشرفتی افزون به همراه خود ایجاد خواهد کرد. بنابراین تمام مطالب و تجربیات خود را در سایت‌های مختلف به اشتراک می‌گذارم. به فراخور کار و تجربه ای که داشتم تصمیم گرفتم برای اولین بار کتاب فورتی‌گیت را به زبان فارسی ترجمه کنم که خوشبختانه بسیار مورد استقبال قرار گرفت. در تجربه دوم کتابی با نام نکات امنیتی ویندوز ۱۰ را ترجمه کردم. مهر و لطف شما عزیزان سبب شد که کتاب سوم را با قدرتی وصف ناپذیر ترجمه کرده و برای اولین بار مرجع کامل کتاب آموزش دسکتاپ مجازی را به زبان فارسی ارائه نمایم که استقبال از آن برای خود بنده غیرقابل باور بود. تمام آثار ترجمه بنده به صورت رایگان در اینترنت وجود داشته و می‌توانید از آنها بدون محدودیت استفاده نمایید.(دانلود کتاب فارسی مجازی سازی دسکتاپ و دانلود کتاب آموزش فورتی‌گیت به زبان فارسی از طریق سایت پردیس پارس امکان‌پذیر می باشد)

در این اثر سعی کردم ساده‌ترین کلمات تخصصی را بکار برده و استفاده از لغات پیچیده بپرهیزم. در مواردی هیچ معادل فارسی برای کلمه پیدا نکرده و اصل لغت را عینا در متن بکار برده‌ام. هر گونه خطای مفهومی که در متن کتاب مشاهده شود برعهده مترجم می‌باشد. همچنین آخرین نسخه مجازی فورتی آنالایزر از طریق این لینک قابل دانلود می‌باشد تا حین مطالعه کتاب بتوانید با امکانات دستگاه به صورت عملی کار نمایید.

این کتاب نیز مانند سایر کتاب های بنده به صورت رایگان در اینترنت در دسترس عموم قرار خواهد گرفت. اما اگر خوانندگانی هستند که تمایل دارند به صورت داوطلبانه کمک نمایند به اطلاع می‌رساند که اینجانب عضو گروه خیریه‌ای با نام مهراندیشان هستم که در زمینه کمک برای تحصیل دانش آموزان مناطق محروم و مرزنشین فعالیت می‌کنیم. کمک‌های شما می‌تواند به حساب این گروه واریز تا صرف کمک‌های انسان دوستانه در جهت تحصیل دانش آموزان مناطق محروم و مرزنشین گردد.

جهت ارائه پیشنهادات و انتقادات خود می‌توانید از طریق آدرس های زیر با من در تماس باشید.

بهمن ماه ۱۳۹۷

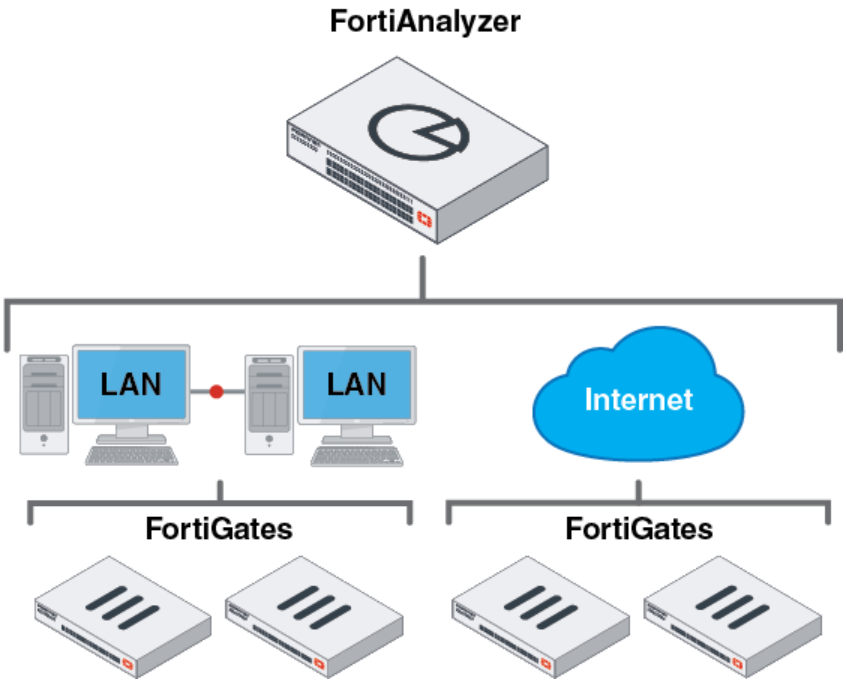
Contents

معرفی

فورتی آنالایزر پلتفرمی در جهت ادغام لاگ‌های شبکه ای، تجزیه و تحلیل آنها و گزارش از یک سیستم می‌باشد. این موارد تاثیر بسزایی در بالا بردن دانش امنیتی ادمین‌ها در مورد رخدادهای درون شبکه‌ای دارد. فورتی آنالایزر تلاش‌های مرتبط با نظارت‌ها را به حداقل رسانده و از سیاست‌های پذیرفته شده سازمانی تبعیت می‌نماید. توسط این وسیله می‌توانید الگوهای حملات را شناسایی کرده و بهترین پالیسی‌های امنیتی را تدوین نمایید. سازمان شما در هر سطح و اندازه‌ای که باشد از یک دستگاه امنیتی مرکزی بهره مند می‌شود که رخدادهای امنیتی را ثبت کرده، گزارشگیری می‌کند، محتواها را آرشیو کرده، داده کاوی‌ها را انجام داده و فایل‌های مخرب را شناسایی می‌نماید.

فورتی آنالایزر قابلیت‌های پیشرفته‌ای در جهت شناسایی تهدیدات همراه با انعطاف پذیری بالا در تغییرات بوجود آمده به شما ارائه می‌دهد. فورتی آنالایزر گزارش‌های سطح بالایی از حالت سفارشی سازی بر اساس نیازهای تجاری ، ادغام لاگ‌ها بر اساس ساختار سلسله مراتبی، توپولوژی ورود به سیستم‌ها فراهم می‌کند. امکان پیاده‌سازی فورتی آنلایزر به صورت فیزیکی یا مجازی برای جمع آوری داده ها، آنالیز جغرافیایی و داده‌های امنیتی به ترتیب زمانی وجود دارد.

رخدادها و لاگ‌های اطلاعاتی از دستگاه‌های فورتی‌نت و سایر دستگاه‌های جانبی جمع آوری شده و در یک مرکز واحد تجمیع می‌گردد. این کار سبب سادگی و ثبت تمام شرایط امنیتی در یک مکان مشخص می‌شود. پلتفرم فورتی آنالایزر دیتاها را بر اساس ضوابط و قوانین تعریف شده و با توجه به پیروی از سیاست‌های کلی سازمانی کپچر کرده و حریم خصوصی افراد را حفظ می‌کند.



حالت Collector:

زمانی که فورتی آنالایزر در این حالت کار می‌کند وظیفه اصلی آن ارسال لاگ‌ها از دستگاه‌های متصل به یک آنالیزر و آرشیو لاگ‌ها می‌باشد. در عوض ثبت لاگ‌ها در دیتابیس، به صورت فرمت باینری و دست نخورده در کالکتور باقی می‌ماند. در این حالت بیشتر امکانات غیرفعال می‌باشد.

مقایسه امکانات کالکتور و آنالایزر:

Feature	Analyzer Mode	Collector Mode
Device Manager	Yes	Yes
FortiView/LogView	Yes	No
Event Management	Yes	No
Monitoring devices	Yes	No
Reporting	Yes	No
System Settings	Yes	Yes
Log Forwarding	Yes	Yes

همکاری بین آنالایزر و کالکتور:

امکان پیاده‌سازی حالت آنالایزر و حالت کالکتور بر روی دو دستگاه مختلف فورتی آنالایزر وجود داشته و این دو دستگاه می‌توانند با هم کار کنند و روند کلی دریافت لاگ، آنالیزها و گزارشات را بهبود بخشند. آنالایزر امور مربوط به دریافت لاگ‌ها را به کالکتور میسپارد. با این کار آنالایزر می‌تواند بر روی آنالیز دیتاها و ایجاد گزارشات درخواستی فوکوس کند این امر سبب می‌شود کارایی جمع آوری لاگ برای کالکتور به حداکثر برسد.

Administrative domains:

ADOMها وقتی فعال می‌شوند که در نظر داریم ادمین‌ها را به سایر زیرشاخه‌های ایجاد شده در دستگاه (سایر قسمت‌های ایجاد شده) محدود نماییم. برای دستگاه‌های فورتی‌نت که همراه با دامین‌های مجازی ارائه می‌شوند (VDOM) امکان محدود کردن دسترسی‌ها از یک VDOM خاص برای یک دستگاه وجود دارد.

فعال نمودن ADOMها سبب بروز اخطارهایی در سطح GUI و CLI می‌شود. جهت دسترسی به توابع و فرامین باید بعنوان ادمین سیستم لاگین کنید. اگر با ادمین به سیستم لاگین نمایید تمام دسترسی‌های مربوط به ADOMها را دارید. اگر با ادمین وارد نشده باشید بر اساس تنظیمات اعمال شده توسط administrator دسترسی‌های شما مشخص می‌گردد.

ذخیره‌سازی لاگ‌ها

فایل‌ها و لاگ‌ها بر روی دیسک‌های فورتی آنالایزر ذخیره می‌شوند. لاگ‌ها به صورت موقتی در دیتابیس SQL ثبت می‌گردند. امکان تعریف پالیسی دیتا و تنظیمات مربوط به مصرف دیسک‌ها برای دستگاه وجود دارد. این مجموعه تنظیمات

ذخیره‌سازی لاگ نامیده می‌شود. امکان پیکربندی تمام لاگ‌ها و تنظیمات ذخیره‌سازی فایل وجود دارد. بدون در نظر گرفتن تنظیمات ذخیره‌سازی لاگ این موارد به تمام لاگ‌ها اعمال می‌گردد.

دیتابیس SQL :

فورتی آنالایزر از ساختار Structure Query Language برای لاگ گیری و گزارش گیری پشتیبانی می‌کند. اطلاعات لاگ در دیتابیس SQL وارد شده تا جهت آنالیز و تحلیل در فورتی ویوو، لاگ ویوو و گزارش‌ها مورد استفاده قرار گیرد. دیتابیس‌های SQL به صورت ریموت پشتیبانی نمی‌شوند.

تنظیمات ذخیره‌سازی لاگ‌ها تعیین کننده مقدار فضای مورد استفاده دیسک برای دیتابیس SQL در فورتی آنالایزر می‌باشد. به صورت پیش فرض دیتابیس SQL غیرفعال است تا زمانی که فورتی آنالایزر درحالت Collector قرار بگیرد.

آرشیو کردن لاگ‌ها و تجزیه و تحلیل آنها :

لاگ‌ها در فورتی آنالایزر در یکی از شرایط زیر قرار دارند. البته توجه داشته باشید که پالیسی‌های شما است که مشخص می‌کند لاگ تا چه زمانی در هر مرحله باقی بماند.

- تحلیل لاگ‌ها: فهرست بندی در دیتابیس SQL و آنلاین بودن آنها
- لاگ‌های آرشیوی: فشرده‌سازی شده بر روی دیسک‌ها و آفلاین بودن آنها

در مرحله ایندکس گذاری، لاگ‌ها برای یک مدت زمان مشخص و به هدف تجزیه و تحلیل در دیتابیس SQL فهرست بندی می‌شوند. لاگ‌ها در فاز ایندکس گذاری در دیتابیس SQL به صورت آنلاین در نظر گرفته می‌شوند و جزئیات در مورد این لاگ‌ها در Log View، FortiView و صفحه Event Management کاملا قابل مشاهده می‌باشند؛ همچنین امکان ایجاد گزارش در مورد لاگ‌ها در بخش Reports وجود دارد. در مرحله فشرده‌سازی، لاگ‌ها برای یک مدت زمان مشخص به منظور نگهداری در دیسک‌های فورتی آنالایزر فشرده و آرشیو می‌شوند. لاگ‌ها در فاز فشرده‌سازی به صورت آفلاین درنظر گرفته می‌شوند و امکان مشاهده جزئیات به صورت آنی و بلافاصله وجود ندارد. همچنین در این مرحله امکان تولید گزارش درباره لاگ‌ها در صفحه Reports وجود ندارد.

با استفاده از دیتا پالیسی امکان کنترل کردن مقدار لاگ‌های آرشیوی و تحلیلی داده می‌شود.

دیتا پالیسی و حذف خودکار:

دیتاپالیسی‌ها در جهت کنترل مدت زمان نگهداری و فهرست بندی لاگ‌ها بکار می‌روند. وقتی ADOMها فعال می‌شوند، امکان انجام تنظیمات خاص برای هر ADOM وجود دارد و تنظیمات به تمام دستگاه‌هایی که در آن ADOM وجود دارد اعمال می‌گردد. وقتی ADOMها غیرفعال می‌شوند، تنظیمات به تمام دستگاه‌های مدیریت شده اعمال می‌گردد.

یک دیتاپالیسی مشخص می‌کند که:

- مدت زمانی که طول میکشد تا لاگ‌های تحلیل شده در دیتابیس فهرست بندی و نگهداری شوند. هنگامی که یک زمان برای منقضی شدن دیتاپالیسی مشخص می‌کنید لاگ‌ها به صورت خودکار از دیتابیس پاک شده اما به صورت فشرده در لاگ فایل باقی خواهند ماند.
- مدت زمانیکه لاگ‌های آرشیویی بر روی دیسک‌های فورتی آنالایزر باقی می‌ماند. وقتی که یک بازه زمانی جهت منقضی شدن دیتاپالیسی مشخص می‌کنید، لاگ‌های آرشیو شده از دیسک‌های فورتی آنالایزر پاک می‌شوند.

استفاده از دیسک برای آرشیو و تحلیل لاگ‌ها

امکان تعیین مقدار فضای موجود دیسک برای ذخیره کردن لاگ‌ها در فورتی آنالایزر وجود دارد. امکان تخصیص نسبت فضای ذخیره‌سازی جهت استفاده لاگ‌هایی که در دیتابیس SQL ایندکس شده‌اند و لاگ‌هایی که در یک فرمت فشرده قرار دارند بر روی دیسک‌های فورتی آنالایزر وجود دارد. همچنین می‌توانیم بر روی سرعت روند پر شدن نظارت داشته باشیم.

تـوجه کنید که لاگ‌های تحلیلی که در دیتابیس SQL ایندکس می‌شوند نیازمند فضای بیشتری نسبت به لاگ‌های آرشیوی هستند. (از دیتابیس SQL خالی می‌شوند اما به صورت فشرده بر روی دیسک‌های فورتی آنالایزر باقی می‌ماند.) میانگین لاگ ایندکس شده عدد ٤٠٠ بایت می‌باشد و متوسط لاگ فشرده شده ٥٠ بایت است. این اختلاف را در ذهن داشته باشید برای زمانی که نسبت ذخیره‌سازی برای لاگ‌های تحلیلی و آرشیوی را انجام می دهید.

وقتی ADOMها را فعال کردید می‌توانید برای هر ADOM تنظیمات به خصوصی را مشخص و به تمام دستگاه‌های موجود در آن ADOM اعمال نمایید.

وقتی ADOMها را غیرفعال می‌کنید، تنظیمات به تمام دستگاه‌های تحت نظارت اعمال می‌گردد.

Security Fabric

شناسایی یک گروه از دیوایس‌ها و نمایش تمام دستگاه‌ها در یک دسته به نام Device Manager توسط فورتی آنالایزر امکان پذیر می‌باشد. فورتی آنالایزر از Security Fabric پشتیبانی می‌کند بدین صورت لاگ دستگاه‌هایی که در یک Security Fabric گروه قرار دارند را آنالیز و ذخیره‌سازی می‌کند. در این شرایط تمام لاگ‌ها به یک دستگاه اصلی ارسال می‌شود.

امکان مشاهده وضعیت Loggingها بر روی تمام دستگاه‌هایی که در یک گروه Security Fabric قرار دارند وجود دارد.

فورتی آنالایزر اطلاعات داینامیک و متادیتا را فراهم می‌کند تا با Security Fabric تبادل داشته و از این دیتاها در FortiView و گزارش‌ها استفاده نماید. یک قالب گزارشی پیش فرض به شما اجازه می‌دهد تا کاربران جدید، دستگاه‌ها، برنامه ها، آسیب‌پذیری ها، تهدیدات و سایر موارد را از Security Fabric مانیتور نمایید.

مجموعه‌ای از ویجت‌های موجود بر روی داشبورد مروری خواهند داشت بر روی امتیازات ممیزی برای گروه فورتی‌گیت‌های متصل شده به فورتی آنالایزر همراه با بهترین توصیه‌ها در جهت کاهش خطرات امنیتی و آسیب‌پذیری‌هایی که ممکن است منجر به تهدید سیستم‌ها گردد.

اگر فورتی کلاینت جهت کنترل دستگاه بوسیله فورتی‌گیت بر روی endpoint نصب شده باشد، می‌توانید از دیتای جمع آوری شده در endpoint استفاده کرده و گزارش مناسبی تهیه نمایید.

داشبور NOC/SOC

فورتی آنالایزر داشبوردی مناسب برای Network Operations Center (NOC) یا Security Operations Center (SOC) ایجاد نموده است. داشبوردها شرایط بصری را برای فعالیت‌های بلادرنگ و وضعیت تاریخچه‌ای جهت تجزیه و تحلیل موثر اتفاقات شبکه‌ای و کنترلی بهبود میبخشند.

GUI

برای پیکربندی اغلب تنظیمات فورتی آنالایزر می‌توانید از محیط GUI استفاده نمایید. مواردی مثل تاریخ، زمان، نام دستگاه، ریبوت کردن، خاموش کردن و ... امکان پذیر است.

اتصال به GUI

دستگاه فورتی آنالایزر طوری طراحی شده است که امکان مدیریت و انجام تنظیمات از طریق GUI و CLI وجود دارد. این قسمت مراحل اتصال به دستگاه از طریق GUI را بیان می‌کند.

اتصال به GUI:

۱. بوسیله یک کابل اترنت از طریق کامپیوتر خود به دستگاه فورتی آنالایزر متصل شوید.

۲. کامپیوتری و دستگاه فورتی آنالایزر باید در یک subnet باشند تا امکان اتصال وجود داشته باشد.

   a. آدرس IP: 192.168.1.x

   b. Net mask:255.255.255.0

۳. در کامپیوتر خود مرورگری را باز کرده و آدرس https://192.168.1.99 را وارد نمایید.

٤. در فیلد Name از نام کاربری admin استفاده کرده و مقدار پسورد را خالی بگذارید. سپس بر روی Login کلیک نمایید.

۵. اگر ADOMها فعال باشند، صفحه ADOM جهت انتخاب نمایش داده می‌شود. بر روی یک ADOM کلیک کرده و آن را انتخاب نمایید. صفحه اصلی فورتی آنالایزر برای شما نمایش داده می‌شود.

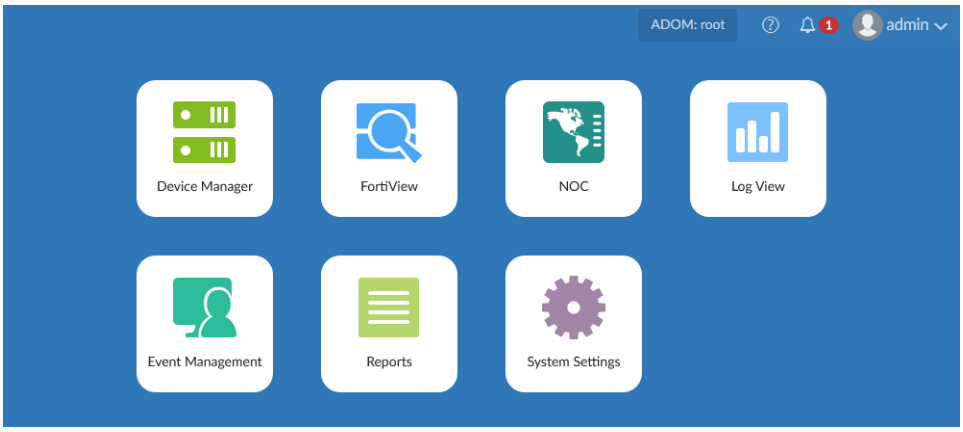
٦. بر روی یکی از tileها (کاشی ها، مدل ویندوز ۸ یا ویندوز ۱۰) کلیک نمایید تا به آن قسمت بروید. برای مثال با کلیک بر روی Device Manager به صفحه Device Manager خواهیم رفت.

اگر URL که وارد کردید درست است و هنوز امکان دسترسی به GUI وجود ندارد باید دست به کار شوید و یک خط route به صورت استاتیک بنویسید.

بعد از اولین لاگین، باید یک اکانت ادمین برای خود ایجاد کرده و پروفایل Super_User را به آن اکانت تخصیص بدهید. سپس با استفاده از اکانت جدید ادمینی که ایجاد کردید بر روی دستگاه فورتی آنالایزر لاگین می‌کنید.

نگاهی کلی بر GUI:

وقتی به GUI فورتی آنالایزر لاگین می‌کنید، صفحه زیر به صورت tile (کاشی) برای شما نمایش داده می‌شود:



یکی از tileهای نمایش داده شده را انتخاب کنید تا صفحه مربوطه باز شود. با توجه به دسترسی‌های کاربر کنونی گزینه‌های متفاوتی وجود دارد.

اضافه کردن، مدیریت دستگاه‌ها و VDOM ها	Device Manager
خلاصه‌ای از دیتا لاگ‌ها که در فرمت‌های گرافیکی مشاهده می‌شود. برای مثال، امکان مشاهده برترین تهدیدات موجود در شبکه، بالاترین مصرف ترافیک شبکه بر اساس مبدا، بالاترین مصرف ترافیک شبکه بر اساس مقصد، برای هر	FortiView

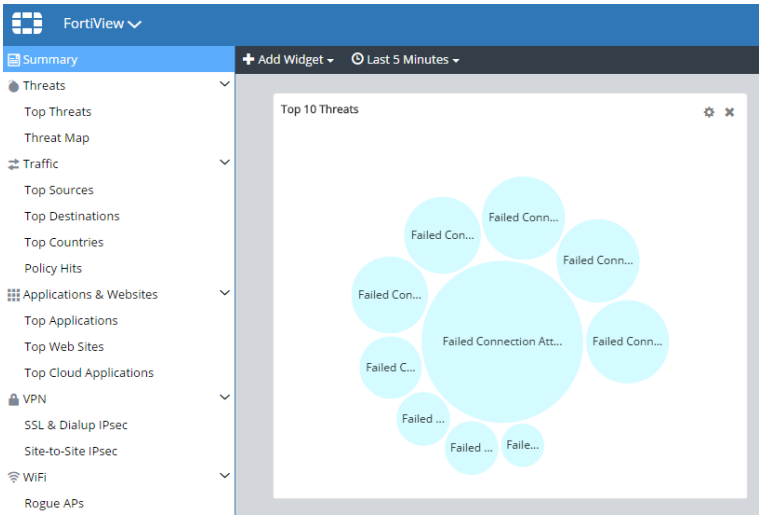
خلاصه‌ای که مشاهده می‌کنید جزئیات دقیق آن نیز موجود می‌باشد.	
مشاهده امنیت شبکه، امنیت **WiFi** و عملکرد سیستم در لحظه. امکان انتخاب مواردی که قرار است مانیتور شود وجود دارد. همچنین می‌توانید داشبوردهای دلخواه ایجاد نمایید.	NOC
برای مدیریت دستگاه‌ها از این قسمت استفاده می‌کنیم. در این صفحه امکان مشاهده، دانلود، **import** و پاک کردن لاگ‌ها وجود دارد. در این قسمت می‌توانید دیدگاه‌های سفارشی و گروه‌های لاگ ایجاد نمایید.	Log View
پیکربندی و مشاهده رخدادها برای لاگ دستگاه‌ها در این قسمت صورت می‌پذیرد.	Event Management
ایجاد گزارش‌ها در این قسمت انجام می‌شود. امکان پیکربندی قالب‌های گزارشی، زمانبندی و پروفایل‌های خروجی و مدیریت چارت‌ها و دیتابیس‌ها در این مرحله انجام می‌گردد. این صفحه وقتی دستگاه در حالت **Collector** قرار دارد موجود نمی‌باشد.	Reports
مواردی مثل اینترفیس‌های شبکه، تعریف و تغییر در وضعیت ادمین‌ها، زمان سیستم، تنظیمات سرور و سایر موارد در این بخش انجام می‌شود. همچنین می‌توانید تعمیرات و عملیات سیستمی را انجام دهید.	System Settings
اگر **ADOM**ها فعال باشند، **ADOM** درخواستی از لیست انتخاب می‌شود. از **ADOM**های موجود و از طریق منوی **ADOM** بنا به دسترسی شما فعال می‌گردد.	ADOM
این قسمت مربوط به راهنمای آنلاین فورتی آنالایزر می‌باشد. همچنین اطلاعاتی در مورد دستگاه در اختیار شما می‌گذارد. **(Product, Version, and Build Number)**	Help

Notification	برای نمایش لیستی از اعلان‌ها بر روی این گزینه کلیک کنید. با انتخاب یک اعلان از لیست اقدامی در مورد آن موضوع صورت می‌گیرد.
Admin	با کلیک بر روی این گزینه کلمه عبور تغییر داده می‌شود یا از محیط **GUI** خارج می‌شوید.

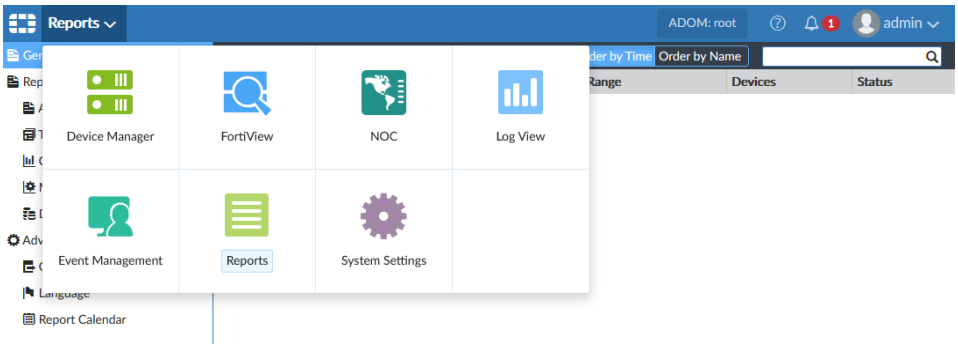
Panes

به طور کلی، صفحات چهار قسمت اصلی دارند: بنر، نوار ابزار، منوی درختی و پنجره محتوا.

Banner	در بالای صفحه قرار گرفته است شامل دکمه هوم (لوگوی فورتی‌نت)، **tile** منو، **ADOM** منو (وقتی فعال باشد)، منو ادمین، اعلان‌ها و دکمه **help** می‌باشد.
Tree menu	در گوشه سمت چپ صفحه قرار گرفته است که شامل منوهایی برای انتخاب صفحات است. در **Device Manager** موجود نمی‌باشد.
Content pane	شامل ویجت‌ها، لیست ها، گزینه‌های پیکربندی، منو یا گزینه‌های انتخابی می‌باشد. اغلب امور مدیریتی در این **content pane** انجام می‌شود.
Toolbar	مستقیم در بالای پنجره کانتنت قرار دارد; شامل گزینه‌هایی برای مدیریت **Content** در این قسمت است.



برای جابجایی بین صفحات، یا انتخاب دکمه هوم برای بازگشت به صفحه اصلی بروید یا tile منو را انتخاب نمایید.



تم‌های رنگی

برای محیط GUI فورتی آنالایزر می‌توانید تم‌های رنگی مختلفی را انتخاب نمایید. برای مثال، یک رنگ را انتخاب کنید، رنگی مثل آبی یا زرد یا حتی می‌توانید یک عکس را انتخاب نمایید. عکس‌هایی مثل تابستان یا پاییز.

حالت تمام صفحه

امکان مشاهده چندین و چند پنجره در حالت تمام صفحه وجود دارد. وقتی که پنجره‌ای در حالت تمام صفحه قرار دارد، منوی درختی که در سمت چپ صفحه قرار دارد ناپدید می‌شود.

با کلیک بر روی دکمه Full Screen بر روی نوار ابزار به حالت تمام صفحه می‌روید، و با زدن دکمه Esc بر روی صفحه کلید از از حالت تمام صفحه خارج می‌شوید.

سوئیچ کردن بین ADOM ها

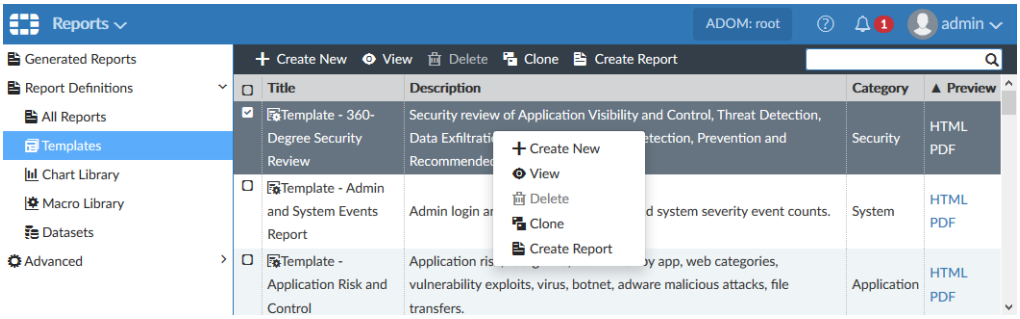
وقتی ADOMها فعال شوند، امکان جابجایی بین آنها وجود دارد بدین صورت که ADOM دلخواه را از منوی ADOM در بنر انتخاب کرده و به آن ADOM می‌روید.

بر اساس دسترسی‌های اکانت شما امکان ورود یا تغییرات در ADOMها وجود دارد. همچنین ممکن است امکان دسترسی به تمام ADOMها وجود نداشته باشد.

استفاده از راست کلیک در منو

این گزینه بعضی اوقات در منو با استفاده از راست کلیک موجود می‌باشد. راست کلیک یک آیتم در پنجره content است و یا در بعضی از منوهای درختی وجود دارد.

در مثال زیر که در پنجره Reports است، با راست کلیک کردن بر روی یک تمپلیت و انتخاب Create New، View، Clone یا Create Report با امکان راست کلیک کردن بیشتر آشنا می‌شوید.



آواتارها

وقتی لاگ‌ها از فورتی کلاینت به فورتی آنالایزر ارسال می‌شوند، در ستون مبدا در پنجره‌های Log View و FortiView یک آواتار برای هر کاربر نمایش داده می‌شود. فورتی آنالایزر آواتار را نمایش می‌دهد به شرطی که پیش نیازهای زیر را فراهم کنیم:

- فورتی کلاینت توسط فورتی‌گیت مدیریت شود یا FortiClient EMS با ورود به فورتی آنالایزر فعال شده باشد.
- فورتی کلاینت لاگ‌ها و یک عکس از هر کاربر را برای فورتی آنالایزر ارسال می‌کند.

اگر فورتی آنالایزر نتواند عکس تعریف شده را مشخص کند، به صورت کلی، آواتار را خاکستری نمایش می‌دهد.

امکان انتخاب یک آواتار برای ادمین‌ها وجود دارد.

نمایش دادن یا مخفی کردن کلمات عبور

در بعضی موارد امکان نمایش دادن یا مخفی کردن کلمات عبور وجود دارد. وقتی می‌توانید پسورد را مشاهده کنید که بر روی آیکون Toggle کلیک نمایید.

زمانی پسورد به حالت مخفی و ستاره برمی‌گردد که آیکون Toggle را به صورت زیر تغییر شکل دهید.

ملاحضات امنیتی

مواردی که با رعایت آنها از دسترسی‌های غیرمجاز جلوگیری کرده و یا دسترسی به محیط GUI را کنترل شده و محدود می‌نمایید.

محدودیت دسترسی به محیط GUI بوسیله هاست مورد اطمینان

برای جلوگیری از دسترسی غیرمجاز به محیط GUI امکان انجام تنظیماتی برای اکانت‌های ادمین با تراست هاست‌ها وجود دارد. با پیکربندی هاست‌های مورد اطمینان، کاربرانی که ادمین هستند فقط در صورتی می‌توانند به GUI لاگین کنند که کامپیوتری که با آن کار می‌کنند بعنوان تراست هاست در لیست تعریف شده باشد. برای هر اکانت ادمین تا ۱۰ هاست تراست شده قابل تعریف است.

سایر ملاحظات امنیتی

سایر موارد امنیتی برای ایجاد محدودیت در دسترسی به محیط GUI فورتی آنالایزر شامل موارد زیر است:

- پسورد اکانت‌های ادمین را پیچیده انتخاب نمایید.
- پیکربندی اکانت‌های ادمین با استفاده از RADUIS، LDAP، TACACS صورت پذیرد.
- پیکربندی اکانت ادمین طوری انجام شود که دسترسی فقط به ADOMهای خاص و مورد درخواست امکان پذیر باشد.

ریستارت و خاموش کردن

جهت ریستارت کردن دستگاه از طریق GUI کافی است:

۱. به مسیر System Settings> Dashboard بروید.

۲. از قسمت Unit Operation بر روی دکمه Restart کلیک کنید.

۳. جهت ثبت در لاگ رخدادها پیغامی یادداشت کنید که دلیل ریستارت کردن دستگاه چیست. حال بر روی OK کلیک کنید تا دستگاه ریستارت شود.

ریستارت کردن فورتی آنلایزر از طریق CLI:

۱. از طریق CLI، یا از طریق ویجت کنسول CLI، دستور زیر را وارد کنید:

```
execute reboot
The system will be reload.
Do you want to continue? (y/n)
```

۲. Y را بزنید تا دستگاه ریستارت شود.

خاموش کردن فورتی آنالایزر از طریق GUI :

۱. به مسیر System Settings> Dashboard بروید.

۲. از قسمت Unit Operation بر روی دکمه Shutdown کلیک کنید.

۳. جهت ثبت در لاگ رخدادها پیغامی یادداشت کنید که دلیل ریستارت کردن دستگاه چیست. حال بر روی OK کلیک کنید تا دستگاه خاموش شود.

خاموش کردن دستگاه از طریق CLI :

۱. از طریق CLI، ویجت کنسول CLI، دستور زیر را وارد نمایید:

```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```

۲. برای ادامه کار Y را زده و منتظر بمانید تا دستگاه خاموش شود.

ریست کردن دستگاه فورتی آنالایزر:

۱. از طریق CLI، دستور زیر را وارد کنید:

```
Execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

۲. برای ادامه کار Y را زده و منتظر بمانید تا تنظیمات دستگاه به حالت کارخانه‌ای برود و ریستارت شود.

ریست کردن لاگ‌ها و انتقال مجدد همه لاگ‌های SQL به دیتابیس:

۱. از CLI، دستور زیر را وارد کنید:

```
execute reset-sqllog-transfer
WARNING: This operation will re-transfer all logs into database.
Do you want to continue? (y/n)
```

۲. برای ادامه کار Y را بزنید. تمام لاگ‌های SQL دوباره به دیتابیس ارسال خواهد شد.

شروع کنیم

در این بخش اطلاعاتی در مورد انجام تنظیمات بر روی دستگاه فورتی‌گیت به شما می‌دهیم.

کاربران و سطح دسترسی

این بخش برای ادمین‌هایی تدوین شده که سطح دسترسی کاملی داشته و می‌توانند تمام صفحات مربوط به فورتی آنالایز را باز نمایند.

در فورتی آنالایزر، دسترسی‌های کنترلی توسط پروفایل ادمین‌ها داده می‌شود. ادمین‌هایی که پروفایل‌هایی با دسترسی محدود دارند امکان مشاهده و یا انجام بعضی دستورات را در محیط GUI ندارند.

اگر با اکانت ادمین لاگین کرده‌اید پروفایلی با نام super_user دارید که به صورت پیش فرض به شما تخصیص داده شده است. این کاربر با این پروفایل بالاترین سطح دسترسی را دارد.

راه اندازی اولیه

این بخش مروری اولیه‌ای دارد بر کارهایی که هنگام راه اندازی دستگاه انجام خواهید داد.

تنظیمات فورتی آنالایزر

۱. به محیط GUI متصل شوید.

۲. RAID مورد نظر خود را تنظیم نمایید، البته در صورتی که مدل خریداری شده از RAID پشتیبانی می‌کند.

۳. تنظیمات شبکه را انجام دهید.

اولین باری که IP آدرس فورتی آنالایزر را تغییر می‌دهید، اتصالاتان با دستگاه قطع می‌شود. جهت اتصال دوباره باید با IP جدیدی که تعیین کرده‌اید به دستگاه متصل شوید.

٤. ادمین دامین‌ها را مشخص نمایید.(دلخواه می‌باشد)

۵. تنظیمات مربوط به اکانت‌های ادمین را انجام دهید.

بعد از پیکربندی اکانت‌های ادمین، با استفاده از اکانت‌های جدید لاگین نمایید.

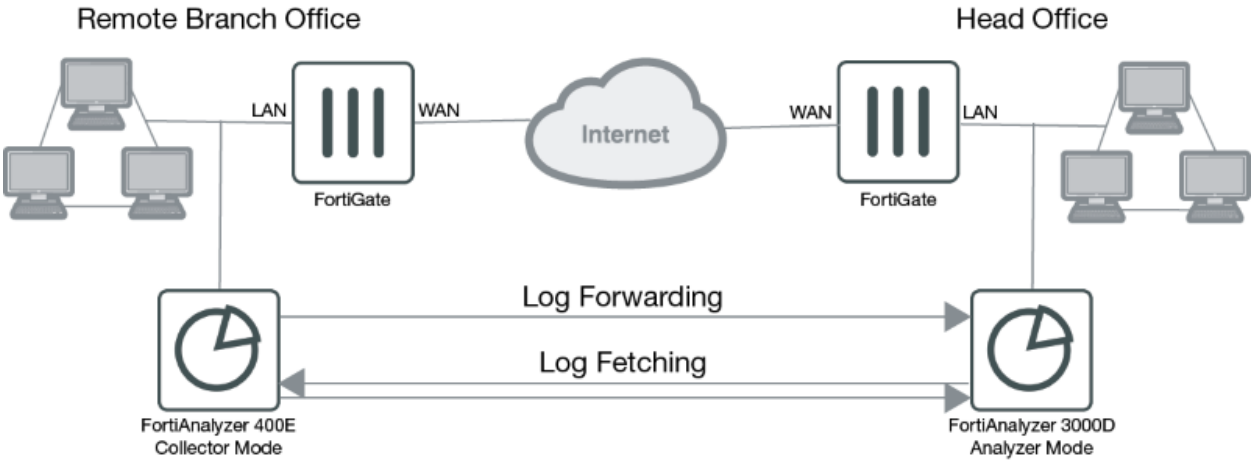
٦. دستگاه‌ها را به فورتی آنالایزر اضافه نمایید تا بتوانند لاگ‌های خود را ارسال کنند.

۷. شرایط و حالت عملیاتی که دستگاه در آن کار خواهد کرد را مشخص نمایید.

پیکربندی به صورت آنالایزر – کالکتور

در این قسمت در مورد چگونگی تنظیم و پیکربندی دو دستگاه فورتی آنالایزر توضیحاتی خواهیم داد که یکی از آنها در حالت آنالایزر و دیگری در حالت کالکتور در کنار هم کار می‌کنند. سناریو در دیاگرام زیر نمایش داده شده است. شرکت A شعبه‌ای در شهر دیگر دارد که در آن شعبه یک دستگاه فورتی‌گیت و یک دستگاه فورتی آنالایزر400E وجود دارد که این دستگاه در مد کالکتور تنظیم شده است. در دفتر مرکزی، یک دستگاه فورتی‌گیت و یک فورتی آنالایزر مدل 3000D

که در مد آنالایزر تنظیم شده موجود است. کالکتور لاگ‌هایی را که از فورتی‌گیت شعبه دریافت می‌کند به آنالایزر دفتر مرکزی ارسال می‌کند. این کار باعث می‌شود که ابتدا لاگ‌ها آنالیز و سپس گزارش‌های درخواستی ایجاد گردد. کالکتور جهت بایگانی و آرشیو لاگ‌ها مورد استفاده قرار می‌گیرد.



تنظیم و پیکربندی کالکتور

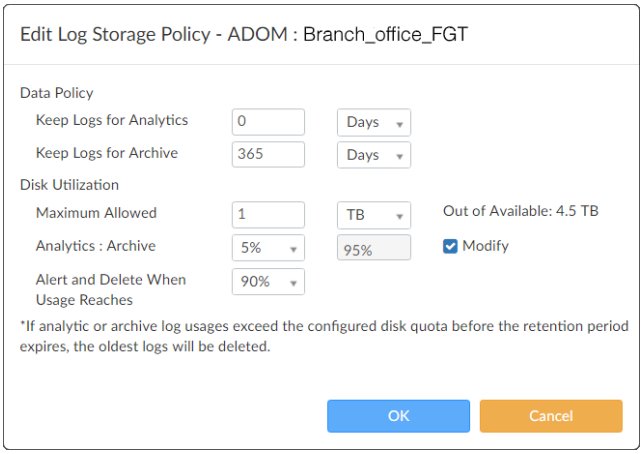
انجام تنظیمات کالکتور:

۱. مطمئن شوید که حالت دستگاه به صورت Collector است.

۲. برای حالت کالکتور پالیسی‌های مربوط به ذخیره‌سازی را مورد بازبینی و پیکربندی قرار دهید.

برای حالت کالکتور، بهتر است تخصیص بیشتر فضای دیسک در جهت لاگ‌های آرشیوی انجام پذیرد. از لاگ‌های آرشیوی برای مدت زمان طولانی نگهداری کنید چون احتمالا در زمان‌های آتی مورد استفاده قرار خواهند گرفت. بعد از انجام تنظیمات ابتدایی این امکان وجود دارد که میزان استفاده از فضای ذخیره شده را مانیتور نمایید.

تنظیمات زیر مثالی برای یک کالکتور می‌باشد:



۳. تنظیم فعال سازی ارسال لاگ‌ها از کالکتور به آنالایزر.

- Remote server Type را برای فورتی آنالایزر مشخص می‌کنیم.
- IP سرور را مشخص نمایید. این IP مربوط به آنالایزری است که کالکتور، لاگ‌ها را برای آن ارسال می‌کند.
- بر روی Select Device کلیک کنید و دستگاه فورتی‌گیتی که کالکتور لاگ‌ها را برای آن ارسال می‌کند را انتخاب نمایید.

تنظیمات پیش فرض ارسال لاگ‌ها از کالکتور به آنالایزر به صورت بلادرنگ Realtime می‌باشد. این در صورتی است که تمایل دارید کالکتور فایل‌ها را آپلود نماید. فایل‌هایی مثل DLP، قرنطینه آنتی ویروس، IPS و ...

تنظیمات آنالایزر

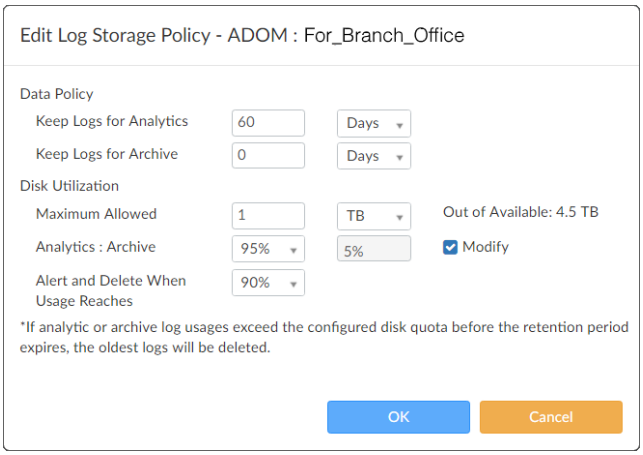
تنظیم کردن آنالایزر:

۱. مطمئن شوید که آنالایزر در حالت کالکتور قرار دارد.

۲. بررسی و پیکربندی به صورتی باشد که پالیسی ذخیره‌سازی برای حالت آنالایزر در نظر گرفته شود.

در حالت آنالایزر بیشتر فضای دیسک باید برای لاگ‌های تحلیلی و آنالیزی درنظر گرفته شود. ممکن است لاگ‌های آنالیز شده بین ۳۰ الی ۹۰ روز نگهداری شوند. بعد از تنظیمات اولیه، امکان مانیتور کردن مصرف استورج و تصمیم گیری در مورد وضعیت موجود وجود دارد.

تنظیمات زیر مثالی برای آنالایزر است.



۳. مطمئن شوید که سرویس تجمیع –ادغام– بر روی دستگاه فورتی آنالایزر فعال است. اگر فعال نیست، با استفاده از دستور زیر در محیط CLI آن را فعال نمایید:

```
Config system log-forward-service
        Set accept-aggregation enable
End
```

٤. اضافه کردن دستگاه فورتی‌گیت شعبه که کالکتور لاگ‌های آن را ارسال خواهد کرد.

اولین باری که فورتی‌گیت شعبه اضافه می‌شود، آنالایزر شروع به دریافت لاگ‌ها از کالکتور می‌کند.

گرفتن لاگ‌ها از کالکتور به آنالایزر

مواقعی است که تمایل دارید لاگ‌ها را از کالکتور به آنالایزر واکشی کنید. کالکتور نقش fetch سرور را بازی می‌کند و آنالایزر نقش fetch کلاینت را دارد.

مراحل بعدی

حالا که دستگاه راه اندازی شده و دریافت لاگ‌ها از دستگاه‌های دیگر آغاز شده است می‌توانید مانیتورینگ و تحلیل دیتاها را شروع کنید. این امکان وجود دارد که:

- مشاهده لاگ‌های جمع آوری شده توسط فورتی آنالایزر در Log View وجود دارد.
- مشاهده خلاصه‌ای از تهدیدات امنیتی، ترافیک‌ها و ... در FortiView وجود دارد.
- مشاهده صفحات مختلف از فعالیت‌های شبکه‌ای در NOC یا SOC وجود دارد.

- ایجاد و مشاهده رخدادها در Event Management وجود دارد.
- ایجاد و مشاهده گزارش‌ها در Reports وجود دارد.

شبکه

تنظیمات شبکه‌ای جهت پیکربندی پورت‌های دستگاه فورتی آنالایزر مورد استفاده قرار می‌گیرد. در این قسمت مشخص می‌شود که کدام پورت و با چه روشی ادمین‌ها می‌توانند به دستگاه فورتی آنالایزر دسترسی داشته باشند. در صورت نیاز، می‌توانید route استاتیک نیز اضافه نمایید.

پورت پیش فرض دستگاه Port 1 است. این پورت یک IP آدرس جهت انجام تنظیمات دستگاه دریافت می‌کند. شما می‌توانید چندین IP برای پورت‌های مختلف دستگاه در نظر بگیرید این امر سبب می‌گردد وضعیت امنیتی سیستم بهتر شود.

دسترسی ادمین‌ها می‌تواند از طریق IPv4 و IPv6 و در حالت‌های HTTPS،HTTP ، PING، SSH، Telnet، SNMP، Web Service صورت گیرد.

با استفاده از هاست‌های مطمئن (Trusted host) و ساخت اکانت‌های ادمین می‌توانید از دسترسی‌های غیرمجاز و تعریف نشده به محیط GUI جلوگیری نمایید. با تنظیم هاست‌های مطمئن، ادمین‌ها فقط در شرایطی می‌توانند در محیط GUI دستگاه لاگین کنند که بر روی کامپیوتری کار کنند که در Trusted host تعریف شده است.

تنظیمات اینترفیس‌های شبکه:

دستگاه‌های فورتی‌نت این قابلیت را دارند تا به هر کدام از اینترفیس‌های فورتی آنالایزر متصل شوند. سرورهای DNS باید در شبکه وجود داشته باشند تا دستگاه به آن وصل شود. بهتر است که دو عدد IP آدرس متفاوت داشته باشیم.

اعمال تنظیمات زیر به پورت توصیه می‌گردد:

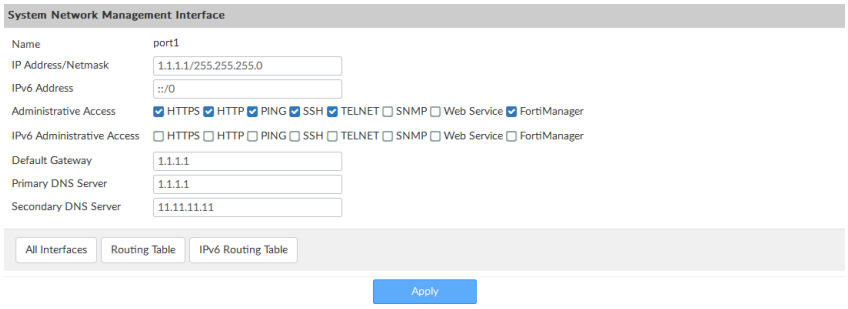
- از پورت ۱ برای ترافیک لاگ دستگاه استفاده کنید. سرویس‌های غیر ضروری را غیرفعال نمایید. سرویس‌هایی مثل Telnet،SSH ، Web Service و غیره.
- پورت دومی بعنوان دسترسی ادمین‌ها در نظر بگیرید و سرویس‌هایی مثل HTTPS، Web Service و SSH برای این پورت فعال کنید. بقیه سرویس‌ها را به صورت غیرفعال باقی بگذارید.

انجام تنظیمات پورت ۱:

۱. به مسیر زیر بروید:

System Settings> Network.

پنجره System Network Management Interface نمایش داده می‌شود.



۲. تنظیمات زیر را برای پورت ۱ اعمال نمایید، سپس بر روی Apply کلیک کنید تا تغییرات اعمال گردد.

Name	نمایش دهنده نام اینترفیس می‌باشد.
IP Address/Netmask	**IP** آدرس و **Netmask** مربوط به این اینترفیس است.
IPv6 Address	آدرس **IPv6** که با این اینترفیس مرتبط است.
Administrative Access	سرویس پروتکل‌هایی که ادمین اجازه استفاده از آنها را دارد. **HTTPS**، **HTTP**، **PING** و ...
Default Gateway	**Gateway** پیش فرضی که با این اینترفیس مرتبط است.
Primary DNS Server	**IP** آدرس اصلی **DNS** سرور است.
Secondary DNS Server	**IP** آدرس دومی **DNS** سرور است.

تنظیمات پورت دوم:

۱. به مسیر زیر بروید:

System Settings> Network

بر روی All interfaces کلیک کنید. لیست اینترفیس‌ها باز می‌شود.

۲. بر روی یک پورت دو بار کلیک کنید، بر روی یک پورت راست کلیک کرده سپس از منوی پاپ آپ باز شده Edit را انتخاب نمایید، پنجره Edit System Interface نمایش داده می‌شود.

۳. با توجه به نیاز تنظیمات مربوطه را انجام دهید.

٤. برای اعمال تغییرات بر روی OK کلیک کنید.

نام پورت، گیت‌وی پیش فرض و DNS سرورها از پنجره Edit System Interface قابل تغییر نمی‌باشند. در صورت نیاز می‌توانید به پورت یک نام مستعار اختصاص دهید.

غیرفعال کردن پورت ها

امکان غیرفعال کردن پورت وجود دارد. این امر به این دلیل انجام می‌شود تا از پذیرش ترافیک شبکه‌ای توسط پورت جلوگیری گردد.

غیرفعال کردن یک پورت:

۱. به مسیر System Settings> Network بروید و بر روی All Interfaces کلیک کنید. لیست مربوط به اینترفیس باز می‌شود.

۲. بر روی یک پورت دوبار کلیک کنید، بر روی یک پورت راست کلیک کرده و از منوی پاپ آپ باز شده گزینه Edit را انتخاب نمایید یا یک پورت را انتخاب کرده و سپس Edit را در نوار ابزار انتخاب نمایید. پنجره Edit System Interface نمایش داده می‌شود.

۳. در فیلد Status، بر روی گزینه Disable کلیک کنید.

٤. با کلیک کردن بر روی OK پورت غیرفعال می‌شود.

تغییرات در دسترسی‌های ادمین

دسترسی ادمین بر اساس پروتکل‌های مورد استفاده جهت اتصال به فورتی آنالایزر از طریق اینترفیس تعریف می‌شوند. گزینه‌هایی که موجود عبارت اند از:

HTTP, HTTPS, PING, SSH, TELNET, SNMP, Web Services, FortiManager

تغییر دسترسی ادمین:

۱. به مسیر System settings> Network بروید و بر روی All Interfaces کلیک کنید. لیست اینترفیس‌ها باز می‌شود.

۲. بر روی یک پورت دوبار کلیک کنید، بر روی یک پورت راست کلیک کرده و از پاپ آپ باز شده گزینه Edit را انتخاب کنید. پنجره Edit System Interface نمایش داده می‌شود.

۳. یک یا چند پروتکل دسترسی برای این اینترفیس با استفاده از IPv4 یا IPv6 انتخاب نمایید.

٤. برای اعمال تغییرات بر روی OK کلیک کنید.

استاتیک route

Routeهای استاتیک توسط جدول routeهای IPv4 و IPv6 مدیریت می‌شوند.

برای دسترسی به جداول routing کافی است به مسیر زیر بروید:

System Settings> Network> Routing Table

اضافه کردن استاتیک route:

۱. از جدول روتینگ قسمت IPv4 یا IPv6 ، بر روی نوار ابزار گزینه Create New را انتخاب کنید. پنجره Create New Network Route باز می‌شود.

۲. IP آدرس مقصد را وارد کنید در فیلدهایی که وارد می‌کنید Gateway حتما باید مقدار داده شود.

۳. اینترفیسی که به Gateway متصل می‌شود را از لیست وارد کنید.

٤. با کلیک بر روی OK یک استاتیک route ایجاد می‌کنید.

ویرایش استاتیک route

۱. از جدول routing، بر روی یک route دوبار کلیک کنید، راست کلیک بر روی route سپس از پاپ آپ باز شده Edit را انتخاب کنید یا یک route را انتخاب، سپس از نوار ابزار بر روی Edit کلیک کنید.

۲. تنظیمات را بر اساس درخواست‌های خود تغییر دهید. Route IDها قابل تغییر نمی‌باشند.

۳. با کلیک کردن بر روی OK تغییرات اعمال می‌شوند.

پاک کردن استاتیک route :

۱. از جدول routing، بر روی یک route کلیک راست کنید سپس از منوی پاپ آپ باز شده Delete را انتخاب کنید، یک route یا routeهایی را انتخاب کنید سپس از نوار ابزار بر روی Delete کلیک کنید.

۲. با انتخاب OK تمام routeهای انتخاب پاک خواهد شد.

مدیریت RAID

RAID به ما کمک می‌کند تا ذخیره‌سازی دیتاها را بر روی چندین دیسک انجام دهیم. همین امر سبب افزایش قابلیت اطمینان داده‌ها می‌شود. برای دستگاه‌های فورتی آنالایزر که دارای چندین دیسک می‌باشند امکان RAID بندی وجود دارد و این امکان سبب می‌شود تا با امکاناتی مانند افزایش ظرفیت، کارایی و در دسترس پذیری برخوردار شوید.

منوی RAID Management فقط در دستگاه‌هایی وجود دارد که از این قابلیت پشتیبانی می‌کنند.

پشتیبانی از سطوح RAID:

دستگاه‌های فورتی آنالایزر با چند هارددیسک از سطوح RAID زیر پشتیبانی می‌کنند:

Linear RAID

RAID بندی به صورت Linear به صورتی است که تمام هارددیسک‌ها در داخل یک دیسک مجازی بزرگ ترکیب می‌شوند. کل فضای موجود در این گزینه ظرفیت قابل استفاده تمام دیسک‌ها می‌باشد. وقتی از این مدل RAID بندی استفاده می‌کنید تغییر کارایی خیلی کمی وجود دارد. اگر هر کدام از درایوها fail شود تمام مجموعه درایوها غیرقابل استفاده می‌گردد تا زمانی که درایو خراب جایگزین شود. البته توجه داشته باشید که در این شرایط کل دیتا Lost خواهد شد.(تمام دیتاها از بین می‌رود!)

RAID 0

RAID بندی به صورت صفر چیزی شبیه به striping می‌باشد. دستگاه فورتی آنالایزر اطلاعات را به صورت مساوی بر روی تمام هارددیسک‌ها می‌نویسند. کل فضای موجود شامل تمام دیسک‌های RAID شده می‌باشد. افزونگی Redundancy وجود ندارد اگر هر درایوی fail شود دیتای موجود در آن درایو از بین می‌رود و قابلیت بازیابی وجود ندارد. مزیت این نوع RAID بندی کارایی مناسبی است که در اختیار ما می‌گذارد.

- کمترین درایو مورد نیاز برای راه اندازی: ۲ عدد
- حفاظت از دیتا: حفاظتی وجود ندارد.

RAID 0 برای محیط‌های کاری و عملیاتی که شرایط بحرانی دارند و دارای کارهای بسیار حساسی هستند اصلا توصیه نمی‌شود زیرا همان طور که بیان شد تحمل پذیری خطایی وجود ندارد.

RAID 1

RAID بندی به صورت ۱ چیزی شبیه به mirroring می‌باشد. دستگاه فورتی آنالایزر اطلاعات را بر روی یک هارد دیسک می‌نویسند و سپس یک کپی از آن را بر روی تمام دیسک‌های دیگر قرار می‌دهد. کل فضای دیسک موجود فقط یک هارد است. همان طوری که صرفا برای mirroring استفاده می‌شود. این نوع از ذخیره‌سازی دیتا یک نقطه از خطا ندارد single point of failure

اگر هر کدام از دیسک‌ها fail شود هارد دیسک‌های جایگزین موجود می‌باشند.

- کمترین درایو مورد نیاز برای راه اندازی: ۲ عدد
- حفاظت از دیتا: از دست دادن یک درایو

برای هر mirror یک write و دو read وجود دارد. RAID 1 داده‌های اضافی به همراه دارد. Re-build دیتا در صورت خرابی درایو نیاز نیست. این RAID بندی ساده ترین حالت طراحی ذخیره‌سازی می‌باشد که البته بالاترین overhead را بر روی دیسک‌ها دارد.

RAID 1s

این مدل از RAID به همراه hot spare مورد استفاده قرار می‌گیرد.(یک دیسک استندبای برای RAID در نظر گرفته می‌شود). اگر یک هارددیسک Fail شود در کمترین زمان ممکن دیسکی که بعنوان hot spare مشخص شده است جایگزین دیسک خراب می‌شود و با RAID ادغام شده و دیتا rebuild می‌شود. وقتی هارد دیسک جدیدی را با هارد خراب قبلی جایگزین می‌کنید هارد دیسک جدید بعنوان یک hot spare شناخته می‌شود. کل فضای دیسک برابر با تعداد دیسک‌های مورد استفاده منهای ۲ می‌باشد.

RAID 5

RAID بندی به صورت ۵ با استفاده از تکنولوژی parity چک کار می‌کند. چیزی شبیه به RAID 0 است، فورتی آنالایزر تمام اطلاعات را به صورت مساوی بر روی تمام درایوها می‌نویسند اما parity اضافه شده بر روی قسمت‌های مشابه نوشته می‌شود. بلاک‌های parity برای هر خط وجود دارد. کل فضای دیسک برابر است با تعداد کل دیسک‌های موجود در RAID منهای یک دیسک که برای parity درنظر گرفته شده است. برای مثال، با چهار دیسک کل ظرفیت موجود در واقع سه هارددیسک می‌باشد.

کارایی و پرفورمنس در RAID 5 به صورت معمولی می‌باشد. در این حالت read بهتر از write است. اگر چه باید اعتراف کرد که عملکرد ضعیف بوده ولی وقتی یک دیسک fail می‌شود روند کاری بدون مشکل و از دست دادن دیتا ادامه پیدا می‌کند. اگر درایو fail شود با دیسک جدید جایگزین شده و دستگاه فورتی آنالایزر با استفاده از اطلاعات parity دیتاها را در دیسک جدید بازیابی می‌کند.

- کمترین درایو مورد نیاز جهت راه اندازی: ۳ عدد
- حفاظت از دیتا: از دست دادن یک درایو

RAID 5s

یک RAID5 با hot spare از یک هارد دیسک بعنوان هات اسپیر استفاده می‌کند. (یک دیسک استندبای برای RAID). اگر هارد دیسکی fail شود، در یک دقیقه بعد از fail شدن، دیسک hot spare جایگزین می‌شود و rebuild دیتا آغاز می‌گردد. وقتی شما هارددیسک خراب را جایگزین می‌کنید. هارددیسک جدید بعنوان hot spare جدید قرار می‌گیرد. کل فضای قابل استفاده برابر با کل تعداد دیسک‌ها منهای ۲ است.

RAID 6

RAID بندی به صورت ٦ شبیه به RAID 5 است که یک parity بلاک اضافه دارد. در این نوع RAID دو parity بلاک توزیع شده و توسعه یافته در میان تمام دیسک‌های عضو داریم.

- کمترین درایو مورد نیاز جهت راه اندازی: ٤ عدد
- حفاظت از دیتا: از دست دادن دو درایو امکان پذیر است

RAID 6s

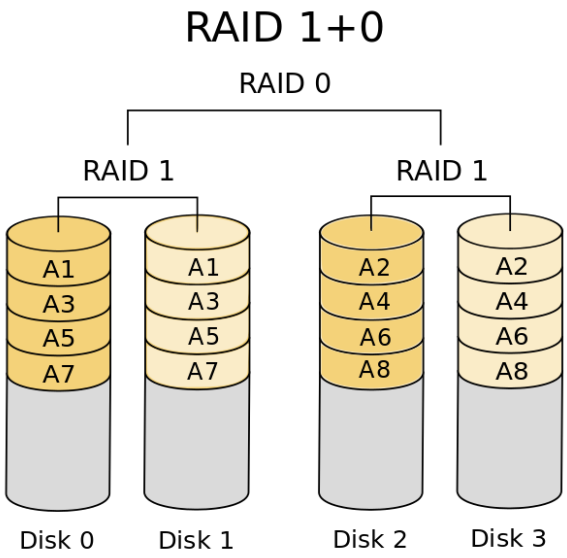
RAID 6 همراه با hot spare چیزی شبیه به RAID 5 است که با parity بلاک اضافه شده همراه گردیده است.

RAID 10

RAID 10 (1+0) شامل سطوح RAID بندی تو در تو می‌باشد. در این مدل RAID بندی حالت ۰ در بیرون بوده و ۱ داخل است. کل فضای موجود برابر است با کل تعداد دیسک‌های موجود در RAID که حداقل ٤ عدد می‌باشد تقسیم بر ۲ فضای RAID بندی ما در این حالت می‌شود.

یک درایو از یک RAID1 امکان Fail شدن را دارا است بدون اینکه دیتایی از دست برود. هرچند توجه داشته باشید که اگر یک درایو دیگر در RAID 1 دچار خرابی گردد تمام دیتاها از بین خواهد رفت. در این شرایط، خیلی مهم است که درایو خراب سریعا جایگزین گردد.

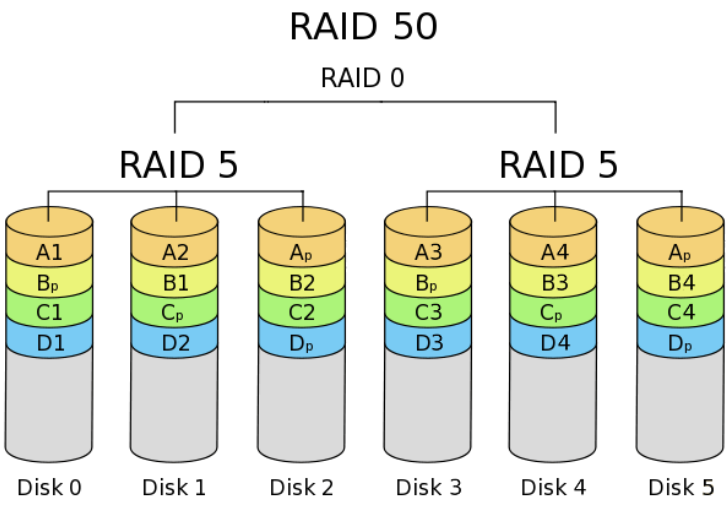
- کمترین درایو مورد نیاز جهت راه اندازی: ٤ عدد
- حفاظت از دیتا: از دست دادن دو درایو در هر sub-array امکان پذیر است



این نوع RAID جایگزینی مناسب برای RAID 1 است زمانی که عملکرد و کارایی مورد نیاز شما است.

RAID 50

RAID 5 شامل (5+0) است که RAID سطح 0 و 5 به صورت تو در تو می‌باشند. یعنی ابتدا RAID 0 بوده و سپس RAID 5 می‌باشد. کل فضای دیسک برابر است با تعداد کل دیسک‌ها منهای تعداد RAID 5 مربوط به sub-array ها. RAID 50 افزایش کارایی را برای شما به ارمغان می‌آورد و مطمئن می‌شوید که از دست دادن دیتا شبیه به دلایل موجود در RAID 5 وجود ندارد. یک درایو در هر شاخه RAID 5 امکان fail دارد بدون اینکه نگران از دست دادن دیتا باشید.



- کمترین درایو مورد نیاز جهت راه اندازی: ٦ عدد
- حفاظت از دیتا: از دست دادن یک درایو در هر sub-array امکان پذیر است.

این نوع RAID دارای تحمل پذیری خطا بالاتری نسبت به RAID 5 می‌باشد و بازده بالاتری نسبت به RAID 0 دارد.

RAID 50 بر روی مدل‌هایی موجود است که از تعداد ۹ دیسک یا بیشتر پشتیبانی می‌کنند. به صورت پیش فرض، دو گروه مورد استفاده قرار میگرند مگر اینکه از طریق محیط CLI پیکربندی شده باشند. از طریق دستور زیر می‌توانید سطح RAID کنونی دستگاه، وضعیت، سایز، گروه‌بندی و اطلاعات سایر هارددیسک‌ها را مشاهده نمایید.

Diagnose system raid status

RAID 60

از ترکیب RAID 0 با RAID 6 حاصل می‌شود. ویژگی‌های RAID 50 را دارد با این تفاوت که sub-array در اینجا RAID 6 است.

- کمترین درایو مورد نیاز جهت راه اندازی: ۸ عدد
- حفاظت از دیتا: از دست دادن دو درایو در هر sub-array امکان پذیر است.

نرخ انتقال و تراکنش بالا برای read، نرخ write معمولی و دارای عملکردی پایین تر از RAID 50 می‌باشد.

پیکربندی و تنظیم سطح RAID :

اخطار: هرگونه تغییر در سطح RAID تمام دیتاهای شما را پاک خواهد کرد.

پیکربندی سطح RAID:

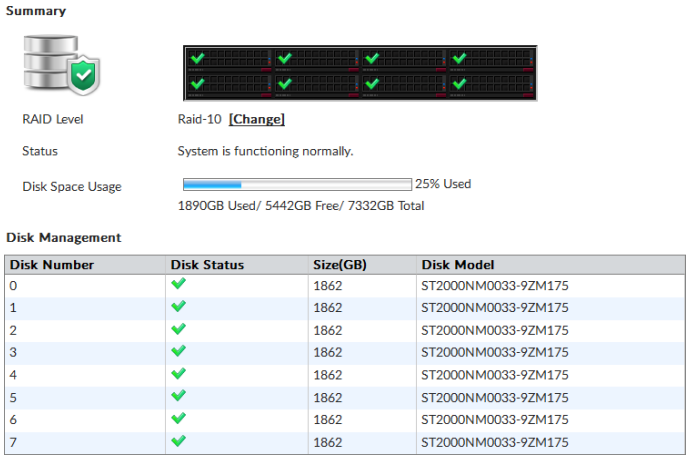
۱. به مسیر System Settings > RAID Management بروید.

۲. در قسمت RAID Level با انتخاب گزینه Change پنجره RAID Settings نمایش داده می‌شود.

۳. از لیست RAID Level، یک RAID جدید را انتخاب نمایید و سپس OK کنید. دستگاه فورتی آنالایزر ریبوت می‌شود. بر اساس RAID ی که انتخاب کرده‌اید ممکن است زمان قابل توجهی برای ایجاد RAID صرف شود.

مانیتور کردن وضعیت RAID :

برای مشاهده وضعیت RAID، به مسیر System Settings > RAID Management بروید. پنجره RAID Management که شامل وضعیت، میزان فضای دیسک استفاده شده و ... است نمایش داده می‌شود.



Summary	نمایش خلاصه‌ای از اطلاعات مربوط به **RAID** است.
Graphic	نمایش دهنده موقعیت و وضعیت هر دیسک در **RAID** بندی می‌باشد. با قرار دادن نشانگر موس بر روی هر کدام وضعیت و جزئیات دیسک‌ها نمایش داده می‌شود.
RAID Level	سطح **RAID** انتخابی را نمایش می‌دهد. با کلیک بر روی **Change** می‌توانید سطح **RAID** را تغییر دهید. وقتی تنظیمات **RAID** را تغییر می‌دهید تمام دیتاها پاک می‌شوند.
Status	وضعیت کلی از **RAID** بندی را نمایش می‌دهد.
Disk Space Usage	حجم کلی فضای دیسک را نمایش می‌دهد. چه مقداری از فضای دیسک استفاده شده است و چه مقداری از فضای دیسک آزاد است.
Disk Management	نمایش دهنده اطلاعات در مورد هر دیسک است.
Disk Number	برای هر دیسک عدد شناسایی دیسک را مشخص می‌کند.
Disk Status	نمایش دهنده وضعیت هر دیسک در **RAID** می‌باشد.

• **Ready**: هارددیسک به صورت معمول کار می‌کند. • **Rebuilding**: دستگاه دیتاها را بر روی هارددیسک جدید اضافه شده **write** می‌کند تا هارددیسک مجددا به حالت بهینه بازگردد. فورتی آنالایزر در این حالت قابلیت تحمل پذیری خطا را ندارد تا زمانی که **rebuild** به صورت کامل صورت پذیرد. • **Initializing**: دستگاه در حال **write** بر روی تمام هارد درایوها می‌باشد تا تحمل پذیری خطا به حالت نرمال بازگردد. • **Verifying**: دستگاه اطمینان حاصل می‌کند که دیتاهای **Parity** درایو اضافه شده معتبر است. • **Degraded**: هارد درایو توسط **RAID** کنترلر استفاده نمی‌شود. • **Inoperable**: یک یا چند درایو از دستگاه‌های فورتی آنالایزر **miss** شده‌اند. درایو مدت زمان زیادی است که در دسترس نمی‌باشد و عملا دیتایی در دسترس نیست.	
نمایش ظرفیت برای هر دیسک بر اساس **GB** است.	Size (GB)
شماره مدل هر دیسک نمایش داده می‌شود	Disk Model

تعویض هارددیسک ها

اگر هارد دیسکی بر روی دستگاه fail شود باید با دیسک جدیدی جایگزین گردد. دستگاه‌های فورتی آنالایزری که از RAID سخت افزاری پشتیبانی می‌کنند امکان تعویض هارد در زمانی که دستگاه روشن است وجود دارد به این قابلیت hot swapping گفته می‌شود. دستگاه‌های فورتی آنالایزری که دارای RAID نرم افزاری هستند، جهت تعویض هارد دیسک معیوب پروسه خاموش کردن دستگاه حتما باید رعایت شود و بعد جابجایی و تعویض صورت پذیرد.

الکتریسیته ساکن صدمات جبران ناپذیری را به دستگاه وارد می‌کند. توصیه می‌شود دستگاه را در مکان‌هایی قرار دهید که استانداردهای ESD رعایت شده باشد در غیر اینصورت از دستبندهای آنتی استاتیک و یا بندهای مچ پا استفاده نمایید.

قبل از جایگزین کردن دیسک اطمینان حاصل کنید که دیسک جدید از لحاظ سایز مورد پشتیبانی فورتی‌گیت می‌باشد و از لحاظ ظرفیت با هارد دیسک قبلی یکسان است. قرار دادن هاردی با ظرفیت کمتر بر روی RAID تاثیر خواهد گذاشت و ممکن است سبب از دست رفتن دیتا شود. با توجه به تفاوت‌های ممکن در سکتوربندی هاردها تنها راهی که میتوان تضمین کرد دو دیسک دارای سایزی مشابه و یکسان هستند استفاده از برندها و مدل‌های یکسان است. اندازه ارائه شده توسط سازنده هارددیسک برای یک مدل دیسک داده شده فقط مقداری تقریبی است. اندازه دقیق و حقیقی بر اساس تعداد بخش‌های موجود در یک دیسک مشخص می‌شود.

Hot swap بودن هارد دیسک بر روی یک دستگاه که از RAID سخت افزاری پشتیبانی می‌کند:

۱. هارد دیسک خراب را جدا کنید.

۲. یک دیسک جدید نصب نمایید.

دستگاه به صورت خودکار دیسک جدید را بر روی RAID کنونی اضافه می‌کند. سپس می‌توانید از طریق کنسول وضعیت را مشاهده نمایید. پنجره RAID Management آیکونی که نشان دهنده تیک سبز رنگی بر روی تمام دیسک‌ها می‌باشد نمایش می‌دهد.

یکبار که RAID ایجاد می‌شود، اضافه نمودن دیسک دیگر با ظرفیت مشابه تاثیری بر روی سایز RAID درست شده ندارد تا زمانی که مجددا Rebuild کرده و دستگاه فورتی آنالایزر را ریستارت نمایید.

اضافه کردن هارددیسک

بعضی از مدل‌های فورتی آنالایزر فضای لازم جهت اضافه کردن هارد دیسک‌های اضافه را دارند این کار سبب می‌شود فضای ذخیره‌سازی شما افزایش پیدا کند.

فورتی‌نت توصیه می‌کند که از دیسک‌های مشابهی که مورد تایید خودش است استفاده نمایید.

اضافه کردن هارد دیسک‌های بیشتر:

۱. تخصیص دیسکی که بوسیله ی فورتی‌نت ساپورت می‌شود.

۲. از دیتا لاگ موجود بر روی دستگاه فورتی آنالایزر بکاپ تهیه نمایید.

اگر فورتی آنالایزر دیگری دارید این قابلیت وجود دارد که دیتا لاگ‌ها را به دستگاه دوم منتقل نمایید. انتقال دیتا down time شما را کاهش می‌دهد و ریسک از دست دادن دیتا را به کمترین مقدار ممکن می رساند.

۳. دیسک‌ها را بر روی دستگاه نصب کنید.

اگر فورتی آنالایزر از hot swap پشتیبانی می‌کند، در حالی که دستگاه در حال فعالیت می‌باشد این کار را انجام دهید. در غیر این صورت اول باید دستگاه را خاموش کنید.

٤. نوع RAID خود را مشخص کنید.

٥. اگر از دیتا لاگ بکاپ گرفته‌اید آن را بازیابی کنید.

Administrative Domains

Administrative Domains یا ADOMها قابلیتی است که به ادمین اجازه می‌دهد دستگاه‌های خاصی را مدیریت نماید. ماهیت وجودی ADOMها بر پایه این است که چه کسانی به آنها دسترسی داشته باشند. وقتی حالت ADOM پیشرفته است، دستگاه‌های فورتی‌گیت با چندین VDOM می‌توانند بین چند ADOM تقسیم شوند.

اکانت‌های ادمین می‌توانند به یک یا چند ADOM تخصیص داده شوند و یا از دسترسی به ADOMهای خاص محروم شوند. به صورت خاص وقتی یک ادمین لاگین می‌کند فقط دستگاه‌ها یا VDOMهایی که به آنها دسترسی دارد قابل مشاهده است. ادمین‌هایی که اکانت آنها در گروه Super user قرار دارد مثل اکانت admin این امکان را دارند که تمام ADOMها و دستگاه‌های متصل به آنها را مشاهده نمایند. در هر ADOM مشخص می‌شود که چه مدت زمانی و چه مقداری از فضای دیسک برای نگهداری لاگ‌ها تخصیص داده شود. امکان مانیتور کردن مصرف دیسک و تنظیمات مورد نیاز برای ذخیره‌سازی لاگ‌ها برای هر ADOM وجود دارد.

بیشترین تعداد ADOM ی که می‌توانیم اضافه نماییم به مدل دستگاه بستگی دارد. برای کسب اطلاعات بیشتر بهتر است به مشخصات فنی دستگاه خود رجوع کنید.

به صورت پیش فرض ADOM غیرفعال است. فعال سازی و تنظیم‌های مربوط به ADOM فقط توسط ادمین‌هایی که در پروفایل super_user قرار دارند انجام می‌شود.

ADOMهای پیش فرض

فورتی آنالایزر برای نوع خاصی از دستگاه‌ها، شامل ADOMهای پیش فرض است. وقتی یک یا چند مدل از این دستگاه‌ها به فورتی آنالایزر اضافه می‌شوند، دستگاه‌ها به صورت خودکار به ADOM مناسب اضافه شده و ADOM قابل انتخاب می‌شود. وقتی ADOM پیش فرض شامل هیچ دستگاهی نیست آن ADOM قابل انتخاب نیست.

برای مثال وقتی یک دستگاه فورتی کلاینت EMS به فورتی آنالایزر اضافه می‌شود، دستگاه فورتی کلاینت EMS به صورت خودکار به ADOM پیش فرض اضافه می‌گردد. بعد از اینکه فورتی کلاینت EMS در ADOM مربوطه قرار گرفت، وقتی شما می‌خواهید به فورتی آنالایزر متصل شوید ADOM فورتی کلاینت قابل انتخاب می‌شود و می‌توانید بین ADOMها سوئیچ کنید.

تمام ADOMها در داخل ADOM پیش فرض بدون دستگاه‌ها از طریق مسیر System Settings > All ADOMs قابل مشاهده می‌باشند.

سازمان‌دهی دستگاه‌ها در داخل ADOM ها

امکان مرتب‌سازی دستگاه‌ها در داخل ADOMها وجود دارد این کار سبب می‌شود تا مدیریت دستگاه‌ها راحت‌تر صورت پذیرد. دستگاه‌ها با هر روشی که مورد قبول شما باشند مرتب‌سازی می‌شوند. برای مثال:

- نسخه فریمور: گروه‌بندی تمام دستگاه‌ها با فریمورهای مشابه در داخل یک ADOM صورت می‌گیرد.
- مناطق جغرافیایی: گروه‌بندی تمام دستگاه‌ها بر اساس یک منطقه جغرافیایی مشخص در داخل یک ADOM صورت می‌گیرد و دستگاه‌هایی که برای منطقه‌ای متفاوت هستند در داخل ADOM دیگری قرار می‌گیرند.
- ادمین‌ها: گروه‌بندی دستگاه‌ها بر اساس تفکیک ADOMها طوری انجام میشود که ادمین‌های مسئول برای هر دستگاه گروه‌بندی می‌شوند.
- مشتریان: گروه‌بندی تمام دستگاه‌ها برای یک مشتری در داخل یک ADOM و دستگاه‌های دیگر برای سایر مشتریان در داخل ADOM متفاوتی انجام می‌گیرد.

پشتیبانی فورتی کلاینت و ADOM ها

لاگ‌های فورتی کلاینت بر روی دستگاهی که فورتی کلاینت روی آن رجستر شده است ذخیره می‌گردد.

برای مثال، وقتی دستگاه نهایی یا endpoint بر روی فورتی‌گیت ثبت می‌شود. لاگ‌های فورتی کلاینت بر روی دستگاه فورتی‌گیت ثبت و نمایش داده می‌شود.

ADOMها جهت پشتیبانی از دستگاه‌های فورتی کلاینت EMS باید فعال شوند.

ادغام لاگ‌های فورتی آنالایزر برای فورتی کلاینت EMS در کروم بوک ها

۱. از دستورات زیر استفاده نمایید:

```
config system interface
"edit "port1
set allowaccess https ssh http http-logging https-logging
next
end
```

۲. اضافه کردن SSL برای فعال نمودن ارتباط

SSL certificate جهت برقراری ارتباط و ارسال لاگ‌ها بین فورتی کلاینت و فورتی آنالایزر مورد نیاز است. اگر از SSL certificate عمومی استفاده می‌کنید فقط باید SSL را به فورتی آنالایزر اضافه نمایید. اگر ترجیح می‌دهید از certificate استفاده کنید که از یک CA رایج نمی‌باشد باید SSL را به فورتی آنالایزر اضافه کنید. باید root CA را به Google chromebooks معرفی کنید. در غیر اینصورت کانکشن HTTPS بین فورتی کلاینت EMS کروم بوک و فورتی آنالایزر کار نخواهد کرد. نام معمول سرتیفیکیت (common name) باید IP آدرس فورتی آنالایزر باشد.

a. در فورتی آنالایزر به مسیر System Settings> Certificates> Local Certificates بروید.

b. بر روی Import کلیک کنید. پنجره Import Local Certificate مشخص می‌شود.

c. در Type لیست، Certificate را انتخاب نمایید. یا در Type لیست، PKCS#12 را انتخاب تا certificate با فرمت PK12 آپلود شود.

d. در کنار فیلد Certificate File، بر روی Browse کلیک کنید تا certificate را انتخاب نمایید.

e. کلمه عبور و نام سرتیفیکیت را وارد کنید.

f. بر روی OK کلیک کنید.

۳. Certificateهای انتخاب شده برای کانکشن‌های HTTPS:

a. در فورتی آنالایزر، به مسیر System Settings> Admin> Admin Settings می‌رویم.

b. در قسمت HTTPS & Web Service Certificate، سرتیفیکیتی که تمایل به استفاده از آن را دارید انتخاب و سپس بر روی Apply کلیک کنید.

٤. فعال نمودن ADOM فورتی کلاینت با استفاده از دستورات زیر در محیط CLI امکان پذیر است:

```
onf sys global
set adom-status enable
end
```

٥. برای اضافه کردن فورتی کلاینت EMS برای کروم بوک همانند ADOM فورتی کلاینت :

به مسیر Device Manager> + بر روی دکمه Add Device کلیک کنید تا فورتی کلاینت EMS برای کروم بوک همانند یک دیوایس فورتی کلاینت ADOM اضافه گردد.

فعال / غیرفعال کردن قابلیت ADOM

به صورت پیش فرض ADOMها غیرفعال می‌باشند. فعال کردن و پیکربندی ADOMها بوسیله ادمین‌های super user انجام می‌شود.

وقتی ADOMها فعال هستند، Device Manager، FortiView، LogView، Event Management و Reportها برای هر ADOM نمایش داده می‌شوند. وقتی در دستگاه فورتی آنالایزر لاگین می‌کنید ADOM که می‌خواهید بر روی آن کار کنید را انتخاب نمایید.

ADOM باید فعال باشد تا از لاگ‌ها و گزارش‌های مربوط به FortiMail و FortiWeb پشتیبانی کند.

فورتی‌گیت و FortiCarrier امکان گروه‌بندی در ADOM یکسان را ندارند.

فعال کردن قابلیت ADOM:

۱. با اکانت ادمینی که سوپر یوزر است به فورتی آنالایزر لاگین کنید.

۲. به مسیر System Settings> Dashboard بروید.

۳. در ویجت System Information ، گزینه Administrative Domain را بر روی ON سوئیچ کنید.

به صورت خودکار از دستگاه Logged out می‌شود و صحفه لاگین برای شما ظاهر می‌گردد.

غیرفعال کردن قابلیت ADOM:

۱. تمام دستگاه‌هایی که در روت ADOM نمی‌باشند را پاک کنید.

۲. تمام ADOMها را حذف نمایید. به جز ADOM روت که امکان پاک کردن آن وجود ندارد.

۳. به مسیر System Settings> Dashboard بروید.

٤. در ویجت System Information، سوئیچ گزینه Administrative Domain را بر روی حالت OFF قرار دهید.

به صورت خودکار از فورتی آنالایزر Logged out می‌شوید و صفحه لاگین مجددا برای شما نمایش داده می‌شود.

قابلیت ADOMها امکان غیرفعال شدن ندارد مگر در ADOMها تنظیمات وجود داشته باشد.

حالت‌های ADOM دستگاه

ADOM در دستگاه دارای دو حالت می‌باشد: نرمال (پیش فرض) و پیشرفته

در حالت نرمال، امکان تخصیص VDOMهای متفاوت از فورتی‌گیت به ADOMهای مختلف وجود ندارد. این کار سبب می‌شود تحلیل دیتا برای VDOMهای تک صورت گیرد اما نتایج در سناریوهای مدیریتی پیچیدگی بیشتری پیدا خواهد کرد. توصیه می‌شود فقط کاربران حرفه‌ای از این روش استفاده نمایند.

برای تغییر و رفتن از حالت پیشرفته به نرمال، ابتدا مطمئن شوید هیچکدام از VDOMهای فورتی‌گیت به یک ADOM تخصیص داده نشده است.

تغییر حالت ADOM دستگاه:

۱. به مسیر System Settings> Advanced> Advanced Settings بروید.

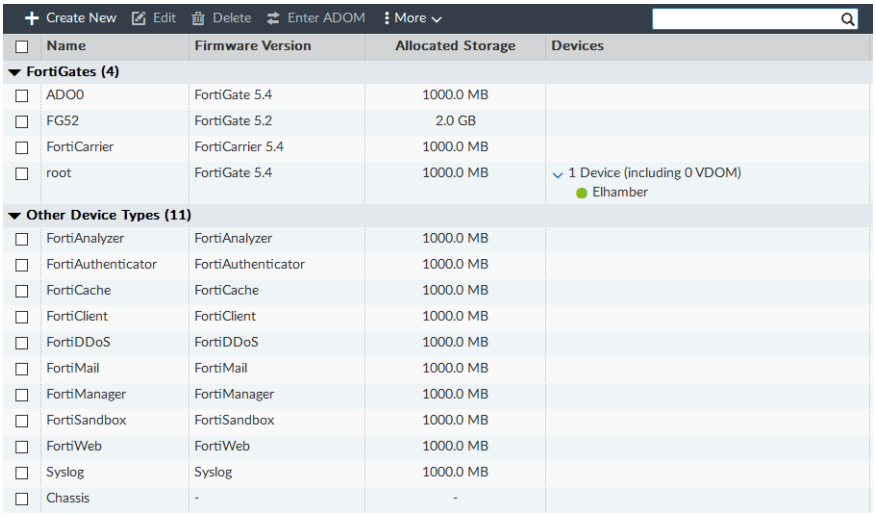
۲. در فیلد ADOM Mode، هر کدام از حالت‌های Normal یا Advanced را انتخاب نمایید.

۳. با انتخاب گزینه Apply تغییرات اعمال می‌گردد.

مدیریت ADOM ها

برای ساخت و مدیریت ADOMها به مسیر System Settings> All ADOMs بروید.

قبل از ایجاد و پیکربندی ADOMها باید قابلیت ADOM را فعال کنید.



Create New	یک ADOM جدید ایجاد می‌شود.
Edit	ADOM انتخابی را ویرایش می‌کنید. این قابلیت با راست کلیک کردن بر روی منو در دسترس قرار می‌گیرد.
Delete	ADOM یا ADOMهای انتخابی را پاک می‌کنید. امکان پاک کردن ADOM پیش فرض وجود ندارد. این گزینه با راست کلیک کردن بر روی منو ظاهر می‌گردد.
Enter ADOM	جابجا شدن در ADOMهای انتخاب شده توسط این گزینه صورت می‌پذیرد.
More	گزینه Expand Devices را انتخاب نمایید تا تمام ADOMها نمایش داده شوند. با انتخاب گزینه Collapse devices لیست دستگاه‌ها نمایش داده می‌شوند.

Search	**عبارتی را جهت جستجو در لیست ADOM وارد نمایید.**
Name	**نام ADOM را انتخاب می‌کنید.**
Firmware Version	**نسخه فریمور ADOM نمایش داده می‌شود. دستگاه‌های موجود در یک ADOM باید فریم‌ورهای یکسان داشته باشند.**
Allocated Storage	**مقدار فضای تخصیص داده شده برای ذخیره‌سازی که در اختیار ADOM است.**
Devices	**تعداد دستگاه‌ها و VDOMهایی که در یک ADOM هستند. در صورتی که راست کلیک کنید لیست دستگاه‌ها باز می‌شود.**

ساخت ADOMها:

جهت ساخت ADOM باید با دسترسی ادمینی که جزو گروه سوپر یوزر است وارد شوید.

در هنگام ایجاد ADOM به موارد زیر اهمیت دهید:

- حداکثر تعداد ADOM که میتوان ساخت به مدل دستگاه فورتی آنالایزر شما بستگی دارد.
- از اکانت ادمینی استفاده نمایید که پروفایل سوپر یوزر به آن تخصیص داده شده است.
- می‌توانید دستگاهی را اضافه نمایید که فقط یک ADOM است. تخصیص یک دستگاه به چندین ADOM امکان پذیر نمی‌باشد.
- فورتی‌گیت و FortiCarrier در یک ADOM مشابه قرار نمی‌گیرند.
- امکان اضافه کردن VDOMهای مختلف از یک دستگاه فورتی‌گیت به یک ADOM وجود دارد. اگر درنظر دارید تا VDOMهای تک ر از یک دستگاه فورتی‌گیت به ADOMهای متفاوت اضافه کنید اول باید حالت پیشرفته دستگاه را فعال نمایید.

- چگونگی پیکربندی لاگ فایل‌ها از هر دستگاه در ADOMها مشخص می‌گردد. برای مثال، امکان تنظیم حالتی که مقدار فضای مورد استفاده یک دیسک از ADOM برای لاگ‌ها وجود دارد. همچنین مشاهده مقدار فضای دیسک مورد استفاده امکان پذیراست. مقدار لاگ ایندکس شده در دیتابیس SQL قابل تنظیم می‌باشد. علاوه بر این امکان نگهداری لاگ‌ها به صورت یک فایل کمپرس شده وجود دارد.

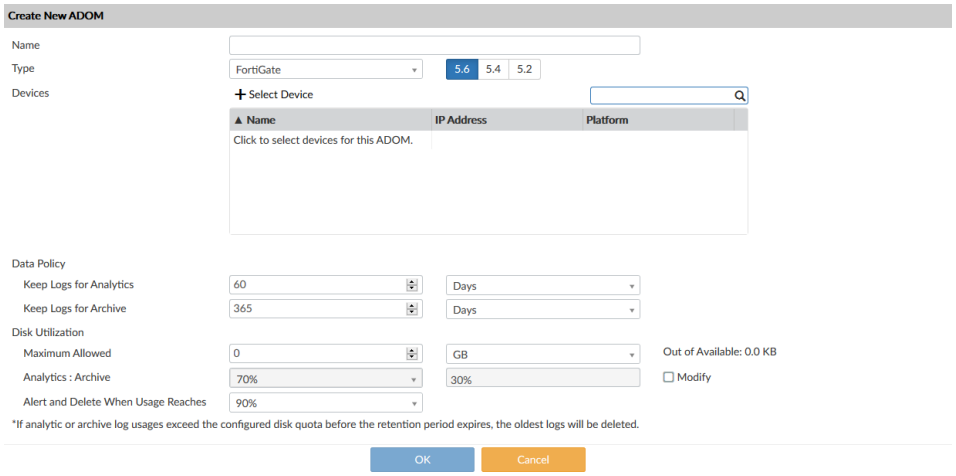
ساخت و ایجاد یک ADOM:

۱. مطمئن شوید که ADOMها فعال هستند.

۲. به مسیر System Settings> All ADOMs بروید.

۳. در نوار ابزار بر روی Create New کلیک نمایید.

٤. پنجره Create New ADOM نمایش داده می‌شود.



۵. تنظیمات را بر اساس موارد زیر انجام و سپس بر روی OK کلیک نمایید تا ADOM جدید ساخته شود.

NAME	**نامی را انتخاب کنید که ADOM را از سایر ADOMها متمایز خواهد کرد. نام‌های ADOM باید یونیک باشد.**
Type	**مدل دستگاهی که برای آن ADOM ایجاد می‌کنید را انتخاب نمایید. نام ADOM قابل ویرایش نمی‌باشد.**

اگر چه امکان ایجاد **ADOM** متفاوت برای هر مدل دستگاه وجود دارد.	
نسخه دستگاه را در **ADOM** انتخاب نمایید. نسخه **ADOM** قابلیت ویرایش ندارد. امکان ایجاد کردن یک **ADOM** برای هر نسخه وجود دارد. این گزینه در شرایطی در دسترس است که نوع دستگاه فورتی‌گیت یا **FortiCarrier** باشد.	Version
اضافه کردن یک یا چند دستگاه با انتخاب نسخه **ADOM** انجام می‌پذیرد. فیلد مربوط به جستجو می‌تواند برای یافتن یک دستگاه مشخص مورد استفاده قرار گیرد.	Devices
مدت زمانی که قرار است لاگ‌ها در حالت ایندکس و فشرده قرار بگیرند مشخص می‌گردد.	Data Policy
چه مدت لاگ‌ها در حالت ایندکس باقی بمانند. در طی این وضعیت لاگ‌ها در دیتابیس **SQL** ایندکس شده و برای مدت زمان مشخص باقی می‌ماند. اطلاعات لاگ‌ها در **Event Manager** **FortiView** قابل مشاهده است بعد از مشخص کردن مدت زمان منقضی شدن، لاگ‌ها به صورت خودکار از دیتابیس **SQL** پاک می‌شوند	Keep Logs for Analytics
مدت زمانی که لاگ‌ها به صورت فشرده نگهداری می‌شوند. وقتی لاگ‌ها به صورت فشرده ذخیره‌سازی می‌شوند در **FortiView**، **Event Management**، **Reports** قابل مشاهده نمی‌باشند. وقتی زمان انقضای لاگ می‌رسد آرشیو	Keep logs for Archive

لاگ‌ها به صورت خودکار از دستگاه فورتی آنالایزر پاک می‌شوند.	
مقدار فضای دیسک جهت استفاده از لاگ‌ها مشخص می‌گردد.	Disk Utilization
بیشترین مقدار فضای دیسک که توسط فورتی آنالایزر جهت نگهداری از لاگ‌ها استفاده می‌شود. واحد اندازه‌گیری هم در این بخش مشخص می‌گردد. کل فضای موجود بر روی فورتی آنالایزر نمایش داده می‌شود. بعد از مشخص کردن مقدار زمان انقضا، لاگ‌های آرشیوی به صورت خودکار از روی دستگاه فورتی آنالایزر پاک می‌شوند.	Maximum Allowed
درصد فضای اختصاص داده شده برای تجزیه و تحلیل لاگ‌های آرشیوی در این بخش مشخص می‌گردد. لاگ‌های تحلیلی نسبت به لاگ‌های آرشیوی نیاز به فضای بیشتری دارند. برای مثال تنظیم به صورت ۷۰٪ و ۳۰٪ نشان دهنده آن است که ۷۰ درصد دیسک برای استفاده تجزیه و تحلیل لاگ‌ها درنظر گرفته شده است و ۳۰ درصد مابقی در جهت استفاده لاگ‌های آرشیو مورد استفاده قرار می‌گیرد. با انتخاب گزینه **Modify** می‌توانید این مقدار را تغییر بدهید.	Analytics Archive
در چه درصدی از استفاده دیتاها پیغام‌های اخطار نمایش داده شود و لاگ‌ها به صورت خودکار پاک شوند. قدیمی‌ترین لاگ‌های آرشیوی پاک شوند یا جدول دیتابیس تحلیلی کدام یک ابتدا از بین برود ؟	Alert and Delete When Usage Reaches

اختصاص دستگاه به یک ADOM

برای انجام این مورد باید با اکانت ادمینی وارد شوید که جزو super userها باشد. امکان تخصیص دستگاه‌ها به چند ADOM وجود ندارد.

اختصاص دستگاه‌ها به یک ADOM:

۱. به مسیر System Settings> All ADOMs بروید.

۲. بر روی یک ADOM دابل کلیک کنید، با راست کلیک کردن بر روی ADOM از منوی باز شده گزینه Edit را انتخاب نمایید و یا ADOM را انتخاب کرده و از نوار ابزار بر روی Edit کلیک کنید. پنجره Edit ADOM نمایش داده می‌شود.

۳. بر روی Select Device کلیک کنید. لیست Select Device باز می‌شود.

٤. دستگاه‌هایی که درنظر دارید تا به ADOM اضافه کنید را مشخص نمایید. فقط دستگاه‌هایی با نسخه‌های مشابه می‌توانند به ADOM اضافه شوند. دستگاه‌های انتخاب شده در لیست Devices نمایش داده می‌شوند. اگر ADOM در حالت پیشرفته است امکان اضافه کردن VDOMهای مجزا به یک ADOM وجود دارد.

۵. وقتی انتخاب دستگاه‌ها پایان پذیرفت، بر روی Close کلیک کنید تا لیست بسته شود.

٦. بر روی OK کلیک کنید.

دستگاه‌های انتخاب شده از ADOM قبلی پاک می‌شوند و به این ADOM اضافه می‌گردند.

واگذاری ADOM به ادمین‌ها

ادمین‌هایی که در پروفایل super user هستند امکان ایجاد اکانت‌های ادمین جدید را دارند همچنین می‌توانند به سایر ADOMها یک اکانت اختصاص دهند.

تخصیص یک ADOM خاص به یک ادمین

۱. با اکانتی که ادمین است و جزو گروه super user می‌باشد لاگین کنید. سایر اکانت‌ها امکان انجام تنظیمات را ندارند.

۲. به مسیر System Settings> Admin> Administrator بروید.

۳. بر روی یکی از ادمین‌ها دابل کلیک کنید، راست کلیک کرده و از منوی باز شده بر روی Edit کلیک کنید یک اکانت ادمین را کلیک کرده و سپس از نوار ابزار بر روی Edit کلیک کنید. پنجره Edit Administrator باز می‌شود.

٤. موارد مورد نیاز خود را در فیلد Administrative Domain ویرایش نمایید.

٥. برای اعمال تغییرات بر روی دکمه OK کلیک نمایید.

توجه داشته باشید که اکانت admin را نمی‌توانید بر روی یک ADOM خاص محدود نمایید.

ویرایش ADOM

برای ویرایش ADOM باید دسترسی ادمین داشته باشید و این ادمین باید در پروفایل super user باشد. نوع ADOM و نسخه آن قابل ویرایش نیست. برای ADOMهای پیش فرض، نام قابل ویرایش نمی‌باشد.

ویرایش ADOM:

۱. به مسیر System Settings> All ADOMs بروید.

۲. بر روی ADOM دابل کلیک کنید، راست کلیک کرده و از منو باز شده گزینه Edit را انتخاب کنید و یا ADOM را انتخاب سپس از نوار ابزار بر روی Edit کلیک کنید. پنجره Edit ADOM باز می‌شود.

۳. بر اساس خواست خود تنظیمات را ویرایش کرده و برای اعمال تغییرات OK کنید.

حذف کردن ADOMها

برای پاک کردن ADOM با اکانت ادمین وارد شوید. این اکانت باید در پروفایل super user قرار داشته باشد.

قبل از حذف کردن ADOM :

- تمام دستگاه‌ها باید از ADOM حذف شوند. دستگاه باید به یک ADOM دیگر منتقل شود و یا به روت ADOM جابجا شود.
- ارتباط ADOM با اکانت ادمین باید حذف گردد.

حذف کردن یک ADOM:

۱. به مسیر System Settings> All ADOMs بروید.

۲. مطمئن شوید که ADOM یا ADOMهایی که درنظر دارید تا حذف کنید هیچ دستگاهی در داخل آنها وجود نداشته باشد.

۳. ADOM یا ADOMهایی که قرار است حذف شوند را انتخاب نمایید.

٤. از نوار ابزار بر روی Delete کلیک کنید و یا راست کلیک کرده و Delete را انتخاب نمایید.

٥. با انتخاب گزینه OK تمام ADOM یا ADOMها حذف می‌شوند.

امکان حذف ADOMهای پیش فرض وجود ندارد.

Administrators

از طریق مسیر System Settings> Admins امکان انجام تنظیمات بر روی اکانت‌های ادمین وجود دارد. این تنظیمات شامل دسترسی به پروفایل‌ها، احراز هویت سرورها، تنظیمات کلی برای دستگاه فورتی آنالایزر و ... می‌باشد.

اکانت‌های ادمین جهت دسترسی به دستگاه فورتی آنالایزر مورد استفاده قرار می‌گیرند. احراز هویت به صورت local و یا به صورت راه دور انجام می‌شود. پروفایل‌های ادمین در انواع مختلف تعریف می‌گردد که سطوح دسترسی آنها متفاوت است.

تنظیمات عمومی شامل مواردی مثل زبان GUI و پالیسی‌های پسورد می‌تواند از طریق بخشAdmin Settings انجام شود.

هاست‌های مورد اطمینان

انجام تنظیمات trusted hosts برای ادمین‌ها سبب افزایش امنیت در شبکه می‌شود. علاوه بر دانستن کلمه عبور، یک ادمین فقط از طریق ساب نت یا ساب نت‌های مشخص شده متصل می‌شود. حتی این امکان وجود دارد که ادمین‌ها به یک IP محدود شوند.

وقتی برای تمام ادمین‌ها trusted host مشخص می‌کنید دستگاه فورتی آنالایزر به سایر درخواست‌هایی که جزو Trusted host نیستند پاسخی نمی‌دهد. این کار سبب می‌شود بالاترین شرایط امنیتی برای شما ایجاد گردد. اگر ادمین‌های شما بدون محدودیت در شبکه فعالیت دارند به صورت بالقوه تهدیدات بسیار زیادی وجود خواهد داشت.

بحث Trusted host به صورت GUI و یا CLI بر روی دستگاه مشخص می‌گردد. دسترسی CLI از طریق کانکتور کنسول انجام نمی‌شود. اگر Trusted Host تنظیم شده است و درنظر دارید تا از طریق GUI به کنسول دسترسی داشته باشید باید آدرس 127.0.0.1/24 را در trusted host قرار بدهید.

مانیتور کردن Administrators

قسمت Admin Session List به شما اجازه می‌دهد تا ادمین‌هایی که در حال حاضر به دستگاه فورتی آنالایزر متصل هستند را مشاهده کنید.

مشاهده ادمین‌هایی که لاگین هستند:

۱. به مسیر System Settings> Dashboard بروید.

۲. در ویجت System Information، فیلد Current Administrators، بر روی دکمه Current Sessions List کلیک کنید.

اطلاعات زیر قابل دسترسی می‌باشد:

Username	نام اکانت ادمین مشخص است. **Session** شما به صورت **current** نمایش داده می‌شود.
IP Address	**IP** آدرسی که ادمین با آن لاگین کرده به همراه نوع لاگین برای شما مشخص می‌شود. **GUI, jsconsole, SSH, Telnet**
Start Time	**تاریخ و زمانی که ادمین لاگین کرده مشخص می‌گردد.**
Time Out (mins)	**حداکثر مدت session در دقیقه می‌باشد.**

قطع کردن ادمین‌ها

امکان قطع ادمین‌ها از طریق دستگاه فورتی آنالایزر و در قسمت Admin Session List وجود دارد.

قطع کردن ادمین‌ها:

۱. به مسیر System Settings> Dashboard بروید.

۲. در ویجت System Information، در فیلد Current Administrators، بر روی دکمه Current Session List کلیک کنید.

۳. ادمین/ ادمین‌هایی که در نظر دارید تا قطع نمایید را انتخاب کنید.

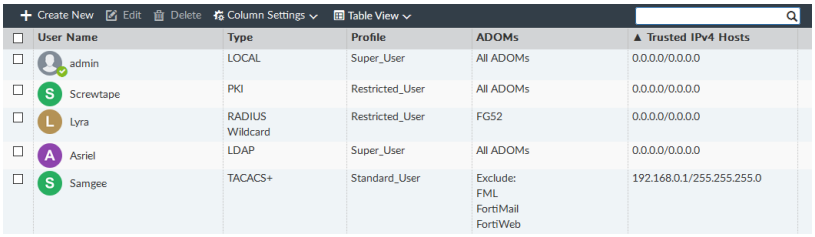
٤. از نوار ابزار بر روی Delete کلیک کنید یا با راست کلیک و انتخاب گزینه Delete این کار را انجام دهید.

ادمین‌های انتخاب شده به صورت خودکار از دستگاه فورتی آنالایزر قطع می‌شوند.

مدیریت اکانت‌های ادمین

به مسیر System Settings> Admin> Administrator بروید تا بتوانید لیستی از ادمین‌ها را مشاهده و مدیریت نمایید.

فقط ادمین‌هایی که جزو پروفایل سوپر یوزر هستند می‌توانند لیست ادمین‌ها را به صورت کامل مشاهده نمایند. وقتی قابلیت ADOM فعال می‌شود ادمین‌ها فقط به ADOM ی دسترسی دارند که بر روی آن Permission تعریف شده است.



گزینه‌های زیر موجود می‌باشند:

Create New	**ساخت یک ادمین جدید از این قسمت صورت می‌گیرد.**
Edit	**ویرایش ادمین انتخابی در این قسمت انجام می‌شود.**
Delete	**حذف کردن ادمین/ ادمین‌های انتخاب شده در این قسمت صورت می‌گیرد.**
Column Settings	**ایجاد تغییرات در ستون‌های نمایش داده شده از این قسمت صورت می‌گیرد.**
Table View	**تغییر در نمایش لیست ادمین‌ها از اینجا انجام می‌شود.**
Search	**جستجوی ادمین‌ها از این قسمت انجام می‌شود.**

Change Password	ادمین‌های انتخاب شده از این قسمت کلمه عبور خود را تغییر می‌دهند.

اطلاعات زیر نشان داده شده است:

User Name	نامی که ادمین هنگام لاگین از آن استفاده کرده است.
Type	نوع کاربر، اگر ادمین محدود باشد یا از **wildcard** استفاده کرده باشد.
Profile	نمایه مورد استفاده ادمین نمایش داده می‌شود.
ADOMs	**ADOM**هایی که ادمین به آنها دسترسی دارد.
Comments	توضیحاتی در مورد اکانت‌های ادمین. این ستون به صورت پیش فرض مخفی است.
Email	ایمیل مربوط به ادمین می‌باشد. این ستون به صورت پیش فرض نمایش داده نمی‌شود.
Phone	شماره تلفن مربوط به ادمین است. این ستون به صورت پیش فرض نمایش داده نمی‌شود.
Trusted Hosts	**Trusted host** که مرتبط با این ادمین می‌باشد.

ایجاد ادمین‌ها

جهت ساخت و ایجاد یک اکانت ادمین جدید باید با کاربری لاگین کنید که دسترسی کافی داشته باشد و یا جزو گروه super user باشد.

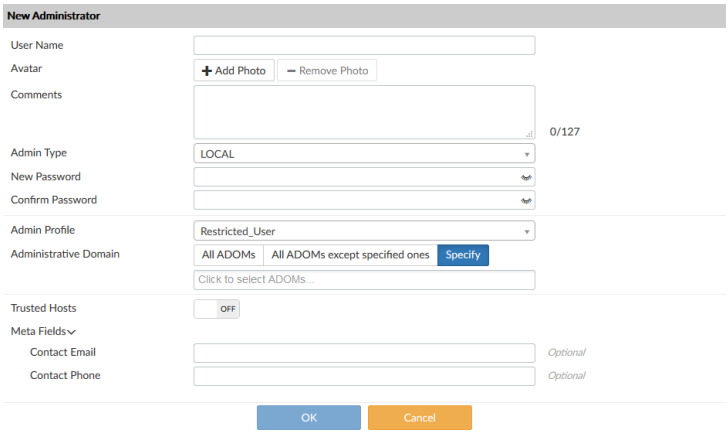
جهت ساخت یک اکانت اطلاعات زیر مورد نیاز است:

- از کدام مدل احراز هویت جهت اتصال به دستگاه استفاده می‌شود. لوکال، ریموت و یا PKI
- کدام مدل پروفایل به ادمین تخصیص داده می‌شود. این اکانت به چه دسترسی‌هایی نیاز دارد.
- اگر ADOM فعال است دسترسی به کدام ADOMها به کاربر داده شود.
- اگر از trusted host استفاده می‌شود. تمامی trusted hostها مشخص شود.

ایجاد یک ادمین جدید:

۱. به مسیر System Settings> Admin> Administrators بروید.

۲. در نوار ابزار بر روی Create New کلیک کنید. پنجره New Administrator نمایش داده می‌شود.



تنظیمات زیر را انجام داده و سپس برای تایید ادمین جدید بر روی OK کلیک کنید.

User Name	نامی را وارد نمایید که بعدا از آن جهت لاگین استفاده می‌شود.
Avatar	عکسی دلخواه برای ادمین انتخاب کنید.
Comments	به صورت کاملا دلخواه می‌توانید توضیحاتی در مورد وظایف فرد، موقعیتی که دارد و یا دلایل ساخت اکانت وارد کنید.
Admin Type	نوع احراز هویت اکانت را مشخص می‌کنیم.
Server or Group	انتخاب **RADIUS** سرور، **LDAP** سرور،**TACACS+** سرور و ... این سرورها قبل از ساخت اکانت ادمین باید پیکربندی شوند.
Wildcard	انتخاب این گزینه تنظیم پسورد همانند یک **wildcard** می‌باشد. فقط یک ادمین بر روی فورتی آنالایزر امکان استفاده از **wildcard** را دارد. این گزینه در شرایطی که نوع ادمین به صورت لوکال یا **PKI** است موجود نمی‌باشد.
Subject	این گزینه در صورتی وجود دارد که **Admin Type** به صورت **PKI** باشد.

CA	انتخاب **CA** سرتیفیکیت از لیست انجام می‌پذیرد. این گزینه در صورتی موجود است که **Admin Type** در حالت **PKI** است.
Required two-factor authentication	انتخاب فعال سازی احراز هویت به صورت دو مرحله‌ای صورت می‌پذیرد. این گزینه در شرایطی فعال است که **Admin Type** به صورت **PKI** است.
New Password	کلمه عبور خود را وارد کنید. اگر **Wildcard** انتخاب شده باشد این گزینه فعال نیست. اگر **Admin Type** به صورت **PKI** باشد، این گزینه فقط در حالت **Require two-factor authentication** فعال است.
Confirm Password	وارد کردن مجدد پسورد جهت تایید کلمه عبور انجام می‌پذیرد.
Admin Profile	انتخاب پروفایل ادمین از لیست انجام می‌شود. انتخاب این پروفایل مشخص می‌کند که ادمین به چه قابلیت‌هایی دسترسی داشته باشد.
Administrative Domain	انتخاب **ADOM** یعنی مشخص می‌کنید که این ادمین به چه قابلیت‌هایی دسترسی داشته باشد. **All domain** : ادمین به تمام **ADOM**ها دسترسی دارد. **All ADOMs except specified ones** : ادمین به همه **ADOM**ها دسترسی ندارد. **Specify**: ادمین به تمام **ADOM**های انتخابی دسترسی دارد.
Trusted Hosts	روشن کردن **Trusted host** و تخصیص **IP** آدرس و **Subnet**
Meta Fields	اختیاری بوده و می‌توانید جهت وارد کردن ایمیل آدرس و یا شماره تلفن ادمین‌های جدید استفاده نمایید.

ویرایش ادمین‌ها

برای ویرایش اکانت یک یوزر باید با دسترسی ادمینی وارد شوید که جزو پروفایل super user باشد. نام ادمین‌ها قابلیت ویرایش ندارد. کلمه عبور ادمین می‌تواند از طریق راست کلیک بر روی منو تغییر کند.

ویرایش ادمین:

۱. به مسیر System Settings> Admin> Administrators بروید.

۲. بر روی ادمین دابل کلیک کنید، با راست کلیک کردن بر روی یک ادمین و انتخاب گزینه Edit از منوی باز شده و یا انتخاب ادمین سپس از نوار ابزار بر روی Edit کلیک کنید. پنجره Edit Administrator باز می‌شود.

۳. تنظیمات مورد نیاز را انجام دهید و سپس جهت اعمال تغییرات بر روی دکمه OK کلیک کنید.

تغییر کلمه عبور ادمین‌ها:

۱. به مسیر System Settings> Admin> Administrators بروید.

۲. بر روی یک ادمین راست کلیک کنید و از منو گزینه Change Password را انتخاب نمایید. صفحه مربوط به Change Password باز می‌شود.

۳. در فیلد Old Password کلمه عبور قبلی خود را وارد نمایید.

٤. کلمه عبور جدید را در فیلد New Password وارد کرده و تکرار آن را در فیلد Confirm Password مجددا تایپ نمایید.

۵. با انتخاب دکمه OK تغییرات پسورد ادمین اعمال می‌گردد.

کلمه عبور ادمین حال حاضر از طریق منوی ادمین در بنر GUI می‌تواند پسورد خود را تغییر دهد.

پاک کردن ادمین‌ها

برای حذف ادمین/ ادمین‌ها باید با اکانتی لاگین کنید که جزو گروه super user است. امکان حذف اکانت admin وجود ندارد.

پاک کردن اکانت ادمین / ادمین‌ها:

۱. به مسیر System Settings> Admin> Administrators بروید.

۲. ادمین/ ادمین‌هایی که در نظر دارید پاک کنید را انتخاب نمایید.

۳. از نوار ابزار بر روی Delete کلیک کنید.

٤. در قسمت تایید گزینه OK را انتخاب کنید تا ادمین/ ادمین‌های انتخابی حذف شوند.

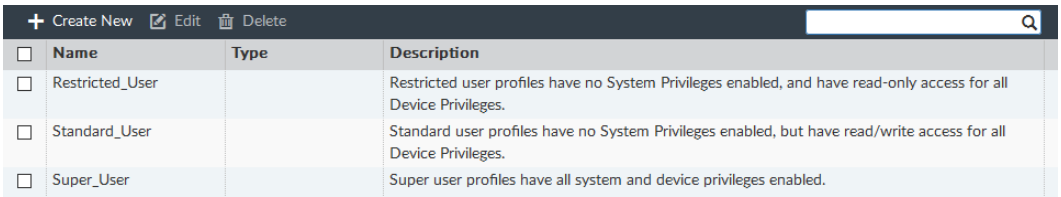
پروفایل‌های Administrators

پروفایل ادمین برای کنترل ادمین‌ها مورد استفاده قرار می‌گیرد تا سطوح دسترسی یک ادمین به دستگاه و یا قابلیت‌های سیستم مشخص گردد. پروفایل‌ها به اکانت‌های ساخته شده تخصیص داده می‌شوند. دسترسی کنترلی پروفایل به هر دو حالت GUI و CLI فورتی آنالایزر داده می‌شود. سه پروفایل از پیش تعریف شده در سیستم وجود دارد:

Restricted_User	**پروفایلی است که کاربر محدود شده و هیچ دسترسی سیستمی برای آن فعال نگردیده است و تمام دسترسی‌های آن به دستگاه به صورت فقط خواندنی می‌باشد.**
Standard_User	**پروفایلی است که کاربر محدود شده و هیچ دسترسی سیستمی برای آن فعال نگردیده است و دسترسی خواندن و نوشتن برای دستگاه وجود دارد.**
Super_User	**تمام دسترسی‌های برای این کاربر وجود دارد. فقط قابلیت ویرایش را ندارد.**

این پروفایل‌ها حذف نمی‌شوند اما پروفایل‌های restricted و standard امکان ویرایش را دارند. پروفایل‌های جدید برحسب نیاز ساخته می‌شوند. فقط Super_user ها امکان مدیریت پروفایل‌های ادمین را دارند.

به مسیر System Settings> Admin> Profile بروید تا بتوانید پروفایل ادمین‌ها را مشاهده و مدیریت نمایید.



گزینه‌های زیر موجود می‌باشد:

Create New	یک پروفایل ادمین جدید ایجاد می‌شود.
Edit	پروفایل انتخاب شده ویرایش می‌شود.
Delete	پروفایل/ پروفایل‌های انتخاب شده حذف می‌شوند.
Search	پروفایل‌های ادمین مورد جستجو قرار می‌گیرند.
اطلاعات زیر نمایش داده می‌شود.	
Name	نامی که ادمین برای لاگین از آن استفاده می‌کند.
Type	نوع پروفایل مشخص می‌گردد.
Description	یک توضیح از سیستم و دستگاهی که اجازه دسترسی به آن داده شده است. این توضیح برای پروفایل انتخابی است.

مجوزها

جدول زیر حاوی لیستی از دسترسی‌های پیش فرض برای پروفایل‌های administrator است.

وقتی Read-Write انتخاب می‌شود، کاربر امکان مشاهده و ایجاد تغییرات در سیستم را دارد. وقتی Read-Only انتخاب می‌شود، کاربر اطلاعات را فقط مشاهده می‌کند. وقتی None انتخاب می‌شود، کاربر امکان مشاهده و اعمال تغییرات در سیستم فورتی آنالایزر را ندارد.

Setting	Super User	Standard User	Restricted User
System Settings system-setting	Read-Write	None	**None**
Administrative Domain adom-switch	Read-Write	Read-Write	**None**
Device Manager device-manager	Read-Write	Read-Write	**Read-Only**
Add/Delete Devices/Groups	Read-Write	Read-Write	**None**

Log View/FortiView/NOC log-viewer	Read-Write	Read-Write	**Read-Only**
Event Management event-management	Read-Write	Read-Write	**Read-Only**
Reports report-viewer	Read-Write	Read-Write	**Read-Only**
CLI only settings			
device-wan-link-load-balance	Read-Write	Read-Write	**Read-Only**
device-ap	Read-Write	Read-Write	**Read-Only**
device-forticlient	Read-Write	Read-Write	**Read-Only**
device-fortiswitch	Read-Write	Read-Write	**Read-Only**
realtime-monitor	Read-Write	Read-Write	**Read-Only**

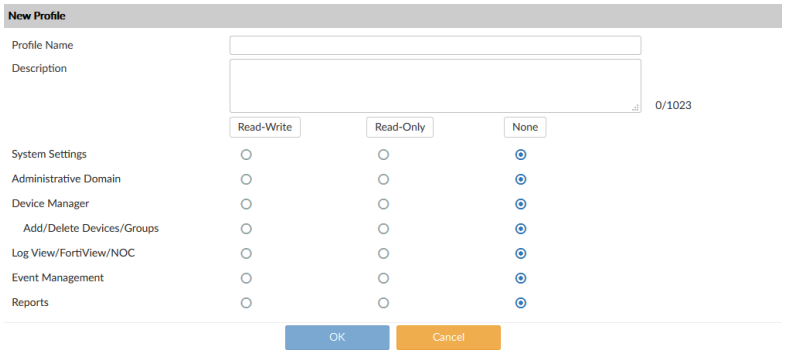
ایجاد پروفایل‌های ادمین

برای ایجاد پروفایل جدید ادمین، با اکانتی که دسترسی‌های لازم را دارد لاگین نمایید. این دسترسی‌ها یعنی ادمینی که اکانت آن در پروفایل super user قرار دارد.

ساختن پروفایل ادمین دلخواه:

۱. به مسیر System Settings> Admin> Profile بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید. پنجره New Profile برای شما نمایش داده می‌شود.



۳. تنظیمات زیر را انجام داده و سپس بر روی دکمه OK کلیک کنید تا پروفایل ادمین جدید ایجاد شود.

Profile Name	نامی برای پروفایل خود انتخاب نمایید.
Description	برای پروفایل توضیحی بنویسید. این کار اجباری نیست اما یک توضیح مناسب کمک شایانی به شناسایی پروفایل می‌کند که برای چه کسانی ایجاد شده و در چه سطحی تنظیم گردیده است.
Permissions	انتخاب دسترسی None، Read Only، Read-Write برای گروه‌هایی که نیاز دارند.

ویرایش پروفایل‌های ادمین

برای ویرایش پروفایل‌های ادمین باید با اکانتی لاگین کنید که دسترسی‌های لازم را داشته یا جزو پروفایل super user باشد. نام پروفایل‌ها قابل ویرایش نیست. پروفایل super user قابلیت ویرایش را ندارد. همچنین پروفایلی که از قبل تعریف شده است امکان حذف را ندارد.

ویرایش ادمین:

۱. به مسیر System Settings> Admin> Profile بروید.

۲. روی پروفایل دابل کلیک کنید یا بر روی یک پروفایل راست کلیک کرده و سپس گزینه Edit را انتخاب نمایید. پنجره Edit Profile باز می‌شود.

۳. تنظیماتی که باید را ویرایش کنید و در انتها با انتخاب گزینه OK تغییرات را اعمال نمایید.

حذف کردن پروفایل‌های ادمین

با اکانتی که دسترسی‌های لازم را دارد لاگین کنید. پروفایل‌هایی که از قبل تعریف شده‌اند امکان حذف را ندارند.

حذف کردن یک پروفایل:

۱. به مسیر System Settings> Admin> Profile بروید.

۲. پروفایل/ پروفایل‌هایی که درنظر دارید حذف شوند را انتخاب نمایید.

۳. از نوار ابزار بر روی Delete کلیک کنید و یا راست کلیک کرده و گزینه Delete را انتخاب نمایید.

٤. با انتخاب OK تایید می‌کنید که پروفایل/ پروفایل‌های انتخابی حذف شوند.

احراز هویت Authentication

سیستم فورتی آنالایزر از روش‌های زیر جهت احراز هویت پشتیبانی می‌کند.

1.local

2.remotly with RADIUS

3.LDAP

4.TACACS+

5.PKI

برای استفاده از احراز هویت به صورت PKI، قبل از ساخت اکانت ادمین باید تنظیمات لازم انجام شود. برای استفاده از سرورهای Remote Authentication باید تنظیمات در دستگاه فورتی آنالایزر را پیکربندی کنید. سرورهای احراز هویت ریموتی که به صورت LDAP کار می‌کنند امکان اضافه شدن به تمام ADOMها یا یک ADOM خاص را دارند.

Public Key Infrastructure

احراز هویت به صورت Public Key Infrastructure از سرتیفیکیت X.509 استفاده می‌کند که لیستی از peer ها، گروه‌های peer و گروه‌های کاربران و وضعیت پذیرش و عدم پذیرش را اعلام می‌کند. ادمین‌ها جهت احراز هویت موفقیت آمیز فقط به یک سرتیفیکیت X.509 نیاز دارند. نام کاربری یا کلمه عبوری مورد نیاز نمی‌باشد.

برای استفاده از احراز هویت به صورت PKI بحث authentication باید قبل از ساخت اکانت‌های ادمین پیکربندی شود. همچنین گواهینامه‌های امنیتی زیر نیز مورد نیاز است:

- یک گواهینامه X.509 برای ادمین فورتی منیجر
- یک گواهینامه X.509 از CA

اخذ CA سرتیفیکیت:

۱. روی FortiAuthenticator لاگین کنید.

۲. به مسیر Certificate Management> End Entities> Users بروید.

۳. Certificate را انتخاب کرده و از نوار ابزار Export را انتخاب نمایید تا بر روی کامپیوتر شما ذخیره شود. نام سرتیفیکیت ذخیره شده بر روی کامپیوتر admin_fortinet.com.p12 خواهد بود.

وارد کردن CA Certificate در داخل فورتی آنالایزر

۱. بر روی فورتی آنالایزر لاگین کنید.

۲. به مسیر System Settings> Certificates> CA Certificates بروید.

۳. بر روی Import کلیک کنید و فایل ca_fortinet.com.crt را از داخل کامپیوتر خود مسیریابی نمایید. سرتیفیکیت با نام CA_Cert_1 نمایش داده می‌شود.

ایجاد کردن اکانت ادمین PKI جدید:

۱. به مسیر System Settings> Admin> Administrator بروید.

۲. بر روی Create New کلیک کنید. کادر محاوره‌ای New Administrator باز می‌شود.

۳. برای نوع Admin گزینه PKI را انتخاب نمایید.

٤. توضیحی برای PKI ادمین در فیلد Subject وارد نمایید.

٥. از لیست دراپ دان موجود CA سرتیفیکیت را انتخاب کنید.

٦. با انتخاب OK اکانت ادمین جدید ساخته می‌شود.

احراز هویت PKI با دستور زیر فعال می‌شود:

```
Config system global
Set clt-cert-reg enable
End
```

اگر می‌خواهید از احراز هویت PKI استفاده کنید باید وقتی به محیط گرافیکی فورتی آنالایزر متصل می‌شوید، از پروتکل HTTPS استفاده نمایید.

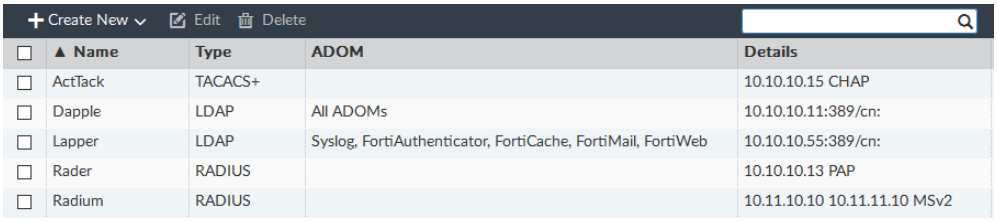
وقتی هر دو دستور set clt-cert-req و set admin-https-pki-required فعال می‌شوند، فقط ادمین‌هایی که از PKI استفاده می‌کنند قابلیت اتصال به محیط گرافیکی فورتی آنالایزر را دارند.

مدیریت سرورهای Remote authentication

سیستم فورتی آنالایزر از احراز هویت به صورت ریموت پشتیبانی می‌کند و این اتفاق با استفاده از RADIUS،LDAP و یا TACACS+ رخ می‌دهد. برای استفاده از این قابلیت، باید سرورهای مورد نظر پیکربندی شوند.

فقط از طریق محیط CLI ویرایش، حذف و یا اضافه کردن سرورهای احراز هویت راه دور به گروه‌های مربوطه وجود دارد.

به مسیر System Settings> Admin> Remote Authentication Server بروید تا بتوانید سرورها را مدیریت کنید.



گزینه‌های زیر موجود می‌باشند:

Create New	**یک LDAP، RADIUS یا TACACS+ ایجاد نمایید.**
Edit	**remote authentication سرور را ویرایش کنید.**
Delete	**remote authentication سرور را حذف کنید.**
اطلاعات زیر نمایش داده می‌شود	
Name	**نام سرور مشخص می‌شود.**
Type	**نوع سرور: LDAP،RADIUS ،TACACS+**
ADOM	**ادمین دامین‌هایی که به سرور متصل شده‌اند احراز هویت راه دور می‌گردند.**
Details	**جزئیاتی مانند IP آدرس سرورها مشخص گردیده است.**

ویرایش remote authentication servers

برای ویرایش سرور باید با اکانتی لاگین کنید که دسترسی‌های لازم را داشته باشد. نام سرور قابلیت ویرایش را ندارد.

ویرایش سرور احراز هویت راه دور

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. بر روی سرور دابل کلیک کنید، سپس راست کلیک کرده و از منوی باز شده گزینه Edit را انتخاب نمایید.

۳. تغییرات لازم را اعمال نموده و با زدن OK آنها را اعمال نمایید.

حذف سرورهای احراز هویت ریموت

برای حذف سرورها باید دسترسی‌های لازم را داشته و یا عضو پروفایل super user باشید.

حذف کردن یک سرور احراز هویت راه دور:

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. سرور یا سرورهایی را که می‌خواهید حذف شوند را انتخاب کنید.

۳. از نوار ابزار Delete را انتخاب نمایید یا با راست کلیک گزینه Delete را بزنید.

٤. از قسمت تایید OK را انتخاب کنید تا کار حذف سرور/ سرورها انجام شود.

LDAP سرورها

Lightweight Directory Access Protocol پروتکلی اینترنتی است که برای نگهداری دیتاهایی مانند دپارتمان‌ها، افراد،گروه‌ها، پسوردها، ایمیل آدرس‌ها و پرینترها مورد استفاده قرار می‌گیرد. LDAP می‌تواند شامل یک طرح ارائه دیتا، مجموعه‌ای از عملیات تعریف شده و یا یک درخواست/ جواب شبکه‌ای باشد.

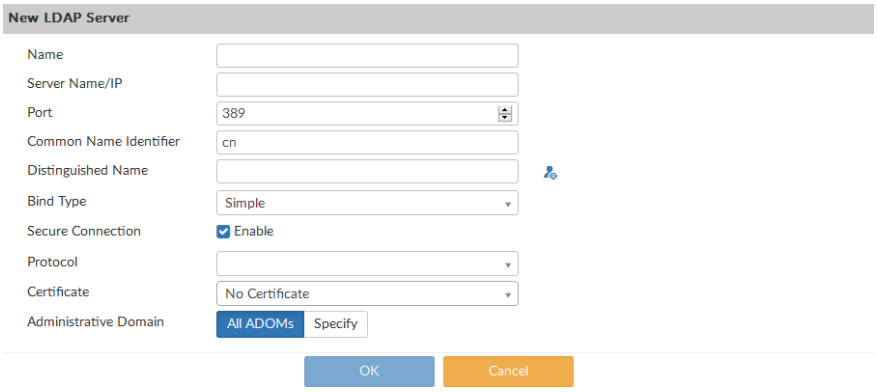
اگر LDAP را تنظیم کرده‌اید و ادمینی دارید که با استفاده از LDAP سرور احراز هویت می‌شود، دستگاه فورتی آنالایزر اعتبارسنجی ادمین را برای LDAP سرور ارسال می‌کند تا احراز هویت انجام شود. اگر LDAP سرور بتواند احراز هویت را انجام دهد، ادمین با موفقیت احراز هویت می‌شود و بر روی دستگاه لاگین می‌کند. اگر LDAP نتواند این پروسه را انجام دهد دستگاه فورتی آنالایزر اجازه اتصال را نمی‌دهد و اصطلاحا کانکشن ریفیوز می‌شود.

برای استفاده از LDAP سروری که احراز هویت ادمین‌ها را انجام می‌دهد باید قبل از پیکربندی اکانت‌های ادمین سرور LDAP را ساخته و تنظیمات لازم را انجام دهید.

یک LDAP سرور اضافه کنید:

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. از نوار ابزار Create New> LDAP Server را انتخاب کنید. پنجره New LDAP Server باز می‌شود.



۳. تنظیمات زیر را انجام داده و سپس بر روی OK کلیک کنید تا LDAP سرور اضافه شود.

Name	نامی را جهت شناسایی **LDAP** سرور وارد نمایید.
Server Name/IP	**IP** آدرس یا **FQDN** سرور **LDAP** را وارد نمایید.
Port	پورتی را برای ترافیک **LDAP** مشخص نمایید. پورت پیش فرض **389** است.
Common Name Identifier	نام متعارف شناسایی برای **LDAP** سرور می‌باشد. اغلب **LDAP** سرورها از **cn** استفاده می‌کنند. هرچند، بعضی از سرورها از نام‌های شناسایی متعارف دیگری مثل **UID** استفاده می‌کنند.
Distinguished Name	این نام برای شناسایی **LDAP** سرور مورد استفاده قرار می‌گیرد. نام **distinguished** سلسله مراتب دیتابیس **LDAP** را برای شناسه مشترک نشان می‌دهد. با زدن دکمه **query distinguished** یک پرس و جو از **LDAP** سرور انجام می‌شود و نتیجه نمایش داده می‌شود.

Bind Type	**انتخاب نوع اتصال برای احراز هویت LDAP: Simple، Anonymous و Regular**
User DN	**وقتی Bind Type را بر روی Regular قرار می‌دهید، کاربر DN را وارد نمایید.**
Password	**وقتی Bind Type را بر روی Regular قرار می‌دهید، کلمه عبور را وارد کنید.**
Secure Connection	**جهت ایجاد ارتباط امن LDAP سرور از این گزینه استفاده می‌کنیم.**
Protocol	**وقتی Secure Connection فعال باشد، LDAPS یا STARTTLS قابل انتخاب است.**
Certificate	**وقتی Secure Connection فعال می‌شود، از لیست دراپ دان سرتیفیکیت را انتخاب نمایید.**
Administrative Domain	**ADOMهایی انتخاب می‌گردند که با این سرور لینک خواهند شد.**

سرورهای RADIUS

Remote Authentication Dial-in User یک احراز هویت کاربر و سیستم اکانتینگ شبکه‌ای است. وقتی کاربران نام کاربری و کلمه عبور خود را وارد می‌کنند می‌توانند به سرور متصل شوند. این اطلاعات به RADUIS سرور ارسال و سرور کاربر را تایید می‌کند و اجازه دسترسی به شبکه را به او می‌دهد.

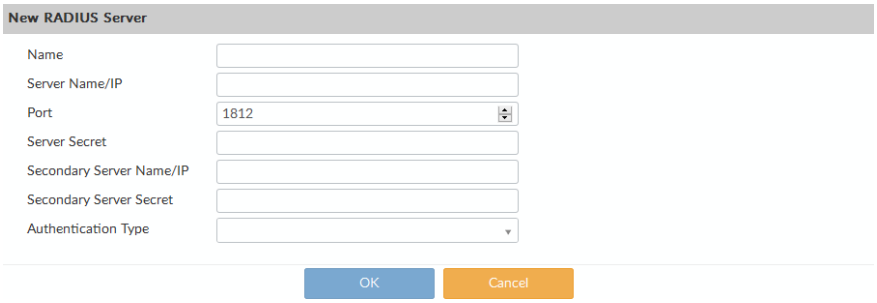
امکان ساخت و ویرایش سرورRADIUS در لیست سرورهای وارد شده جهت احراز هویت ادمین‌ها وجود دارد. وقتی اکانت ادمینی با RADIUS سرور تنظیم می‌شود، دستگاه فورتی آنالایزر از RADIUS سرور در جهت تایید پسورد ادمین در هنگام لاگین استفاده می‌کند. در ضمن پسورد بر روی دستگاه فورتی آنالایزر ذخیره نمی‌شود.

جهت استفاده از RADIUS سرور برای احراز هویت ادمین‌ها، تنظیمات مربوط به سرور باید قبل از ساخت اکانت‌های ادمین انجام شود.

یک RADIUS سرور اضافه کنید:

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. از نوار ابزار Create New> RADIUS Server را انتخاب نمایید. پنجره New RADIUS Server باز می‌شود.



۳. تنظیمات زیر را انجام داده و سپس بر روی OK کلیک کنید تا RADIUS سرور اضافه شود.

Name	نامی را برای شناسایی **RADIUS** سرور وارد نمایید.
Server Name/IP	**IP** آدرس یا **FQDN** برای سرور انتخاب کنید.
Port	پورتی که قرار است ترافیک **RADIUS** سرور از آن عبور نمایید. پورت پیش فرض **1812** است. بعضی از **RADIUS** سرورها از **1645** استفاده می‌کنند.
Server Secret	رمز مشخص شده **RADIUS** سرور را وارد کنید.
Secondary Server Name/IP	**IP** آدرس یا **FQDN** مربوط به **RADIUS** سرور دوم را مشخص نمایید.
Secondary Server Secret	رمز مشخص شده **RADIUS** سرور دوم را وارد کنید.
Authentication Type	نوع احراز هویت **RADIUS** سرور مشخص شود.

سرورهای TACACS+

Terminal Access Controller Access-Control System پروتکل احراز هویت راه دوری است که دسترسی کنترلی برای روترها، سرورهای شبکه و سایر دستگاه‌های تحت شبکه با یک یا چند سرور مرکزی فراهم می‌کند. این

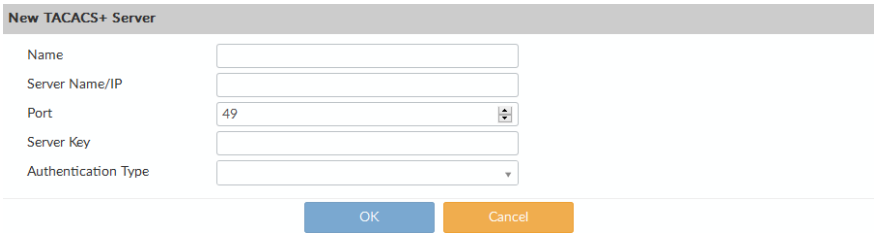
سرور به یک کلاینت اجازه می‌دهد تا نام کاربری و کلمه عبور را پذیرفته و یک query برای سرور احراز هویت TACACS ارسال کند. سرور مشخص خواهد کرد که کدام درخواست قبول یا رد شود و همچنین جوابی مبنی بر رد یا پذیرش درخواست برای کاربر ارسال می‌شود. پورت پیش فرض TACACS بر روی TCP عدد 49 می‌باشد.

اگر برای احراز هویت ادمین‌های خود از سرور TACACS استفاده می‌کنید باید بدانید که از قبل تنظیمات اکانت‌های خود را انجام دهید.

یک +TACACS سرور اضافه کنید:

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. از نوار ابزار Create New> TACACS+ Server انتخاب کنید. پنجره New TACACS+ باز می‌شود.



۳. تنظیمات را بر اساس توضیحات زیر انجام داده و سپس بر روی OK کلیک کنید تا سرور +TACACS اضافه شود.

Name	نامی برای شناسایی سرور **+TACACS** وارد کنید.
Server Name/IP	**IP** آدرس یا **FQDN** برای سرور **+TACACS** وارد کنید.
Port	**پورتی برای ترافیک +TACACS وارد نمایید. پورت پیش فرض 49 است.**
Server Key	**کلیدی جهت دسترسی به سرور +TACACS وارد کنید. کلید حداکثر می‌تواند ۱۶ کاراکتر طول داشته باشد.**
Authentication Type	**نوع احراز هویت RADIUS سرور انتخاب شود.**

تنظیمات کلی administration

صفحه administration settings گزینه‌هایی برای تنظیمات عمومی و کلی جهت دسترسی ادمین‌ها به دستگاه فورتی آنالایزر دارد. این تنظیمات شامل:

- پورت‌های دسترسی ادمین‌ها بر روی پروتکل‌های HTTPS و HTTP فراهم می‌گردد.

در جهت بهبود امنیت می‌توانید پورت پیش فرض را تغییر داده تا اتصال ادمین‌ها از طریق آن پورت صورت گیرد. وقتی پورت تغییر می‌کند جهت اتصال باید به صورت زیر آدرس را وارد نمایید:

https://<ip_address>:<port>

برای مثال، اگر به فورتی آنالایزر متصل شوید از پورت ۸۰۸۰ استفاده می‌کنید و می‌توانید URL زیر را وارد نمایید:

https://192.168.1.99:8080

وقتی پورت پیش فرض را برای HTTPS،HTTP ، Telnet و SSH تغییر می‌دهید مطمئن شوید که شماره پورت یونیک باشد.

- تنظیمات زمان آغاز بکار سیستم

به صورت پیش فرض، اگر برای ۵ دقیقه فعالیتی بر روی سیستم نباشد session مربوط به GUI قطع خواهد شد. اگر بر روی سیستم کلاینتی صفحه مدیریت باز باشد با گذشت این زمان صفحه بسته می‌شود.

- زبان GUI

برای کار در محیط GUI بهتر است زبانی که تمایل دارید با آن کار کنید را انتخاب نمایید.

- زمینه GUI

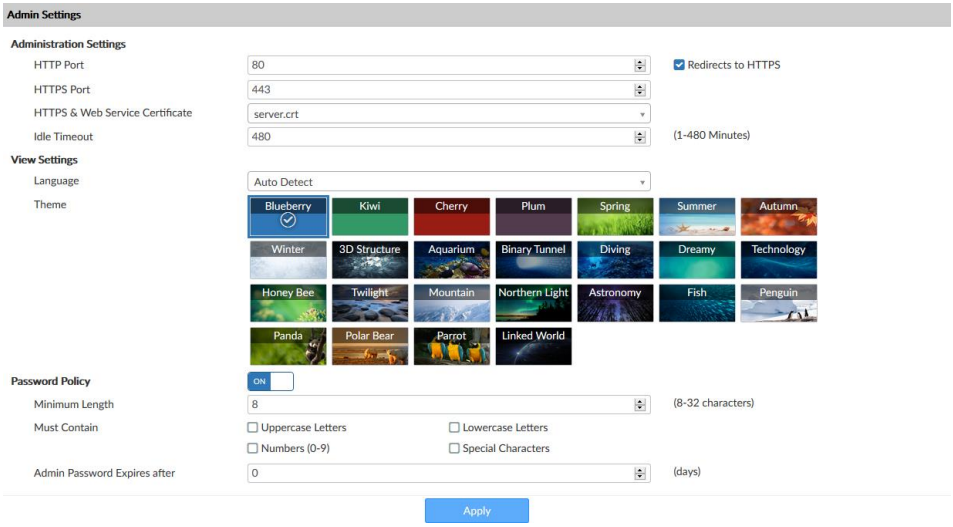
رنگ زمینه پیش فرض محیط GUI با نام Blueberry شناخته می‌شود. این امکان برای شما فراهم شده که رنگ یا تصویر دیگری را انتخاب نمایید.

- پالیسی کلمه عبور

پالیسی‌های پسورد برای ادمین‌ها اعمال می‌شود. فقط ادمین‌هایی که در پروفایل super user قرار دارند امکان انجام این تنظیمات را دارند. این تنظیمات به صورت کلی به تمام ادمین‌های فورتی آنالایزر اعمال می‌گردد.

پیکربندی تنظیمات administration:

۱. به مسیر System Settings> Admin> Admin Settings بروید.



۲. تنظیمات را بر اساس نیاز خود به صورت زیر انجام دهید سپس جهت ذخیره بر روی اکانت ادمین بر روی Apply کلیک نمایید.

Administration Settings	
HTTP Port	پورت **TCP** مورد استفاده جهت دسترسی را وارد نمایید. به صورت پیش فرض این پورت **80** می‌باشد.
HTTPS Port	پورت **TCP** که جهت دسترسی به صورت **HTTPS** می‌باشد را وارد نمایید. به صورت پیش فرض **443** می‌باشد.
HTTPS & Web Service Server Certificate	از لیست دراپ دان سرتیفیکیت را انتخاب کنید.

Idle Timeout	مدت زمانی که سیستم بلااستفاده بوده و ادمین‌ها باید مجددا لاگین نمایند که این زمان با دقیقه مشخص می‌شود و از ۱ تا ٤٨٠ دقیقه قابل تنظیم است.
View Settings	
Language	از لیست زبان دلخواه را انتخاب می‌کنیم.
Theme	انتخاب تِم برای محیط GUI انجام می‌شود.
Password Policy	امکان فعال کردن پالیسی‌ها در مورد کلمه عبور وجود دارد.
Minimum Length	انتخاب کمترین طول پسورد، از ۸ تا ۳۲ کاراکتر که پیش فرض ۸ کاراکتر می‌باشد
Must Contain	انتخاب نوع کاراکترهای یک پسورد که شامل چه مواردی باشد.
Admin Password Expire after	انتخاب مدت زمان اعتبار پسورد بعد از آخرین تغییری که صورت گرفته است.

پالیسی پسورد

امکان فعال کردن پالیسی‌های مرتبط با کلمات عبور در فورتی آنالایزر وجود دارد.

تنظیمات مربوط به پسورد پالیسی:

۱. به مسیر System Settings> Admin> Admin Settings بروید.

۲. بر روی گزینه Password Policy کلیک کنید.

۳. تنظیمات را بر اساس توضیحات زیر انجام داده سپس با کلیک بر روی گزینه Apply پسورد پالیسی را اعمال کنید.

Minimum Length	**مشخص نمودن حداقل تعداد کاراکتری که یک کلمه عبور باید داشته باشد. از ۸ تا ۳۲ کاراکتر است که عدد پیش فرض ۸ کاراکتر می‌باشد.**
Must Contain	**مشخص کردن نوع کاراکترهای یک پسورد، کوچک یا بزرگ بودن کلمات، اعداد و کاراکترهای ویژه**
Admin Password Expire after	**مدت زمانی که کلمات عبور اعتبار دارند در این بخش مشخص می‌گردد. وقتی زمان به اتمام برسد ادمین باید پسورد جدید برای خود انتخاب نماید.**

قفل شدن کلمه عبور و تلاش مجدد

به صورت پیش فرض، سه بار فرصت جهت وارد کردن کلمه عبور برای ادمین وجود دارد. یعنی ادمین می‌تواند برای ورود به اکانت خود سه بار تلاش کند. بعد از این سه بار اکانت برای ۶۰ ثانیه مسدود می‌شود. جهت دلخواه‌سازی این زمان و تعداد تلاش‌ها جهت ورود می‌توانیم از طریق محیط CLI تنظیمات لازم را اعمال نماییم.

تنظیم مدت زمان قفل شدن سیستم:

۱. دستورات زیر را در محیط CLI وارد نمایید:

```
Config system global
      Set admin-lockout-duration <seconds>
End
```

تنظیم تعداد تلاش‌های متناوب جهت اتصال:

۱. دستورات زیر را در محیط CLI وارد نمایید.

```
config system global
    set admin-lockout-threshold <failed_attempts>
end
```

مثال

در این مثال، کاربر بعد از یکبار وارد کردن کلمه عبور اشتباه اکانت به مدت ۵ دقیقه قفل می‌شود.

```
Config system global
```

```
    Set admin-lockout-duration 300
    Set admin-lockout-threshold 1
End
```

زبان

محیط GUI از زبان‌های زیر پشتیبانی می‌کند:

- انگلیسی
- چینی
- ژاپنی
- کره ای

به صورت پیش فرض، زبان GUI در حالت انتخاب خودکار قرار دارد. این انتخاب بدین صورت انجام می‌شود که زبان دستگاه بر اساس زبان سیستم انتخاب می‌شود. در صورتی که زبان سیستم شما در موارد انتخابی فورتی آنالایزر نباشد به صورت خودکار زبان انگلیسی انتخاب می‌گردد.

تغییر زبان دستگاه:

۱. به مسیر System Settings> Admin> Admin Settings بروید.
۲. در قسمت View Settings، فیلد Language، یک زبان انتخاب نمایید یا از لیست Auto Detect را انتخاب کنید.
۳. با کلیک بر روی Apply تغییرات انجام شده بر روی زبان را اعمال نمایید.

زمان بیکاری سیستم

در جهت افزایش امنیت سیستم بهتر است دوره زمان بیکاری سیستم کوتاه باشد. به صورت پیش فرض، اگر ادمین‌ها برای ۵ دقیقه با سیستم کاری انجام ندهند sessionها قطع می‌گردد. توصیه می‌شود زمان بیکاری سیستم طوری تعریف شود تا زمانی که سیستم بلااستفاده است کسی امکان استفاده از محیط GUI را نداشته باشد. توجه کنید که زمان بیکاری سیستم می‌تواند از ۱ دقیقه تا ٤٨٠ دقیقه تنظیم شود.

برای تغییر زمان بیکاری:

۱. به مسیر System Settings> Admin> Admin Settings بروید.

۲. گزینه Idle Timeout را بر اساس نیاز تغییر دهید.

۳. Apply کنید.

احراز هویت دو مرحله ای

برای انجام احراز هویت به صورت دو مرحله‌ای باید تنظیمات را بر روی دستگاه‌های زیر انجام دهید:

- فورتی آنالایزر
- فورتی authenticator
- فورتی توکن

تنظیمات فورتی Authenticator:

در ابتدا باید یک کاربر لوکال و یک کلاینت RADIUS ایجاد کنید.

قبل از اقدام، مطمئن شوید که فورتی Authenticator را تنظیم نموده‌اید. ورودی NAS برای فورتی آنالایزر ایجاد کرده و فورتی توکن را import کنید.

یک کاربر داخلی بسازید:

۱. به مسیر Authentication> User Management> Local Users بروید.

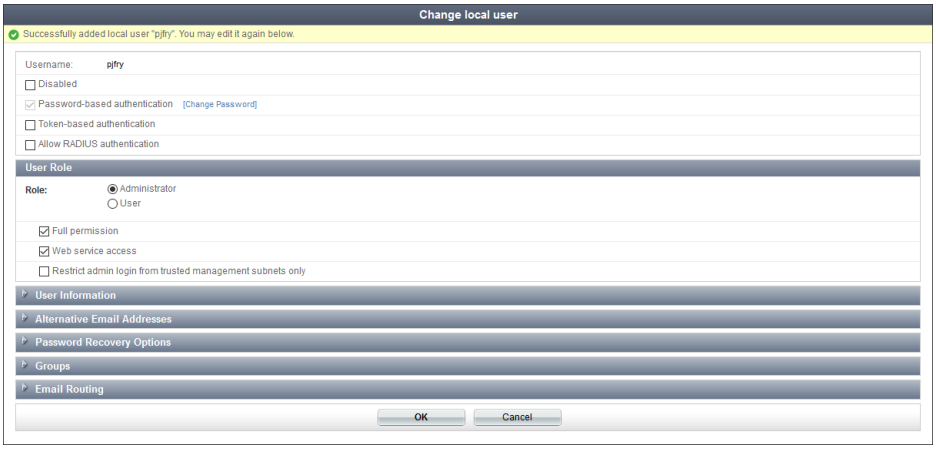
۲. در نوار ابزار بر روی Create New کلیک کنید.

۳. تنظیمات زیر را انجام دهید:

Username	برای کاربر لوکال یک نام کاربری وارد نمایید.
Password creation	از لیست کلمه عبور مشخص شده‌ای را انتخاب کنید.
Password	یک کلمه عبور وارد نمایید. کلمه عبور حداقل ۸ کاراکتر باشد.

Password confirmation	کلمه عبور را مجددا وارد نمایید.
Allow RADIUS authentication	اجازه انجام احراز هویت از طریق **RADIUS** را فعال کنید.
Role	برای کاربر جدید وظیفه‌ای مشخص نمایید.
Enable account expiration	به صورت دلخواه، زمان منقضی شدن اکانت را مشخص کنید.

٤. با کلیک بر روی OK صفحه Change local user باز می‌شود.



٥. تنظیمات را بر اساس موارد زیر انجام داده و سپس بر روی OK کلیک نمایید.

Disable	انتخاب این گزینه سبب غیرفعال شدن کاربر لوکال می‌شود.
Password-based authentication	این گزینه را بدون تغییر بگذارید.
Token-based authentication	فعال سازی احراز هویت بر اساس توکن انجام می‌شود.
Deliver token code by	انتخاب روش دریافت توکن بوسیله **FortiToken** با ایمیل یا پیام کوتاه انجام شود.
Allow RADIUS authentication	اجازه احراز هویت با استفاده از **RADIUS** در این قسمت داده می‌شود
Enable account expiration	به صورت دلخواه، حالت منقضی شدن اکانت را انتخاب نمایید.

User Role	
Role	کاربر یا ادمین را انتخاب نمایید.
Full Permission	با انتخاب این گزینه حالت **full access** خواهیم داشت.
Web Service	اجازه دسترسی از طریق وب سرویس داده می‌شود، این دسترسی باعث می‌گردد ادمین امکان ریست کردن **API** بوسیله برنامه کلاینت را داشته باشد.
Restrict admin login from trusted management subnets only	انتخاب این گزینه سبب محدود سازی لاگین ادمین از ساب نت‌های مشخص می‌شود.
Allow LDAP Browsing	این قسمت اجازه **LDAP Browsing** را می‌دهد.

ایجاد یک RADIUS کلاینت:

۱. به مسیر Authentication> RADIUS Service> Clients بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید.

۳. تنظیمات را بر اساس توضیحات زیر انجام داده و سپس بر روی OK کلیک کنید.

Name	یک نام برای **RADIUS** کلاینت خود وارد نمایید.
Client name/IP	**IP** آدرس یا **FQDN** فورتی آنالایزر را وارد کنید.
Secret	سرور **secret** را وارد نمایید. این مقدار باید با سرور **RADIUS** وارد شده در تنظیمات فورتی آنالایزر یکسان باشد.
First profile name	نگاهی به راهنمای **FortiAuthenticator** داشته باشید.
Description	توضیحاتی برای **RADIUS** کلاینت وارد نمایید.

Apply this profile based on RADIUS attributes	برای اعمال پروفایل بر اساس ویژگی‌های **RADIUS** این گزینه را انتخاب کنید.
Authentication method	انتخاب احراز هویت دو مرحله‌ای از لیست گزینه‌ها صورت گیرد.
Username input format	فرمت نام کاربری انتخاب گردد.
Realms	تنظیم **realms** صورت گیرد.
Allow MAC-based authentication	پیکربندی این قسمت به صورت اختیاری می‌باشد.
Check machine authentication	بررسی بر اساس احراز هویت انجام و به گروه‌ها بر اساس صحت احراز هویت اعمال شود.
Enable captive portal	فعال کردن پورتال‌های مختلف در این قسمت انجام می‌شود.
EAP types	تنظیمات به صورت اختیاری می‌باشد.

پیکربندی فورتی آنالایزر

بر روی فورتی آنالایزر، تنظیماتی مانند ساختن ادمینی که از RADIUS سرور برای احراز هویت استفاده می‌کند و همچنین پیکربندی RADIUS سرور مورد نیاز است.

پیکربندی **RADIUS** سرور:

۱. به مسیر System Settings> Admin> Remote Authentication Server بروید.

۲. از نوار ابزار Create New> RADIUS سرور را انتخاب نمایید.

۳. تنظیمات را بر اساس توضیحات زیر انجام داده و سپس بر روی OK کلیک کنید.

Name	انتخاب نام جهت شناسایی **FortiAuthenticator**
Server Name/IP	**IP** آدرس یا **FQDN** را وارد نمایید.
Server Secret	رمز ارتباطی **FortiAuthenticator** را وارد کنید.

Secondary Server Name/IP	**IP آدرس یا FQDN مربوط به دومین FortiAuthenticator را وارد نمایید. البته در شرایطی که وجود داشته باشد.**
Secondary Server Secret	**رمز ارتباطی FortiAuthenticator دوم را در صورت وجود وارد نمایید.**
Port	**پورتی که قرار است ترافیک FortiAuthenticator از آن عبور کند را وارد نمایید.**
Authentication Type	**انتخاب مدل احراز هویت برای FortiAuthenticator اگر گزینه Any را انتخاب نمایید فورتی آنالایزر تمام انواع احراز هویت را می‌پذیرد.**

ساخت و ایجاد administrator

۱. به مسیر System Settings> Admin> Administrator بروید.

۲. از نوار ابزار گزینه Create را انتخاب نمایید.

۳. تنظیمات را پیکربندی کرده و از لیست RADIUS سرورهای پیشین یک RADIUS سرور را اضافه کنید.

٤. برای ذخیره‌سازی تنظیمات بر روی OK کلیک کنید.

آزمودن تنظیمات:

۱. بوسیله اعتبار جدید ایجاد شده تلاش نمایید تا به محیط گرافیکی فورتی آنالایزر متصل شوید.

۲. نام کاربری و کلمه عبور خود را وارد و سپس بر روی Login کلیک کنید.

۳. پین کد فورتی توکن را وارد نموده و سپس در فورتی آنالایزر لاگین کنید.

Device Manager

از قسمت Device Manager در جهت اضافه کردن، تنظیم و مدیریت دستگاه‌ها و VDOMها استفاده می‌شود.

اگر قابلیت‌های فورتی منیجر فعال باشد، مدیریت دستگاه با فورتی منیجر خواهد بود. بعد از اضافه یا ثبت کردن دستگاه یا VDOM، فورتی آنالایزر شروع به جمع آوری لاگ‌ها از دستگاه یا VDOM می‌کند. این امکان وجود دارد که فورتی آنالایزر خود را طوری تنظیم کنید که لاگ‌ها را برای دستگاه دیگری ارسال نماید.

ADOMs

امکان سازمان‌دهی دستگاه‌ها در ADOM وجود دارد تا مدیریت دستگاه‌ها راحت‌تر صورت پذیرد. امکان سازماندهی ADOMها بوسیله:

- Firmware version: تمام دستگاه‌های 5.4 در داخل یک ADOM گروه‌بندی می‌شوند. تمام دستگاه‌های 5.2 در داخل یک گروه دیگر قرار می‌گیرند.
- مناطق جغرافیایی: گروه‌بندی تمام دستگاه‌ها بر این اساس است که مناطق جغرافیایی مختلف بر اساس منطقه در ADOMهای مختلف قرار می‌گیرند.
- کاربران ادمین: گروه‌بندی دستگاه‌ها در ADOMهای مختلف بر اساس ادمین‌های مشخص صورت می‌گیرد.
- مشتریان: گروه‌بندی تمام دستگاه‌ها برای یک مشتری در داخل یک ADOM انجام می‌شود و برای سایر مشتریان در یک ADOM دیگر صورت می‌پذیرد.

امکان سفارشی سازی پروفایل برای هر ادمین وجود دارد این کار سبب می‌گردد تا تنظیمات و read-only ،write،read برای هر کدام از ادمین‌ها متفاوت باشد. وقتی ادمین اکانت جدیدی می‌سازد امکان ایجاد محدودیت جهت دسترسی به ADOM وجود دارد. این امر سبب افزایش کنترل می‌شود.

دستگاه‌های ثبت نشده:

از فورتی آنالایزر با نسخه 5.2 به بعد دستور

```
Config system global set unregister-pop-up
```

به صورت پیش فرض غیرفعال می‌باشد. وقتی دستگاهی جهت ارسال لاگ‌ها به فورتی آنالایزر پیکربندی می‌شود، دستگاه ثبت نشده در مسیر Device Manager> Devices Unregister نمایش داده می‌شود. امکان اضافه کردن دستگاه‌ها به ADOMهای خاص یا پاک کردن دستگاه‌ها از طریق نوار ابزار وجود دارد.

استفاده از فورتی منیجر جهت مدیریت دستگاه‌های فورتی آنالایزر:

امکان اضافه کردن دستگاه‌های فورتی آنالایزر به فورتی منیجر برای مدیریت متمرکز آنها وجود دارد. وقتی شما فورتی آنالایزر را به فورتی منیجر اضافه می‌کنید فورتی منیجر به صورت خودکار قابلیت‌های فورتی آنالایزر را فعال می‌کند. فورتی آنالایزر و فورتی منیجر باید نسخه‌های OS یکسانی داشته باشند و این نسخه‌ها باید حداقل 5.6 به بالا باشند.

در صفحه Device Manager پیامی مبنی بر مدیریت دستگاه توسط فورتی منیجر نمایش داده می‌شود و تمامی تغییرات باید از طریق فورتی منیجر انجام شود این امر بدلیل آن است که از تداخل تغییرات جلوگیری می‌کند. در بالای سمت راست این صفحه تصویر قفلی را مشاهده می‌کنید که اگر ADOM فعال شود نمایش دهنده یک آیکون قفل در کنار مدیریت ADOM بوسیله فورتی منیجر است. به خاطر داشته باشید که لاگ‌ها بر روی دستگاه فورتی آنالایزر ذخیره می‌شود و فورتی منیجر فقط وظیفه مدیریت دستگاه‌ها را برعهده دارد. انجام تنظیمات مربوط به ذخیره‌سازی لاگ‌ها بر روی دستگاه فورتی آنالایزر صورت می‌گیرد.

اضافه کردن دستگاه‌ها

دستگاه‌ها و VDOMها در فورتی آنالایزر ثبت و اضافه می‌شوند تا امکان ارسال لاگ‌ها برای فورتی آنالایزر ایجاد گردد. دستگاه‌هایی را می‌توانید در فورتی آنالایزر اضافه کنید که در جدول DVM معرفی شده‌اند.

امکان تنظیم دستگاه‌ها جهت ارسال لاگ به فورتی آنالایزر وجود دارد. برای مثال بعد از اضافه کردن و معرفی یک دستگاه فورتی‌گیت باید تنظیمات طوری انجام شود که لاگ‌ها برای فورتی آنالایزر ارسال گردد.

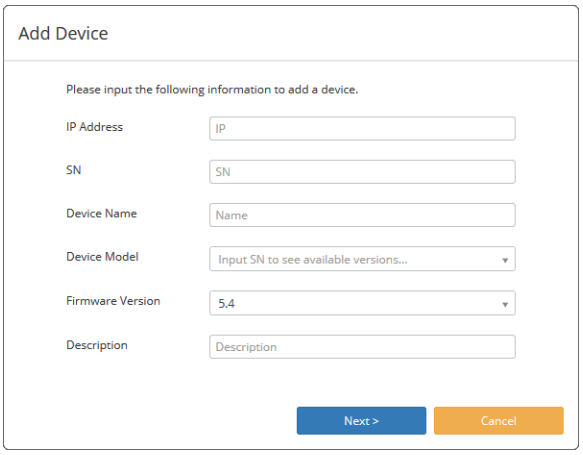
با استفاده از ویزارد دستگاه‌ها را اضافه نمایید

امکان اضافه کردن دستگاه‌ها از طریق ویزارد وجود دارد. وقتی دستگاهی را به فورتی آنالایزر معرفی می‌کنید لاگ‌های آن دستگاه به آنالایزر ارسال می‌شود.

اضافه کردن دستگاه‌ها با استفاده از ویزارد:

۱. اگر از ADOM استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Device Manager رفته و بر روی Add Device کلیک کنید.

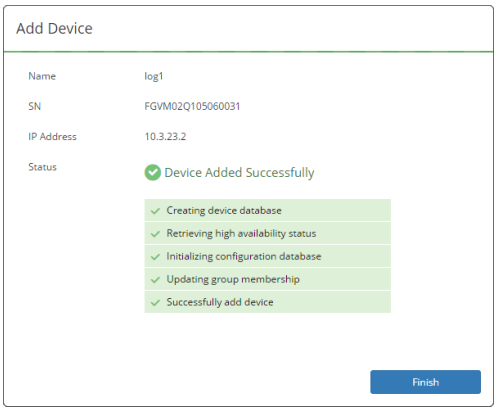


۳. تنظیمات را بر اساس توضیحات زیر انجام دهید:

IP Address	**IP آدرس دستگاه را وارد کنید.**
SN	**سریال دستگاه را وارد نمایید.**
Device Name	**نام دستگاه را وارد نمایید.**
Device Model	**مدل دستگاه را انتخاب نمایید.**
Firmware Version	**فریمور دستگاه را مشخص نمایید.**
Description	**توضیحاتی برای دستگاه وارد نمایید.**

٤. بر روی Next کلیک کنید.

دستگاه به ADOM اضافه شده و اگر این اتفاق با موفقیت انجام شود آماده است تا لاگ‌ها را برای دستگاه فورتی آنالایزر ارسال نماید.



۵. برای اتمام این قسمت و بسته شدن ویزارد کافی است بر روی Finish کلیک کنید.

اضافه کردن دستگاه‌ها به صورت دستی

امکان اضافه نمودن دستگاه‌هایی که در لیست پشتیبانی سیستم قرار دارند جهت ارسال لاگ‌ها مهیا شده است. این دستگاه‌ها به‌عنوان دستگاه ثبت نشده در روت ADOM نمایش داده می‌شوند. جهت مشاهده دستگاه‌های ثبت نشده کافی است بر روی Unregistered Devices کلیک نمایید. هنگامی که به صورت دستی یک دستگاه ثبت نشده را به فورتی آنالایزر اضافه می‌کنید این دستگاه شناسایی شده و دریافت لاگ‌ها آغاز می‌گردد.

اگر ADOMها فعال باشند، می‌توانید دستگاه را به یک ADOM تخصیص دهید. وقتی به صورت دستی چندین دستگاه را در یک زمان اضافه می‌کنید آنها به یک ADOM اضافه می‌شوند.

وقتی یک دستگاه حذف می‌شود یا یک ADOM از دستگاه فورتی آنالایزر پاک می‌شود لاگ فایل‌های RAW نیز پاک می‌گردند. لاگ‌های دیتابیس SQL پاک نمی‌شوند.

اضافه کردن دستی دستگاه‌ها:

۱. در ADOM روت، به قسمت Device Manager رفته و در نوار وضعیت بر روی Unregistered Devices کلیک کنید. چیزی که در این قسمت نمایش داده می‌شود دستگاه‌های ثبت نشده می‌باشد.

۲. دستگاه/ دستگاه‌های ثبت نشده را انتخاب نمایید، سپس بر روی Add کلیک کنید. صفحه Add Devices نمایش داده می‌شود.

۳. اگر ADOMs فعال باشد، ADOM را انتخاب نمایید.

٤. برای ثبت دستگاه OK کنید.

در این مرحله دستگاه اضافه شده و فورتی آنالایزر امکان دریافت لاگ از دستگاه را دارد.

اضافه کردن یک security fabric group

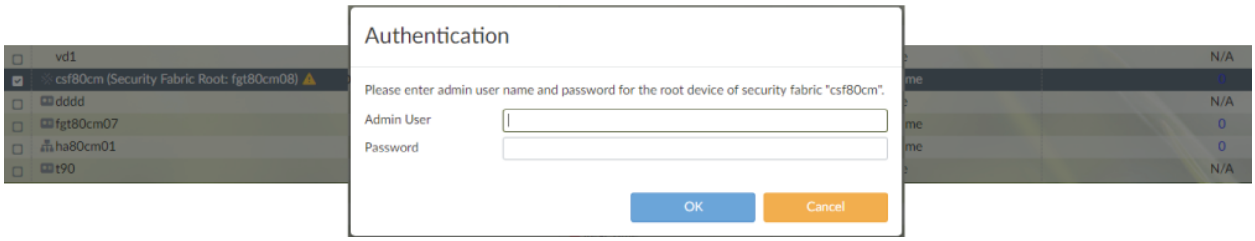
قبل از اضافه کردن fabric group به فورتی آنالایزر نیاز به ساخت و ایجاد یک فابریک گروه امنیتی در فورتی‌گیت می‌باشد.

اضافه کردن security fabric group:

۱. به مسیر Device Manager> Unregistered Devices بروید.

۲. تمام دستگاه‌های مرتبط با security fabric group ساخته شده در فورتی‌گیت را انتخاب نمایید.

۳. احراز هویت security fabric group بوسیله کلیک بر روی آیکون زرد رنگ اخطار کنار گزینه روت فورتی‌گیت صورت می‌پذیرد.



٤. مجوزهای احراز هویت را وارد نمایید. وقتی یکبار احراز هویت را در روت فورتی‌گیت انجام می‌دهید آیکون اخطار ناپدید می‌شود.

۵. بعد از احراز هویت، چند دقیقه‌ای طول میکشد تا به صورت خودکار دستگاه توسط فورتی آنالایزر شناسایی شود.

مدیریت دستگاه‌ها

ابزارها و دستوراتی در پنجره Device Manager وجود دارد که می‌توانیم در جهت مدیریت دستگاه‌ها و VDOMها از آنها استفاده نماییم.

نوار وضعیت سریع (مرور سریع وضعیت)

در بالای صفحه Device Manager گزینه مرور سریع وضعیت را مشاهده می‌کنید. نوار وضعیت سریع شامل تب‌های زیر می‌باشد:

- Device Total:

دستگاه‌های ثبت شده را نمایش می‌دهد.

- Device Unregistered

دستگاه‌های ثبت نشده را نمایش می‌دهد.

- Device Log Status Down

دستگاه‌های ثبت شده با وضعیت لاگ خاموش را نمایش می‌دهد.

- Storage Used

وضعیت فضای استفاده شده نمایش داده می‌شود.

ستون	توضیحات
Device Name	نام دستگاه نمایش داده می‌شود
IP Address	IP آدرس دستگاه نمایش داده می‌شود.
Platform	نمایش دهنده پلتفرم دستگاه می‌باشد.
Logs	شناسایی مواردی مانند اینکه آیا دستگاه با موفقیت لاگ‌ها را برای فورتی آنالایزر ارسال می‌کند. دایره سبز رنگ نمایش دهنده ارسال لاگ‌ها می‌باشد. دایره قرمز رنگ نمایش دهنده لاگ‌هایی است که ارسال نشده‌اند. آیکون قفل نمایش دهنده زمانی است که یک تانل امن برای ارسال لاگ‌ها از دستگاه به فورتی آنالایزر استفاده می‌کند.
Average Log Rate (Logs/Sec)	نرخ متوسطی است که لاگ برای فورتی آنالایزر ارسال می‌کند که این مقدار بر اساس ثانیه است.
Device Storage	میزان فضای اختصاص داده شده برای مصرف لاگ‌ها می‌باشد.
Description	نمایش دهنده توضیحی از دستگاه است.

استفاده از نوار ابزار

دکمه‌ها و منوهای معرفی شده در جدول زیر در نوار ابزار وجود دارند:

دکمه	توضیحات
Add Device	**ویزارد مربوط به اضافه کردن دستگاه باز می‌شود. این ویزارد سبب می‌شود بتوانیم یک فورتی آنالایزر را اضافه نماییم. دستگاه‌های ثبت نشده در منوی درختی Unregistered Devices قرار می‌گیرند.**
Edit	**دستگاه انتخاب شده ویرایش می‌شود.**
Delete	**دستگاه‌ها انتخابی یا vDOM ها از فورتی آنالایزر حذف می‌شوند. وقتی یک دستگاه حذف می‌شود لاگ فایل raw آن نیز پاک می‌گردد. اما توجه داشته باشید که لاگ‌های SQL پاک نمی‌شوند.**
Column Settings	**در این قسمت انتخاب می‌کنید که کدام ستون‌ها نمایش داده شوند یا Reset to default را انتخاب نمایید تا ستون‌های پیش فرض نمایش داده شوند.**
More	**نمایش بیشتر منوها که شامل: Import Device List و Export Device List می‌باشد.**
Search	**نمایش نام دستگاه، پنل محتوا و نمایش نتایج می‌باشد.**

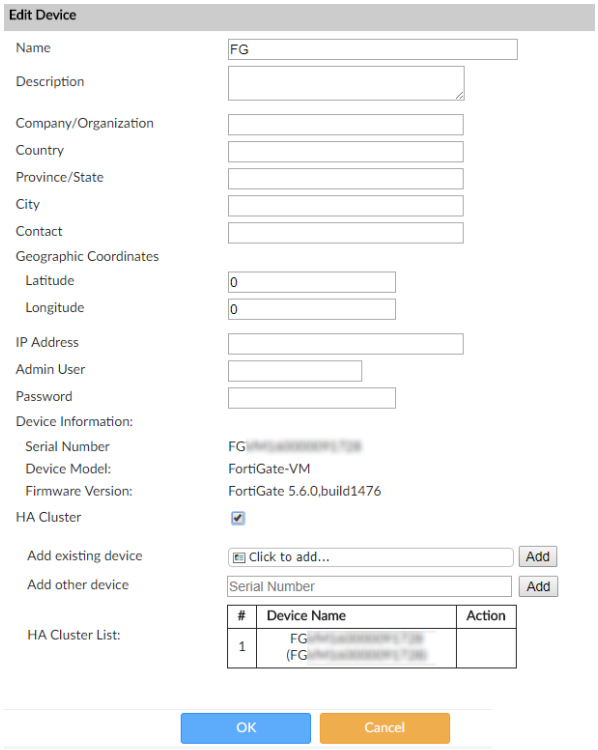
ویرایش اطلاعات دستگاه

صفحه Edit Device اطلاعات ثبت شده در مورد دستگاه را ویرایش می‌کند. اطلاعات و گزینه‌هایی که در صفحه Edit Device موجود است شامل نسخه فریمور و قابلیت‌هایی که فعال گردیده می‌باشد.

اطلاعات مربوط به یک دستگاه یا مدل دستگاه را ویرایش کنیم:

۱. به Device Manager بروید و در قسمت نوار مرور سریع بر روی Devices Total کلیک نمایید.

۲. در پنجره باز شده، دستگاه یا مدل آن را انتخاب کرده و بر روی Edit کلیک کنید. پنجره Edit Device نمایش داده می‌شود.



۳. تنظیمات دستگاه را بر اساس نیاز انجام دهید.

Name	**نام دستگاه را وارد می‌کنید.**
Description	**توضیحاتی در مورد اطلاعات دستگاه می‌باشد.**
Company/Organization	**اطلاعات کمپانی/ سازمان را وارد می‌کنید.**
Country	**کشور را وارد نمایید.**
Province/State	**منطقه را وارد نمایید.**
City	**شهر را وارد نمایید.**

Contact	اطلاعات تماس را وارد نمایید.
Geographic Coordinates	طول و عرض جغرافیایی دستگاه وارد می‌گردد.
IP Address	**IP** آدرس دستگاه را وارد می‌کنید.
Pre-Shared Key	با انتخاب **Pre-Shared Key** کلید نمایش داده می‌شود. این گزینه در شرایطی موجود است که در نظر داشته باشیم مدل دستگاه را ویرایش نماییم.
Admin User	نام کاربری ادمین را وارد می‌کنیم.
Password	کلمه عبور مربوط به کاربر ادمین را وارد می‌کنیم.
Device Information	اطلاعاتی در مورد دستگاه، موارد کلی یا جزئی شامل شماره سریال، مدل دستگاه، نسخه فریمور، اینترفیس‌های متصل، حالت **HA**، نام کلاستر و اعضای موجود در کلاستر را مشخص می‌کنیم.
HA Cluster	انتخاب این گزینه جهت شناسایی دستگاه بعنوان بخشی از یک کلاستر **HA** می‌باشد و جهت شناسایی بقیه دستگاه‌های کلاستر است.

٤. پس از ایجاد تغییرات مناسب بر روی دکمه OK کلیک کنید.

نمایش توپولوژی security fabric

برای دستگاه‌های security fabric، امکان نمایش توپولوژی وجود دارد.

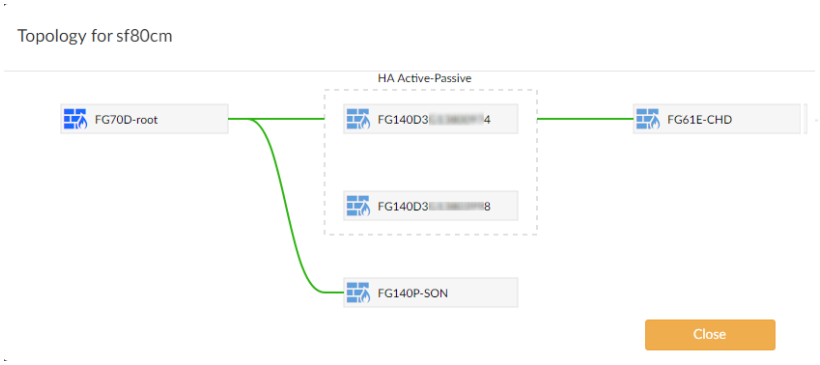
توپولوژی security fabric را نمایش دهید:

١. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

٢. به قسمت Device Manager بروید و بر روی Device Total کلیک کنید.

٣. بر روی یک security fabric راست کلیک کرده و Fabric Topology را انتخاب نمایید .

یک پنجره pop up مربوط به توپولوژی security fabric دستگاه نمایش داده می‌شود. اگر شما Fabric Topology را بوسیله راست کلیک یک دستگاه در داخل گروه Fabric انتخاب نمایید دستگاه در توپولوژی انتخاب می‌گردد. اگر Fabric Topology را با استفاده از راست کلیک بر روی اسم آن انتخاب کنید دستگاه دیگری در آن توپولوژی انتخاب نمی‌شود.



نمایش تاریخ میانگین مقادیر لاگ‌ها

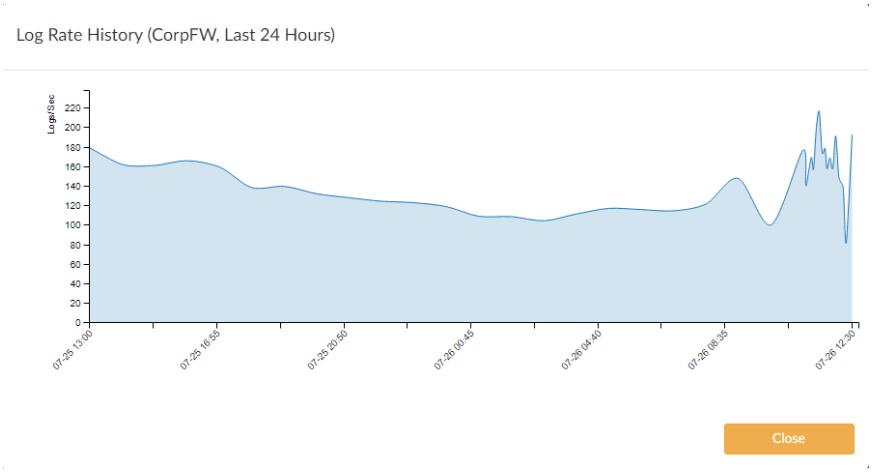
امکان نمایش تاریخچه یک گراف وجود دارد که این امر به صورت میانگین مقادیر لاگ برای هر دستگاه می‌باشد.

تاریخچه میانگین مقادیر لاگ‌ها نمایش داده شود:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به Device Manager بروید و بر روی تب Device Total کلیک کنید.

۳. در ستون Average Log Rate بر روی شماره کلیک کنید تا گراف نمایش داده شود.



٤. جهت نمایش جزئیات بیشتر مکان نما را بر روی نمودار قرار بدهید.

اتصال به یک دستگاه ثبت شده در محیط گرافیکی

امکان اتصال به یک دستگاه ثبت شده از طریق Device Manager وجود دارد.

متصل شدن به یک دستگاه ثبت شده از طریق GUI:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Device Manager رفته و بر روی تب Device Total از نوار مرور سریع کلیک کنید.

۳. بر روی دستگاه راست کلیک کرده و گزینه Connect to Device را انتخاب نمایید.

مستقیما می‌توانید به صفحه لاگین دستگاه متصل شوید.

ذخیره‌سازی فایل و لاگ

لاگ‌ها به همراه فایل‌ها بر روی هارد دیسک‌های فورتی آنالایزر ذخیره می‌شوند. باید خاطر نشان کرد که لاگ‌ها به صورت موقت بر روی دیتابیس SQL ذخیره می‌گردند.

هنگامی که ADOMها را فعال می‌کنید، تنظیمات به صورت مشخص برای هر ADOM اعمال و فقط بر روی همان دستگاه پیاده می‌شود.

تنظیمات پالیسی دیتا و مصرف دیسک برای دستگاه‌ها به صورت کلی می‌باشد که تنظیمات ذخیره‌سازی و جمع آوری نامیده می‌شود. لاگ کلی و تنظیمات ذخیره‌سازی فایل به تمام لاگ‌ها و فایل‌ها اعمال می‌گردد. هر دو حالت کلی و ذخیره‌سازی لاگ همیشه فعال می‌باشد.

تخصیص فضای دیسک

در فورتی آنالایزر، رزرو ۵ تا ۲۵ درصد فضای دیسک برای مصارف سیستمی و موارد غیرمنتظره می‌باشد. باقیمانده ۷۵ درصد تا ۹۵ درصد فضای موجود برای دستگاه‌ها در نظر گرفته می‌شود.

گزارش‌هایی که در فضای رزرو ذخیره شده‌اند.

حجم کل دیسک موجود	مجوز دیسک رزرو شده
Small Disk (up to 500GB)	**این سیستم بین ۲۰٪ یا ۵۰٪ از فضای دیسک درنظر گرفته می‌شود، هرکدام که کوچکتر می‌باشد.**
Medium Disk (up to 1TB)	**این سیستم ۱۵٪ یا 100GB فضای دیسک را در نظر می‌گیرد، هر کدام که کوچکتر می‌باشد.**
Large Disk (up to 5TB)	**این سیستم ۱۵٪ یا 200GB فضای دیسک را در نظر می‌گیرد، هر کدام که کوچکتر می‌باشد.**
Very Large Disk (bigger than 5TB)	**این سیستم ۵٪ یا 300GB فضای دیسک را در نظر می‌گیرد، هر کدام که کوچکتر می‌باشد.**

نوع RAID که انتخاب می‌کنید تعیین کننده سایز دیسک و سطح اندازه دیسک است. برای مثال، فورتی آنالایزر1000C با ٤ عدد هارد دیسک 1TB که به صورت RAID10 و با حالت large disk پیکربندی شده است ۱۰٪ یا 200GB از فضای دیسک رزرو گردیده است.

گردش کار لاگ‌ها و فایل ها

وقتی دستگاه‌ها لاگ‌ها را به فورتی آنالایزر ارسال می‌کنند لاگ به صورت خودکار گردش کار زیر را دارد:

۱. لاگ‌ها فشرده شده و در لاگ فایل روی دیسک‌های فورتی آنالایزر ذخیره می‌شوند.

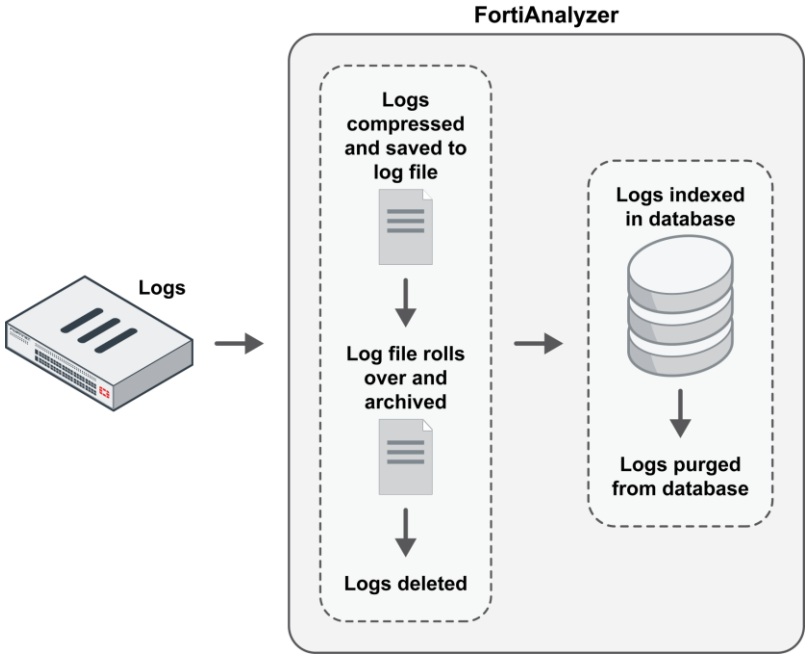
وقتی لاگ فایل به اندازه مشخصی رسید فورتی آنالایزر آن را roll کرده و به صورت آرشیو در می‌آورد و یک لاگ فایل جدید ایجاد می‌کند تا لاگ‌های جدید ورودی دریافت شوند. می‌توانیم اندازه مشخصی را برای لاگ فایل‌ها در نظر بگیریم.

۲. لاگ‌ها در دیتابیس SQL فهرست بندی می‌شوند تا بتوانید آنالیزهای لازم را بر روی آنها انجام دهید.

می‌توانید مدت زمانی که قرار است لاگ‌ها فهرست بندی شوند را مشخص نمایید.

۳. لاگ‌ها از دیتابیس SQL پاکسازی می‌شوند، اما به صورت فشرده در لاگ فایل دیسک‌های فورتی آنالایزر باقی می‌ماند.

٤. لاگ‌ها از دیسک‌های فورتی آنالایزر پاک می‌شوند. این حذف شدن بر اساس دیتا پالیسی مشخص می‌شود.



در فاز فهرست بندی، لاگ‌ها در دیتابیس SQL برای یک اندازه مشخص زمانی ایندکس می‌شوند. بنابراین جهت استفاده‌های تحلیلی و آنالیز می‌توانیم از آنها استفاده نماییم. این کار یعنی ما لاگ‌ها را آنلاین درنظر گرفته‌ایم و جزئیات مربوط به آنها می‌تواند در قسمت‌های FortiView ، NOC، Log View و Event Management مورد استفاده قرار گیرد.

امکان تولید گزارش‌ها در مورد لاگ‌ها در پنجره Reports وجود دارد.

در فاز فشرده‌سازی، لاگ‌ها فشرده‌سازی شده و در دیسک‌های فورتی آنالایزر برای یک بازه زمانی مشخص آرشیو می‌شوند. فشرده‌سازی یا بایگانی لاگ‌ها به صورت آفلاین در نظر گرفته شده و جزئیات آنها نمی‌تواند جهت ایجاد گزارش بازبینی مورد استفاده قرار گیرد.

جدول زیر به صورت خلاصه بیان کننده تفاوت‌هایی بین ایندکس کردن و فشرده‌سازی لاگ‌ها می‌باشد.

فاز لاگ	موقعیت	پشتیبانی از تحلیل فوری
ایندکس گذاری	فشرده‌سازی در لاگ فایل و ایندکس گذاری در دیتابیس SQL	بله. لاگ‌ها برای آنالیز موجود می‌باشد.
فشرده‌سازی	فشرده‌سازی لاگ فایل	خیر

حذف خودکار

بر اساس تنظیمات زیر لاگ‌ها وفایل‌ها از دستگاه فورتی آنالایزر به صورت خودکار حذف می‌شوند:

- حذف کلی فایل به صورت خودکار

تنظیمات مربوط به مدیریت فایل مشخص می‌کند چه زمانی لاگ‌های آرشیوی قدیمی، فایل‌های قرینطیه شده، گزارش‌ها و فایل‌های آرشیوی گذشته از روی دیسکها بدون در نظر گرفتن تنظیمات استورج حذف گردند.

- دیتا پالیسی

مدت زمانی که تحلیل‌ها و لاگ‌های آرشیوی برای هر دستگاه باقی می‌ماند را مشخص می‌کند. وقتی به زمان مشخص شده انقضا می‌رسیم لاگ‌های آرشیوی از روی دیسک‌های دستگاه به صورت خودکار پاک می‌شوند.

- استفاده از دیسک

تنظیمات این قسمت لاگ‌های آرشیو شده قدیمی برای هر دستگاه را پاک می‌کند. هنگامی که فضای دیسک اختصاص داده شده پر شده است. بوسیله تنظیمات لاگ استورج می‌توانید فضای دیسک اختصاص داده شده را مشخص نمایید. پیام‌های هشدار وقتی برای شما نمایش داده می‌شوند که استفاده از فضای دیسک به درصد تنظیم شده رسیده است.

تمام سیاست‌های حذف بر روی فورتی آنالایزر فعال بوده و به همین دلیل بسیار باید مراقب تنظیمات هر پالیسی باشید. برای مثال اگر پالیسی حذف کلی فایل‌ها به آستانه‌ای برسد که لاگ‌های آرشیوی قدیمی بر روی دستگاه فورتی آنالایزر به صورت خودکار پاک شود این اتفاق بدون درنظر گرفتن تنظیمات ذخیره‌سازی مرتبط با دستگاه رخ می‌دهد.

جدول زیر به صورت خلاصه پالیسی‌های پاک کردن خودکار را شرح می‌دهد:

پالیسی – سیاست	حوزه (محدوده)	راه انداختن
پاک کردن کلی فایل‌ها به صورت خودکار	تمام لاگ‌ها، فایل‌ها و گزارش‌های روی سیستم	وقتی به زمان مشخص شده انقضا می‌رسیم فایل‌های قدیمی به صورت خودکار پاک می‌شود. این پالیسی بدون در نظر گرفتن پالیسی‌های دیتا که مرتبط با دستگاه است به تمام فایل‌های سیستم اعمال می‌گردد.

سیاست داده‌ها Data Policy	لاگ‌هایی که مربوط به دستگاه بوده و با دیتا پالیسی در ارتباط است.	وقتی به زمان مشخص شده انقضا می‌رسیم، لاگ‌های آرشیوی قدیمی برای دستگاه پاک می‌شوند. این پالیسی فقط بر روی آرشیو لاگ‌هایی که برای دستگاه با دیتا پالیسی در ارتباط هستند تاثیر می‌گذارد.
مصرف دیسک Disk Utilization	لاگ‌های مربوط به دستگاه که با تنظیمات لاگ‌های ذخیره شده مرتبط است.	هنگامی که مرز مشخص شده برای تخصیص مقدار فضای دیسک برای دستگاه می‌رسد لاگ‌های آرشیوی قدیمی از روی دستگاه پاک می‌شود. این پالیسی فقط بر روی لاگ‌های آرشیوی تاثیر می‌گذارد و بر روی دستگاه‌هایی که تنظیمات ذخیره لاگ مرتبط هستند.

لاگ‌های مربوط به دستگاه‌هایی که حذف شده‌اند

وقتی یک یا چند دستگاه از روی فورتی آنالایزر حذف می‌شوند لاگ فایل‌های raw و آرشیو پکت‌ها نیز از بین می‌روند و تمام این وقایع در ایونت لاگ داخلی ثبت می‌شوند. با این حال، لاگ‌های وارد شده در دیتابیس SQL از دیتابیس پاک نشده و در نتیجه لاگ‌های مرتبط با پاک شدن دستگاه‌ها ممکن است در LogView و FortiView نمایش داده شوند و هر گزارشی بر اساس نتیجه لاگ‌های در برگرفته شده نمایش داده شود. راه حل‌های زیر به شما کمک می‌کند تا از دیتابیس SQL اطلاعات دستگاه‌های پاک شده را حذف نمایید.

- بازسازی مجدد دیتابیس SQL برای ADOM که دستگاه‌های متعلق به آن حذف شده‌اند در این صورت تمام دیتابیس‌ها مجددا باید بازسازی شوند.
- تنظیم و پیکربندی پالیسی ذخیره‌سازی لاگ وقتی که لاگ‌های دستگاه حذف شده قدیمی تر از تنظیمات Keep Logs for Analytics می‌باشند به صورت خودکار حذف می‌شوند. همچنین وقتی لاگ‌های تحلیلی از اندازه تعیین شده بالاتر می‌روند دیتابیس SQL قدیمی‌ترین جداول دیتایس را پاک می‌کند.
- تنظیمات خودکار پاک کردن فایل‌ها در قسمت System Settings> Advanced> File Management قرار دارد. وقتی لاگ‌های یک دستگاه پاک می‌شود که قدیمی تر از تنظیمات اعمال شده باشد.

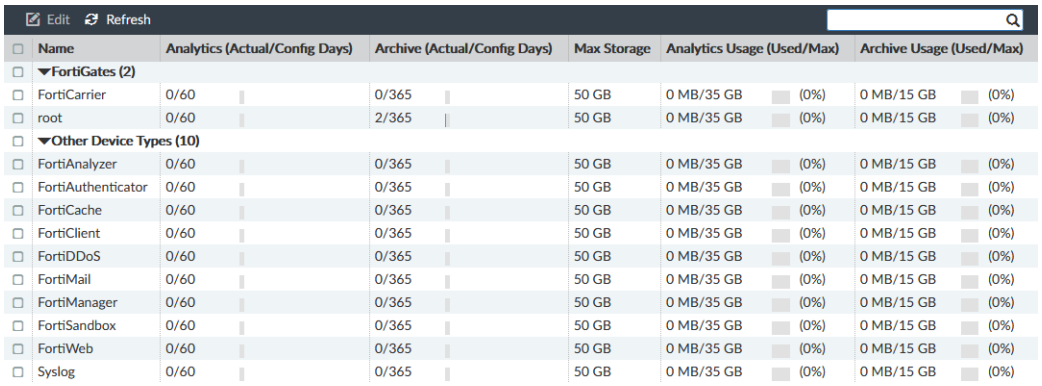
  تنظیمات کلی File Management بر روی تنظیمات ذخیره‌سازی لاگ بازنویسی می‌شود و بر روی تمام ADOMها اعمال می‌گردد.

پالیسی ذخیره‌سازی لاگ

پالیسی ذخیره‌سازی لاگ‌ها فقط بر روی لاگ‌ها و دیتابیس SQL دستگاه‌هایی که مرتبط با پالیسی ذخیره‌سازی لاگ‌ها است تاثیر می‌گذارد. گزارش‌ها تحت تاثیر قرار نمی‌گیرند.

اگر ADOMها فعال باشند، مشاهده پالیسی‌های دیتا و مصرف دیسک‌ها برای هر ADOM در

Info System Settings >Storage امکان پذیر است.



اطلاعات و گزینه‌های زیر موجود می‌باشند:

Edit	ویرایش پالیسی ذخیره‌سازی لاگ از ADOM که انتخاب شده است.
Refresh	ریفرش صفحه انجام می‌شود.
Search	عبارت مورد جستجو را وارد نمایید.
Name	نام ADOM را وارد کنید. ADOMها در دو گروه لیست شده‌اند: FortiGates و سایر مدل‌ها
Analytics (Actual/Config Days)	قدیمی‌ترین آنالیز لاگ و تعداد روزهایی که لاگ‌های تحلیلی با توجه به پالیسی دیتا نگهداری می‌شوند.
Archive (Actual/Config Days)	قدیمی‌ترین آرشیو لاگ و تعداد روزهایی که لاگ‌های تحلیلی با توجه به پالیسی دیتا نگهداری می‌شوند.

Max Storage	**حداکثر فضای تخصیصی به ADOM که برای دو حالت تجزیه و تحلیل و بایگانی استفاده می‌شود.**
Analytics Usage (Used/Max)	**چه مقدار فضا برای لاگ‌های تحلیلی استفاده می‌شود. بیشترین فضای دیسکی که برای آنها در نظر گرفته می‌شود چه مقداری است.**
Archive Usage (Used/Max)	**برای آرشیو لاگ چه مقداری فضا در نظر گرفته می‌شود. بیشترین فضای مورد استفاده چه مقداری است.**

پیکربندی لاگ استورج

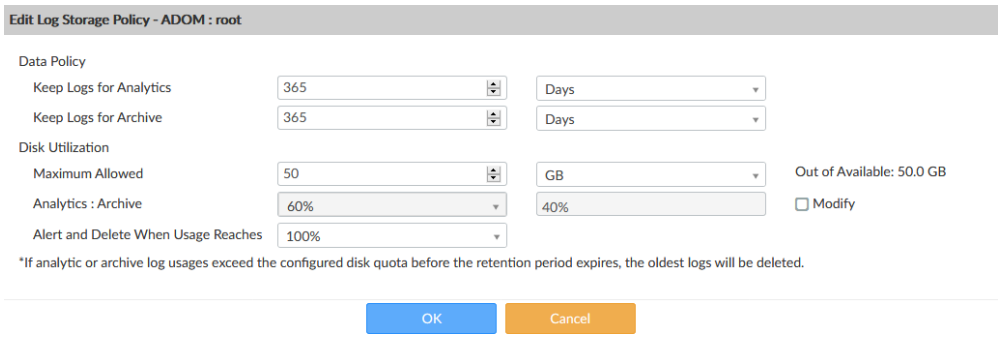
این قسمت تاثیر مستقیم بر روی لاگ‌ها و دیتابیس SQL دستگاه می‌گذارد. SQL ارتباط مستقیمی با پالیسی ذخیره‌سازی دارد.

اگر تغییری در تنظیمات ذخیره‌سازی لاگ ایجاد کنید، محدوده تاریخ جدید بر روی لاگ‌های تحلیلی و آرشیوی تاثیر می‌گذارد. با توجه به تغییر تاریخ، لاگ‌های آنالیزی ممکن است از دیتابیس پاک شود، ممکن است لاگ‌های آرشیوی اضافه شده و به دیتابیس بازگردد و لاگ‌های آرشیوی خارج از تاریخ ممکن است حذف شوند.

تنظیم لاگ ذخیره‌سازی شده:

۱. به مسیر System Settings> Storage Info بروید.

۲. بر روی یک ADOM دابل کلیک کنید، بر روی یک ADOM راست کلیک و سپس از منو گزینه Edit را انتخاب کنید. پنجره Edit Log Storage Policy باز می‌شود.

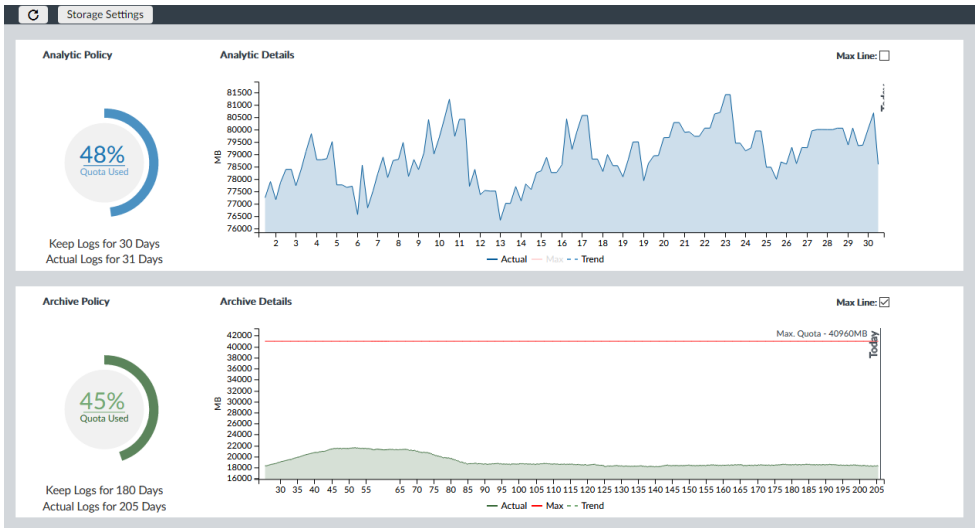


۳. تنظیمات زیر را پیکربندی کنید. سپس بر روی OK کلیک کنید.

Data Policy	
Keep Logs for Analytics	مشخص کنید چه مدت زمانی لاگ‌های تحلیلی نگهداری شوند.
Keep Logs for Archive	مشخص کنید چه مدت زمانی لاگ‌های آرشیوی نگهداری شوند.
Disk Utilization	
Maximum Allowed	مقدار فضای دیسک اختصاص داده شده را مشخص نمایید.
Analytics: Archive	نسبت فضای دیسک بین لاگ‌های تحلیلی و آرشیوی را مشخص نمایید. لاگ‌های تحلیلی نسبت به لاگ‌های آرشیوی فضای بیشتری نیاز دارند. با کلیک بر روی **Modify** می‌توانید تنظیمات را تغییر دهید.
Alert and Delete When Usage Reaches	وقتی پیغام اخطار نمایش داده می‌شود درصد استفاده از فضای دیسک اختصاص داده شده را مشخص می‌کنید و لاگ‌ها به صورت اتوماتیک حذف می‌شوند.

آمار ذخیره‌سازی

پنجره Storage Statistics را باز کنید و به مسیر Log View> Storage Statistics بروید یا از طریق نوار وضعیت مرور سریع گزینه Device Manager و بر روی Storage Used کلیک کنید.

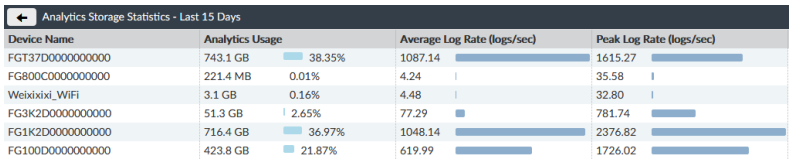


نمودار پالیسی نشان دهنده درصد سهم فضای دیسکی می‌باشد که مورد استفاده قرار گرفته است. اگر موس را بر روی دیاگرام نگه دارید مقدار استفاده، آزاد و کل فضای دیسک تخصیص داده شده را مشاهده می‌کنید. پیکربندی مدت زمانی که لاگ‌های مربوطه ذخیره می‌شوند نیز نمایش داده می‌شود.

مشاهده یا تغییر در پالیسی‌های ذخیره‌سازی لاگ، از نوار ابزار بر روی Storage Settings کلیک کنید تا پنجره Edit Log Storage Policy باز شود.

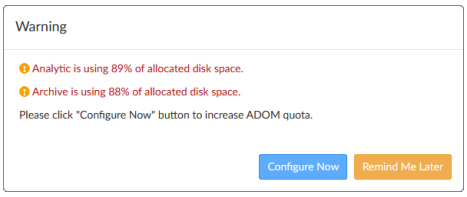
نمودار، جزئیات نمایش دهنده مقدار مصرف شده دیسک را نمایش می‌دهد که واحد آن MB است. با کلیک بر روی Max Line یک خط بر روی گراف نمایش داده می‌شود که برای کل فضای تخصیص داده شده در نظر گرفته شده است.

در نمودار نمایشی روی یک نقطه حرکت کنید تا مقدار مصرفی و فضای موجود دیسک را در یک روز و زمان مشخص مشاهده نمایید. بر روی یک نقطه از نمودار کلیک کنید تا جزئیات نمایش داده شود.


Analytics Storage Statistics - Last 15 Days

Device Name	Analytics Usage		Average Log Rate (logs/sec)	Peak Log Rate (logs/sec)
FGT37D0000000000	743.1 GB	38.35%	1087.14	1615.27
FG800C0000000000	221.4 MB	0.01%	4.24	35.58
Weixixixi_WiFi	3.1 GB	0.16%	4.48	32.80
FG3K2D0000000000	51.3 GB	2.65%	77.29	781.74
FG1K2D0000000000	716.4 GB	36.97%	1048.14	2376.82
FG100D0000000000	423.8 GB	21.87%	619.99	1726.02

هنگامی که سهمیه در نظر گرفته شده نزدیک به صد در صد رسید پیغام اخطاری نمایش داده می‌شود.



بر روی Configure Now کلیک کنید تا پنجره مربوط به Edit Log Storage Policy باز شود در اینجا می‌توانید پالیسی ذخیره‌سازی لاگ را تنظیم نمایید. این کار باعث می‌شود از تخصیص فضای بیشتر و خارج از محدوده جلوگیری شود یا با کلیک بر روی Remind Me Later مشکل را در زمان دیگری حل کنید.

فورتی ویوو – FortiView

فورتی ویوو سیستمی نظارتی و جامع برای شبکه است که به صورت بلادرنگ و با استفاده از داده‌های تاریخی در داخل یک صفحه مشخص تجمیع می‌شود.

فورتی ویوو تهدیدات شبکه‌ای را در چند سطح فیلتر کرده و امکان مانیتورینگ و لاگ گیری از تمام اتفاقات شبکه را دارد. ادمین‌ها با استفاده از این ابزار می‌توانند فعالیت‌های غیرمعمول و ... را ردیابی نمایند.

فورتی ویوو به ادمین اجازه می‌دهد تا از چندین فیلتر در کنسول استفاده نماید. امکان محدودسازی به یک زمان خاص وجود دارد. این محدودسازی می تواند بر اساس یوزر آی دی یا آی پی آدرس بوسیله برنامه‌ها و سایر موراد انجام شود.

از طریق این ابزار می‌توانید فعالیت‌های مربوط به مصرف ترافیک را مانیتور کرده و کاربرانی که مصرف زیادی دارند را شناسایی کنید.

مواردی مثل کاربرانی که دانلود و آپلود ویدئو داشته‌اند این اطلاعات به صورت متنی و یا به صورت نموداری نمایش داده می‌شود.

در فورتی ویوو می‌توانید خلاصه‌ای از دیتا لاگ‌ها، بالاترین تهدیدات بر روی شبکه، بالاترین منابع ترافیکی شبکه، بیشترین مقصدهایی که ترافیک به آنجا هدایت شده را مشاهده نمایید. همچنین این امکان فراهم گردیده که خلاصه‌ای از اطلاعات در فرمت‌هایی مانند جدول، حبابی، نقشه و ... برای شما به صورت خلاصه نمایش داده شود.

چگونه ADOMها بر فورتی ویوو اثر می‌گذارند

هنگامی که ADOMها را در فورتی ویوو فعال می‌کنید هر ADOM آنالیز تحلیلی مربوط به خود را دارد.

لاگ‌هایی که برای فورتی ویوو استفاده شده‌اند

فورتی ویوو دیتاهایی از تحلیل و آنالیز لاگ‌ها نمایش می‌دهد. در فورتی ویوو دیتا از لاگ‌های آرشیوی نمایش داده نمی‌شود.

خلاصه‌ای از لیست فورتی ویوو و توضیحات تکمیلی

گروه‌بندی	مشاهده	توضیحات
خلاصه	مرورکلی وضعیت	مرور کلی از خلاصه وضعیت فورتی ویوو می‌باشد.
تهدیدات	بالاترین تهدیدات	فهرستی از بالاترین تهدیدات شبکه. موارد زیر تهدید محسوب می‌شوند: • برنامه‌هایی که بوسیله application control ریسک تشخیص داده می‌شوند. • رخدادهایی که توسط IPS شناسایی می‌شوند.

		• وب سایت‌های مخربی که بوسیله فیلترینگ شناسایی می‌شوند. • باتنت و malwareهایی که توسط آنتی ویروس شناسایی می‌شوند.
	نقشه تهدیدات	نمایش یک نقشه از جهان که بالاترین مقصد ترافیک‌ها به سوی هر کشور با رنگی مشخص نمایان می‌شود. تهدیدات وقتی نشان داده می‌شوند که سطح آنها برابر یا بزرگتر از اخطارها باشد و IP مبدا یک IP آدرس پابلیک می‌باشد. لیست تهدیدات در پایین صفحه نمایش دهنده موقعیت، تهدید، شدت و زمان حمله می‌باشد. شیبی که با رنگ مشخص نمایش داده می‌شود نمایانگر ریسک ترافیک است. زمانی که شما رنگ قرمز را مشاهده می‌کنید یعنی خطر بسیار زیاد است.
	شاخص‌های سازش IOC	کاربرانی نمایش داده می‌شوند که از سایت‌های مشکوک استفاده می‌کنند، دربرگیرنده IP آدرس کاربر، خطر تهدید کلی، و تعداد تهدیدات می‌باشد. استفاده از ویژگی: ۱. لاگ‌های UTM که متصل به فورتی‌گیت است باید فعال باشد. ۲. فورتی آنالایزر باید فورتی‌گیت را داشته باشد تا دیتابیس مربوط به تهدیدات را بروزرسانی کند.
ترافیک	بالاترین سورس ها	نمایش دهنده بالاترین ترافیک شبکه‌ای بوسیله IP مبدا و اینترفیس، دستگاه، امتیاز تهدید، session ها، و بایت ارسال و دریافت شده می‌باشد.

	بالاترین مقصدها	نمایش دهنده بالاترین ترافیک شبکه‌ای بوسیله IP مبدا و اینترفیس، دستگاه، امتیاز تهدید، session ها، و بایت ارسال و دریافت شده می‌باشد.
	بالاترین کشورها	بالاترین ترافیک شبکه‌ای که به سمت کشوری خاص می‌رود که در اصطلاح ترافیک sessionها نمایش داده می‌شود. شامل مقصد، امتیاز تهدید، sessionها و بایت
	پالیسی بازبینی	لیستی از پالیسی‌های بازبینی، نام دستگاه‌ها، VDOM ها، تعداد hit ها، بایت‌ها و آخرین تاریخ و زمان استفاده می‌باشد.
برنامه‌های تحت وب و سایتها	بالاترین برنامه ها	بالاترین برنامه‌های استفاده شده در شبکه نمایش داده می‌شوند. که شامل نام برنامه، دسته‌بندی، سطح ریسک، تعداد کلاینت ها، sessionهایی که بلاک شده‌اند.
	بالاترین برنامه‌های ابری	بالاترین برنامه‌های ابری استفاده شده در شبکه نمایش داده می‌شود.
	بالاترین وب سایت ها	بالاترین سایت‌های مورد تایید/ بلاک شده در شبکه نمایش داده می‌شود. اطلاعاتی در مورد دامین سایت‌ها می‌باشد.
	بالاترین کاربران browsing	بالاترین کاربرانی که بازدید از وب سایت‌ها را داشته‌اند نمایش داده می‌شود. اطلاعاتی شامل مبدا، گروه، تعداد سایت‌های بازدید شده، زمان بازدید و حجم دریافت و ارسال دیتا بر اساس بایت
	SSL & Dialup IPsec	نمایش کاربرانی که از طریق SSL و یا IPsec به شبکه متصل شده‌اند.
	Site2Site IPsec	نمایش نام تانل‌های VPN که با استفاده از IPsec به شبکه متصل هستند.

	Rough Aps	نمایش SSIDهای غیرمجاز موجود در شبکه
	Authorized Aps	نام WiFi اکسس پوینت‌هایی که در شبکه مجاز هستند نمایش داده می‌شوند.
	Authorized SSIDs	SSIDهای مجاز در شبکه نمایش داده می‌شوند.
	WiFi Clients	لیستی از نام‌ها و IP آدرس‌هایی که بر روی شبکه WiFi لاگین کرده اند.
	Admin Logins	کاربرانی که بر روی دستگاه مدیریتی لاگین کردند نمایش داده می‌شود.
	System Events	رخدادهای دستگاه مدیریتی نمایش داده می‌شود.
	Resource Usage	CPU، ممووری، لاگین‌ها و سایر اطلاعات وضعیتی سیستم مدیریتی نمایش داده می‌شود.
	Failed Authentication Attempts	تمام کاربرانی که نتوانستند به دستگاه لاگین کنند نمایش داده می‌شود.
Endpoints	All Endpoints	لیست ثبت شده فورتی کلاینت‌هایی که در فورتی‌گیت وجود دارند.
	بالاترین آسیب‌پذیری ها	اطلاعاتی در مورد آسیب‌پذیری فورتی کلاینت‌هایی که در فورتی‌گیت ثبت شده‌اند نمایش داده می‌شود. در قسمت Vulnerability جدول یا فرمت حبابی را انتخاب کنید.
	بالاترین تهدیدات	بالاترین تهدیدات برای فورتی کلاینت ثبت شده که شامل تهدید، سطح آن و تعداد رخداد نمایش داده می‌شود.
	بالاترین برنامه ها	بالاترین برنامه‌های مورد استفاده که بوسیله فورتی کلاینت ثبت شده نمایش داده می‌شود. این اطلاعات شامل: نام برنامه، سطح ریسک، sessionهای رد

		شده یا بلاک شده و بایت‌های ارسال و دریافت شده می‌باشد.
	بالاترین وب سایت ها	بالاترین برنامه‌های مورد استفاده توسط فورتی کلاینت نمایش داده می‌شود.

خلاصه‌ای از فورتی ویوو برای دستگاه‌های EMS فورتی کلاینت

گروه‌بندی	نمایش	توضیحات
تهدیدات	بالاترین تهدیدات	لیستی از بیشترین کاربران درگیر با این رخداد که بالاترین تهدید در شبکه محسوب می‌شوند. موارد زیر شامل تهدیدات می‌شود: • برنامه‌هایی که توسط قسمت application control بعنوان ریسک شناسایی شده‌اند. • وب سایت‌های آلوده‌ای که توسط وب فیلترینگ شناسایی شده‌اند. • Malware و بات نت‌هایی که توسط آنتی ویروس‌ها شناسایی شده‌اند.
برنامه‌ها و وب سایت ها	بالاترین برنامه ها	بیشترین برنامه‌های استفاده شده در شبکه که شامل نام برنامه، دسته‌بندی، سطح ریسک، تعداد کلاینت ها، sessionهای بلاک شده/ اجازه داده شده و مقدار بایت ارسالی/ دریافتی نمایش داده می‌شود.
Endpoints	بالاترین وب سایت ها	بالاترین وب سایت‌هایی که باز شده یا بلاک شده نمایش داده می‌شود.
	All Endpoints	لیستی از فورتی کلاینت‌های رجیستر شده در دستگاه EMS نمایش داده می‌شود.

	بالاترین آسیب‌پذیری ها	اطلاعاتی در مورد فورتی کلاینت‌های رجیستر شده در دستگاه EMS فورتی کلاینت که آسیب پذیر هستند نمایش داده می‌شود.

استفاده از فورتی ویوو

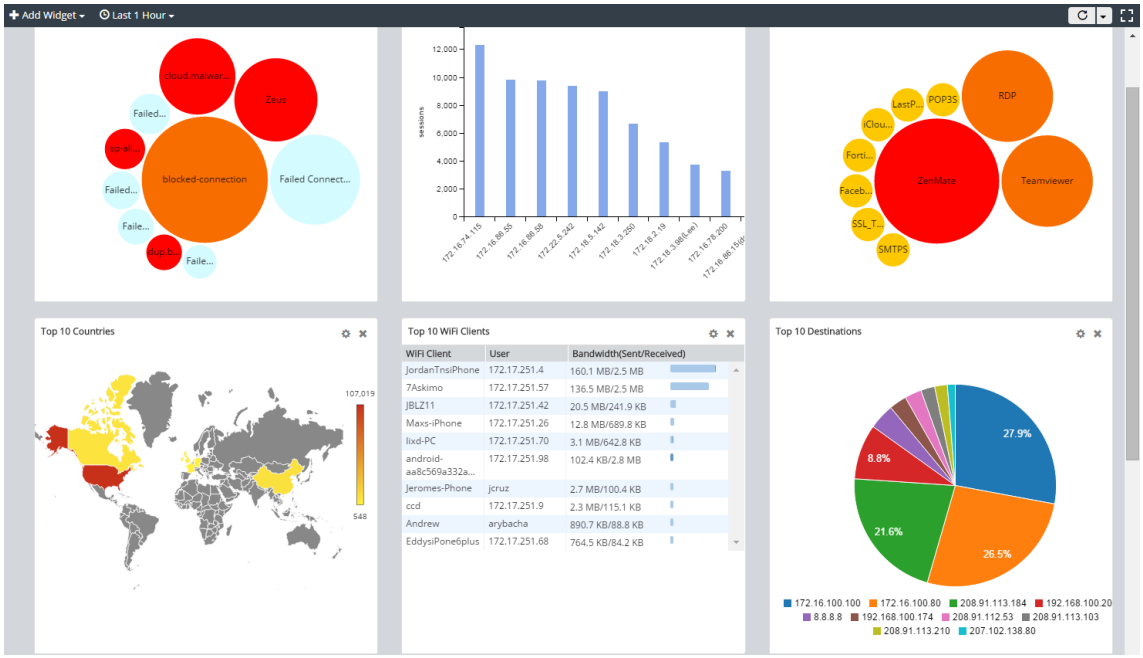
وقتی ADOMها فعال می‌شوند، فورتی ویوو اطلاعاتی در مورد هر ADOM نمایش می‌دهد بنابراین مطمئن شوید که در ADOM درست قرار دارید.

خلاصه‌ای از فورتی ویوو

این صفحه مروری کلی از وضعیت بیشترین استفاده را برای شما نمایش می‌دهد. امکان پیکربندی کلی صفحه از خلاصه نمایش داده شده وجود دارد.

هر خلاصه نمایش داده شده، یک ویجت است. امکان تنظیم هر ویجت وجود دارد فقط کافی است ویجت‌ها را چندبار اضافه کنید که در هر بار نمایش به صورت متفاوتی دیده شوند. برای مثال می‌توانید دو نوع از بالاترین تهدیدات را که نمایش دهنده ۱۰ تهدید بالاتر بوده در یک چارت حبابی و یا جدول اضافه نمایید.

برای مشاهده جزئیات خلاصه نمایش داده شده می‌توانید آنها را مرور کرده و یا از منوی درختی برای مشاهده یک صفحه تک استفاده نمایید.

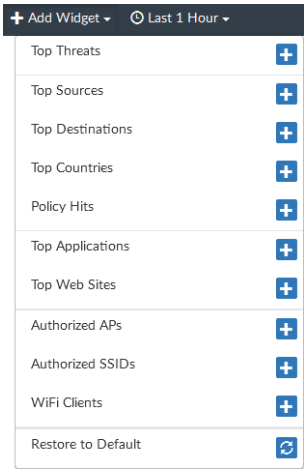


پیکربندی نمای کلی تنظیمات

اضافه کردن ویجت به صفحه خلاصه:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به فورتی آنالایزر بروید. در پنجره نوار ابزار بر روی Add Widget کلیک کنید و سپس از لیست FortiView summary را انتخاب نمایید.



حذف کردن ویجت از صفحه:

در گوشه سمت راست بالا هر ویجت دکمه Remove وجود دارد. با انتخاب آن می‌توانید ویجت را پاک کنید.

مشخص کردن دوره زمانی:

از نوار ابزار دراپ دان گزینه period را انتخاب کرده و یک زمان برای آن مشخص نمایید.

انتخاب ریفرش صفحه:

در صفحه FortiView summary، از نوار ابزار دکمه Refresh Now را کلیک کنید یا از منوی دراپ دان refresh rate را انتخاب نمایید.

سوئیچ کردن به حالت full-screen:

در قسمت FortiView Summary از نوار ابزار بر روی دکمه Full Screen کلیک کنید. برای خارج شدن از حالت تمام صفحه کافی است بر روی Esc کلیک کنید یا از بالا سمت راست بر روی دکمه Exit Full Screen کلیک کنید.

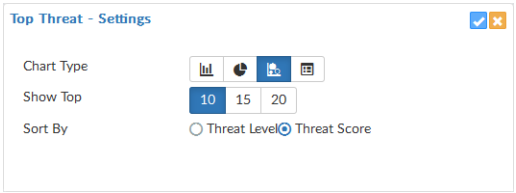
مشاهده هر ویجت در summary page

هر کدام از این صفحات امکان مشاهده در حالت اختصاصی را دارا می‌باشند که از طریق منوی درختی امکان انتخاب را دارند.

پیکربندی تنظیمات نمایش برای یک ویجت خاص

پیکربندی تنظیمات view برای یک ویجت خاص:

۱. در صفحه FortiView Summary، در بالای صفحه سمت راست دکمه Edit Settings را کلیک کنید.



۲. در پنل تنظیمات، تنظیمات ویجت را انجام دهید. تنظیماتی مانند Chart Type، Show Top و Sort By.

۳. در گوشه سمت راست بالا بر روی OK کلیک نمایید تا تغییرات ذخیره شود.

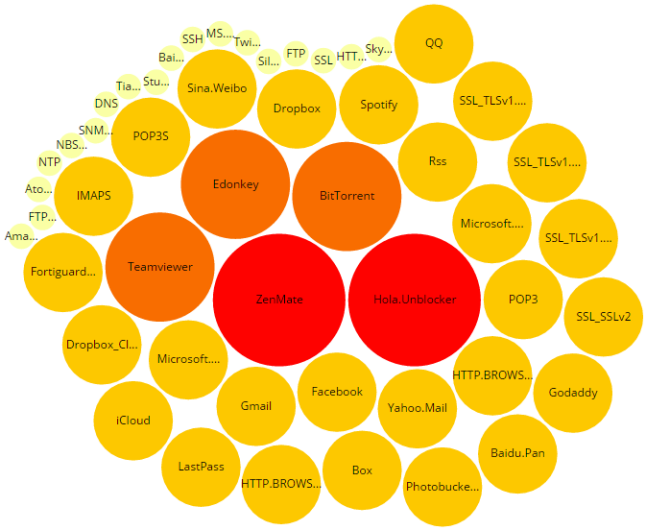
مشاهده خلاصه‌ای از FortiView

وقتی summary view را مشاهده می‌کنید، در نوار ابزار از کنترل‌هایی استفاده می‌کنید تا فرمت نمایشی را انتخاب نمایید، دستگاهی را انتخاب، مدت زمانی را مشخص کرده، زمان بازخوانی، خروجی گرفتن از اطلاعات و سوئیچ کردن به حالت تمام صفحه را مشخص می‌کنید.

با توجه به این موضوع که کدام خلاصه را مشاهده می‌کنید می‌توانید خلاصه‌ای از اطلاعات را در فرمت‌های مختلف مثل جدول، حباب، نقشه و یا حالت کاشی مشاهده کنید.

بعضی از موارد فقط از بعضی فرمت‌ها را پشتیبانی می‌کنند. برای مثال،Threat Map فقط فرمت نقش‌ها را پشتیبانی می‌کند و Policy Hits فقط از فرمت جداول پشتیبانی می‌کنند.

- Summary view از فرمت‌های مختلفی پشتیبانی می‌کند. بر روی آیکون فرمت در بالا سمت راست کلیک نمایید تا بتوانید فرمت دیگری را انتخاب نمایید.
- در قالب ساده:
  - نمایش آیتم‌ها به انتخاب شما بستگی دارد، از سمت چپ بالا لیست دراپ دان Sort By را انتخاب نمایید.
- در قالب جدول:
  - انتخاب تعداد آیتم‌های نمایشی توسط شما صورت می‌پذیرد. با استفاده از لیست دراپ دان Show این انتخاب صورت می‌گیرد.
  - مرتب کردن بر اساس یک ستون با کلیک بر روی عنوان ستون انجام می‌پذیرد.
- در قالب حبابی و نقشه:
  - اگر مرتب‌سازی امکان پذیر باشد، با استفاده از لیست Sort By انجام می‌شود.
  - برای مشاهده اطلاعات بیشتر، موس را بر روی موارد گرافیکی ببرید.



بعضی از summaryها جزئیات بیشتری را نمایش می‌دهند. با راست کلیک بر روی یک المان جزئیات بیشتری در مورد برنامه‌های متفاوت مشاهده خواهید کرد. برای وارد شدن به جزئیات و موارد بیشتر کافی است دابل کلیک کنید. با کلیک کردن بر روی دکمه Back به صفحه قبلی باز می‌گردید.

برای مثال به مسیر Endpoints> Top Vulnerabilities رفته و وضعیت دستگاه و آسیب‌پذیری‌ها را مشاهده می‌کنید. در قسمت Application & Websites>Top Cloud Applications می‌توانید Cloud Applicationها و Cloud User را مشاهده نمایید.

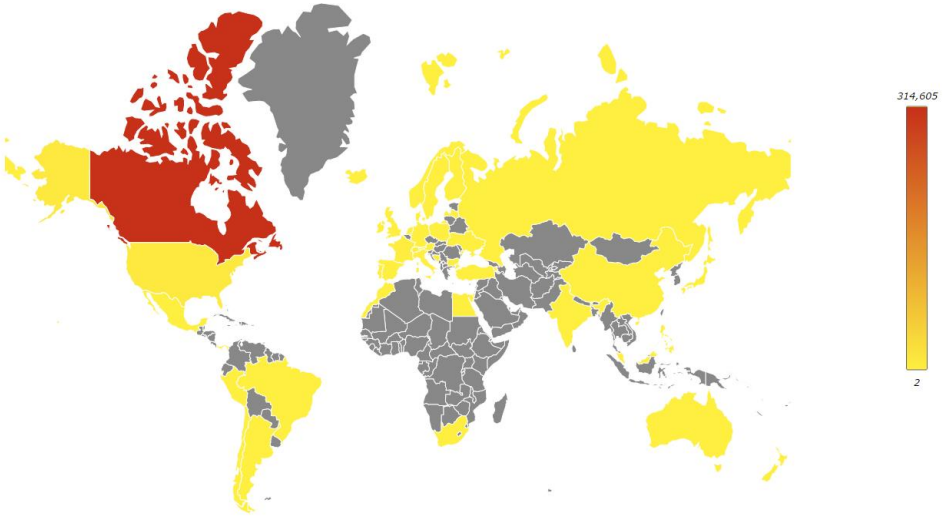
نقشه‌ای از بالاترین کشورهایی که ترافیک به سمت آنها ارسال شده است

از طریق مسیر Traffic>Top Countries می‌توانید خلاصه‌ای از وضعیت را مشاهده نمایید. نقشه نشان دهنده کشور مقصد می‌باشد.

مشاهده نقشه‌ای از کشورهایی که بالاترین ترافیک دریافتی را داشته‌اند

۱. به مسیر FortiView> Traffic>Top Countries بروید.

۲. آیکون Map را از لیست انتخاب نمایید.



۳. از لیست Sort By روشی برای مرتب‌سازی انتخاب نمایید.

٤. برای مشاهده اطلاعات بیشتر، موس را بر روی نقشه نگه دارید.

٥. برای مشاهده جزئیات بیشتر ، بر روی کشوری کلیک نمایید.

٦. با دابل کلیک کردن بر روی یک ورودی اطلاعات و جزئیات بیشتری را به نمایش درآورید.

۷. با کلیک بر روی دکمه Back از نوار ابزار به صفحه قبلی باز می‌گردید.

نمایش نقشه تهدیدات

امکان مشاهده یک تصویر متحرک از نقشه جهان وجود دارد. این نقشه تهدیدات را از طریق مدیریت تهدیدات در یکپارچه سازی لاگ‌ها نمایش می‌دهد. تهدیدات به صورت بلادرنگ نمایش داده می‌شود. هیچگونه نمایش مجدد و یا جزئیات اضافی وجود ندارد.

مشاهده نقشه تهدیدات:

۱. به مسیر FortiView> Threats> Threat Map بروید.

۲. در نقشه، موقعیت جغرافیایی تهدیدات را مشاهده می‌کنید.

۳. در پنجره Threat، تهدیدات، سطح آنها و موقعیتشان را مشاهده می‌کنید.

فیلتر کردن خلاصه‌های FortiView

فیلترکردن خلاصه‌های FortiView با استفاده از باکس Add Filter از نوار ابزار یا راست کلیک بر روی یک ورودی امکان پذیر است. فیلتر کردن با انتخاب دستگاه‌های خاص یا گروه‌های لاگ و یا زمان امکان پذیر است.

فیلتر کردن خلاصه‌های FortiView با استفاده از فیلترهای موجود در نوار ابزار:

فیلترها را در باکس Add Filter مشخص نمایید.

جستجوی منسجم: summary view را انتخاب نمایید، Add Filter را کلیک کرده و فیلتری را از لیست پایین افتادنی انتخاب نمایید سپس مقداری را تایپ کنید. با انتخاب NOT مقدار فیلتر را منفی می‌کنید. امکان اضافه کردن چندین فیلتر وجود دارد و اتصال به آنها با "and" یا "or" انجام می‌شود.

جستجوی پیشرفته: بر روی آیکون Switch to Advanced Search در انتهای سمت راست صفحه کلیک کنید. شرایط مورد نظر خود برای جستجو را وارد نمایید. با کلیک بر روی Switch to Repair search به حالت جستجوی معمولی بازمی‌گردید.

در لیست Device، دستگاه را انتخاب نمایید.

در لیست Time، دوره زمانی را انتخاب نمایید.

بر روی Go کلیک نمایید.

فیلترکردن خلاصه‌های FortiView با استفاده از راست کلیک کردن بر روی منو:

بخش summary Views را انتخاب نمایید بر روی Entry راست کلیک کنید و یک فیلترمناسب را انتخاب نمایید.

با توجه به ستونی که موس شما در آن قرار گرفته است وقتی راست کلیک می‌کنید، FortiView مقدار آن ستون را بعنوان معیار فیلتر استفاده می‌کند. این مقدار فقط برای ستون‌های خاص موجود می‌باشد.

مشاهده لاگ‌های مرتبط

امکان مشاهده لاگ‌های مرتبط برای summary در قسمت Log View وجود دارد. وقتی لاگ‌های مرتبط را مشاهده می‌کنید، فیلترهای شبیه که به FortiView Summary اعمال می‌گردد پیام‌ها را نمایش می‌دهند.

برای مشاهده لاگ‌های مرتبط در FortiView summary بر روی ورودی‌ها راست کلیک کرده و View Related Logs را انتخاب نمایید.

خروجی از خلاصه‌های فیلترشده

امکان گرفتن خروجی از خلاصه‌های فیلترشده FortiView در هر سطحی وجود دارد. خلاصه‌هایی که فیلترشده‌اند همیشه در فرمت جدول قابلیت خروجی گرفتن را دارند.

خروجی از خلاصه فیلترشده:

۱. بر روی دکمه Export کلیک کنید این دکمه در بالای سمت راست صفحه قرار گرفته است که با نام Export to PDF یا Export to Report Chart نامیده می‌شود.

۲. در کادر محاوره‌ای باز شده، تنظیمات زیر را انجام دهید:

- نام فایل خروجی را مشخص نمایید.
- در فیلد Top، تعداد ورودی‌هایی که قرار است export شوند را مشخص نمایید.
- اگر خروجی شما به صورت گزارش چارتی است می‌توانید گزارش خروجی را طوری ایجاد کنید که برای هر تب یک چارت ایجاد شود.

۳. بر روی دکمه OK کلیک کنید.

نمودارها در کتابخانه‌های نموداری ذخیره می‌شوند. امکان استفاده از آنها همانند نمودارهای دیگر وجود دارد.

مشاهده شاخص‌های سازگاری اطلاعات indicators of compromise

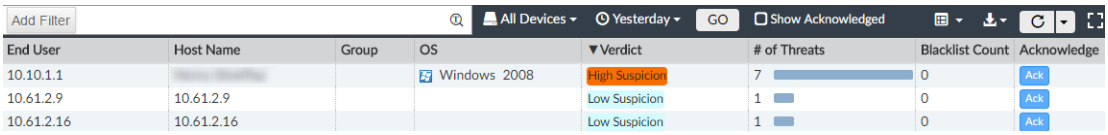
IOC کاربرانی را نمایش می‌دهد که مشکوک به استفاده از سایت‌های آلوده می‌باشند. اطلاعاتی مانند IP آدرس‌های کاربران، نام هاست، گروه، سیستم عامل، خطر تهدیدات کلی، مشاهده نقشه و تعداد تهدیدات را نمایش می‌دهد. همچنین امکان مشاهده تهدیدات وجود دارد.

برای ایجاد IOC، فورتی آنالایزر لاگ‌های وب سایت‌های فیلتر شده برای هر کاربر را که در دیتابیس وجود دارد چک می‌نماید. وقتی تهدیدی وجود داشته باشد، یک امتیاز مبنی بر تهدید به کاربر داده می‌شود. وقتی به صورت کامل همه چیز بررسی شد فورتی آنالایزر تمام نمرات تهدید را جمع آوری می‌کند و قضاوت کلی IOC را اعلام می‌نماید.

برای استفاده از IOC باید قابلیت وب فیلتر را در دستگاه فورتی‌گیت روشن کنید. همچنین به خاطر داشته باشید که برای این قابلیت باید دستگاه فورتی آنالایزر در فورتی گارد اشتراک داشته باشد تا دیتابیس تهدیدات داخلی با دیتابیس موجود در فورتی گارد همسان سازی شود.

مشاهده اطلاعات IOC کاربران:

- به مسیر FortiView>Threats>Indicators of Compromise بروید. صفحه content مروری کلی بر روی کاربران دارد و وضعیت مشکوک را برای شما نمایش می‌دهد. اطلاعات نمایشی شامل IP آدرس‌های کاربران، گروه، OS، خطر تهدیدات به صورت کلی، تعداد تهدیدات، دکمه Map View و دکمه Acknowledge می‌باشد.
- مشاهده IOC در قالب جدول، از منو بر روی Table/Tile در بالا سمت راست کلیک کنید و Table را انتخاب نمایید.



- در حالت کاشی، نقشه‌ای از IOC را مشاهده می‌کنید، بر روی Map View کلیک کنید. با نگه داشتن موس بر روی مقصد جزئیات بیشتری نمایش داده می‌شود.
- برای تایید وضعیت IOC کاربر بر روی Ack کلیک نمایید.
- برای فیلتر ورودی ها، بر روی Add Filter کلیک کرده و دستگاه‌ها را مشخص یا یک بازه زمانی انتخاب نمایید.
- برای مشاهده جزئیات تهدیدات، بر روی یک ردیف کلیک نمایید.

اشتراک گرفتن فورتی آنالایزر با فورتی گارد

فورتی آنالایزر باید در فورتی گارد اشتراک داشته باشد. این اشتراک سبب می‌شود دیتابیس تهدیدات بروزرسانی شود. برای انجام این کار کافی است لایسنس IOC فورتی گارد را تهیه نمایید.

چگونه برای فورتی آنالایزر در فورتی گارد اشتراک بگیریم

۱. به مسیر System Settings> Dashboard می‌رویم.

۲. در ویجت License Information به دنبال فیلد FortiGuard> Indicators of Compromise Service می‌گردیم و بر روی Purchase کلیک می‌کنیم.

مانیتور کردن منابع مصرفی دستگاه‌ها

امکان مانیتور کردن منابع سیستمی هر دستگاه وجود دارد. منابع سیستمی شامل سی پی یو، رم و فضای دیسک می‌شود. وقتی ADOMها فعال هستند این اطلاعات برای هر ADOM نمایش داده می‌شوند. در یک ADOM خاص می‌توانید اطلاعات منابع مصرفی تمام دستگاه‌ها را مشاهده نمایید.

به مسیر

FortiView> System> Resource Usage

بروید تا منابع مورد استفاده هر دستگاه را مشاهده نمایید.

نمونه‌هایی از استفاده FortiView

برای بدست آوردن اطلاعاتی در مورد شبکه خود می‌توانید از FortiView استفاده نمایید. بعضی از مثال‌های زیر را مطالعه بفرمایید:

پیدا کردن برنامه و اطلاعات کاربران

کمپانی ABC بالای ۱۰۰ نفر کارمند دارد که از برنامه‌های مختلفی در سراسر مناطق مختلف جغرافیایی استفاده می‌کنند. این برنامه‌ها شامل زنجیره عرضه، مالی، امکانات و ساخت و سازها، اجرا و IT می‌باشد.

تیم ادمین شرکت فاکتوری با رقم ۶۰۰۰ دلار از یک توسعه دهنده نرم افزار دریافت می‌کند که بابت لایسنس یک برنامه با نام Widget-Pro صادر شده است. توسعه دهنده نرم افزار مدعی است یکی از کارمندان کمپانی ABC در حال استفاده از برنامه Widget-Pro است.

حال مدیر سیستم به جد دنبال کسانی است که از برنامه‌هایی استفاده می‌کنند که در لیست برنامه‌های مجاز نمی‌باشند. ادمین سیستم درنظر دارد مشخص نماید که آیا کاربر برای signatureهای فورتی گارد ناشناخته است، شناسایی لیست کاربران و تجزیه و تحلیل سیستم‌ها انجام شود.

پیدا کردن برنامه و اطلاعات کاربر:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

۲. به آدرس FortiView> Application & Websites> Top Applications بروید.

۳. بر روی Add Filter کلیک کنید، Application را انتخاب کرده، Widget-pro را تایپ و سپس بر روی Go کلیک نمایید.

٤. اگر در نتایج فیلتر شده برنامه‌ای در این زمینه پیدا نکردید به مسیرTraffic> Log View بروید.

٥. بر روی Add Filter کلیک کنید، Source IP را انتخاب، source ip مورد نظر خود را تایپ کرده و سپس بر روی Go کلیک نمایید.

یافتن وایرلس اکسس پوینت‌های ناامن

AAA الکترونیک اکسس پوینت‌های مختلفی را در فروشگاه‌های خود برای عرضه به مشتریان ارائه می‌کند. هکرها با پیدا کردن کانکشن‌های وایرلس ناامن در شبکه AAA الکترونیک می‌توانند اختلال ایجاد نمایند. این اختلال می‌تواند نصب یک برنامه در شبکه و به سرقت بردن دیتاهای شخصی نفرات باشد.

ادمین‌های شبکه با استفاده از اخطارهای فورتی آنالایزر برنامه‌های مجهول را مانیتور کرده و از برنامه‌های غیرمجاز نصب شده آگاه می‌شوند.

یافتن اطلاعات در مورد اکسس پوینت‌های ناامن:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر FortiView> WiFi> Rogue Aps رفته تا لیست اکسس پوینت‌های نامطمئن و یا تقلبی را مشاهده نمایید.

تحلیل و گزارش از وضعیت ترافیک شبکه

ادمین جدید در کالج فنی شروع به کار می‌کند. مدرسه برای دانش آموزان در شرایطی که سیاست‌ها و شرایط مدرسه را بپذیرند وای فای رایگان در اختیار آنها می‌گذارد.

از ادمین جدید خواسته شده که آنالیز لازم را داشته و گزارشی بر اساس بالاترین سورس و destination بر اساس مصرف داشته باشد. مبدا و مقصدی که بالاترین میزان مصرف پهنای باند را داشته و تعداد تلاش‌هایی که در جهت دسترسی به سایت‌های مسدود شده صورت گرفته اعلام شود.

بررسی ترافیک مبدا/مقصد و پهنای باند:

۱. اگر ازADOM ها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر FortiView> Traffic> Top Sorces بروید.

۳. به مسیر FortiView> Traffic> Top Destination بروید.

آسیب‌پذیری‌هایی که شدت درجه بالایی دارند:

معمولا کمپانی‌ها تجربه‌های زیادی از آسیب‌پذیری از طریق شبکه‌های کامپیوتری دارند اما بیشتر آنها شدت کم تا متوسط داشته و اغلب بوقوع می‌پیوندند. مدیر شبکه با توجه به زمان می‌خواهد سریعا آسیب‌پذیری‌هایی که شدت بالاتری دارند را مشاهده نماید.

مشاهده آسیب‌پذیری‌ها با شدت بالا:

۱. اگر از ADOMها استفاده می‌نمایید مطمئن شوید که در ADOM درست قرار دارید

۲. به مسیر FortiView> Endpoints> Top Vulnerabilities بروید.

۳. در نوار ابزار، Vulnerability را انتخاب و فرمت Bubble را انتخاب نمایید.

توجه خود را به بالای سمت راست نمودار حبابی معطوف نمایید جایی که آسیب‌پذیری‌ها با بالاترین درجه و شدت ممکن، نمایش داده می‌شود. اگر موس را چند لحظه بر روی وضعیت آسیب‌پذیری نگه دارید اطلاعات بیشتری قابل نمایش خواهد بود با کلیک بر روی vulnerability جزئیات بیشتری را مشاهده خواهید کرد.

NOC

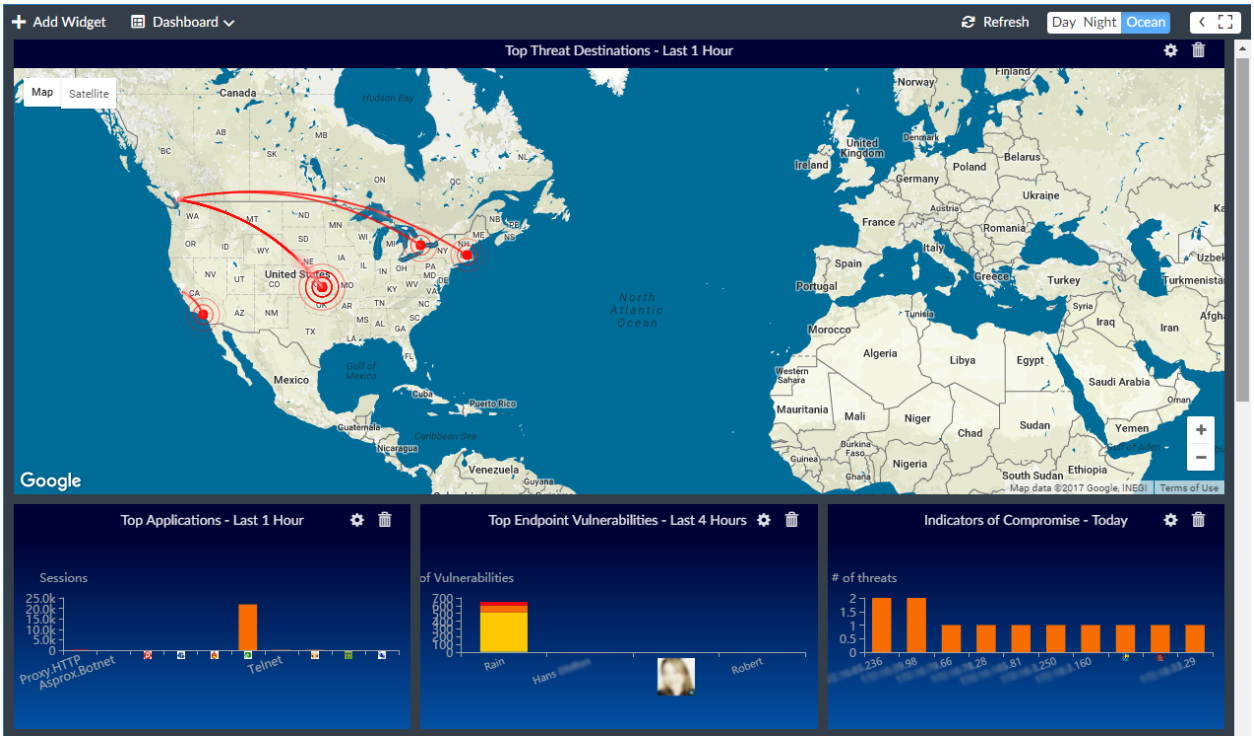
NOC مخفف کلمه Network Operations Center یا SOC مخفف کلمه Security Operations Center است که برای مشاهده چندین پنجره از فعالیت‌های شبکه که شامل مانیتورینگ امنیت شبکه، امنیت WiFi و کارایی سیستم مورد استفاده قرار می‌گیرد.

NOC هر دو حالت مانیتورینگ بلادرنگ و روندهای زمانی را نمایش می‌دهد. مانیتورینگ متمرکز سبب می‌شود به طور موثری رویدادهای شبکه را نظارت نمایید.

داشبورد NOC

NOC شامل پیش تعریف‌هایی مثل Security Monitor، WiFi Monitor و Systems Performance برای داشبوردها می‌شود.

امکان ساختن داشبوردهای دلخواه برای شما وجود داشته و می‌توانید ویجت‌ها را به آنها اضافه نمایید. هر پنجره یا ویجت یک فعالیت را مانیتور می‌کند. انتخاب نمایش ویجت‌ها، دلخواه‌سازی آنها، جابجایی و تغییر سایز ویجت‌ها و نمایش ویجت‌ها در حالت تمام صفحه یا در مانیتور دیگر به انتخاب شما صورت می‌گیرد.



یک راه خوب برای استفاده از تمام داشبوردها بکارگیری آنها در چندین مانیتور است. نمایش ویجت‌های متفاوت دید وسیعی از شبکه و عملیات امنیتی در لحظه را برای شما ایجاد می‌کند و همین امر سبب می‌شود اطلاعات بیشتری نمایش داده شود.

یک سناریو استفاده از مانیتورهای اصلی در وسط برای نمایش ویجت‌ها در بزرگترین اندازه کاربرد دارد. این ویجت‌ها نمایش دهنده اطلاعات مهم شبکه می‌باشند. سپس از مانیتورهای جانبی برای نمایش سایر اطلاعات در ویجت‌های کوچکتر استفاده نمایید.

برای مثال، از مانیتور قرار گرفته در بالا و بخش وسط برای نمایش ویجت Top Threat Destinations در حالت تمام صفحه استفاده نمایید و از مانیتورهای پایین در جهت نمایش Security Monitor استفاده کنید. از مانیتورهای سمت چپ برای نمایش ویجت‌های WiFi Monitor استفاده کرده و در بالا از مانیتورها برای نمایش ویجت‌های System Performance استفاده نمایید. توجه داشته باشید که امکان جابجایی، اضافه کردن و یا حذف تمام ویجت‌ها وجود دارد.

استفاده از داشبورد NOC

داشبوردهای NOC از ویجت‌هایی که شبکه و امنیت اطلاعات را تامین می‌نماید تشکیل شده است.

Add Widget	ویجت‌های از پیش تعریف شده یا داشبوردهای سفارشی سازی شده را اضافه می‌کند.
Dashboard	**ایجاد یا ریست یک داشبورد جدید که از قبل تعریف شده است. برای داشبوردهای شخصی سازی شده می‌توانید داشبورد را rename یا delete نمایید.**
Create New	**یک داشبورد جدید ایجاد نمایید.**
Reset	**داشبورد را ریست کنید.**
Select Security Fabric	**Security fabric انتخاب نمایید تا در داشبورد شما نمایش داده شود.**
Refresh	**ریفرش دیتا در ویجت‌ها صورت می‌پذیرد.**
Background color	**تغییر رنگ پس زمینه داشبورد تا ساخت ویجت‌ها آسان تر انجام شود و امکان نمایش آنها در اتاق‌هایی با نور متفاوت آسان تر شود.** • **Day** رنگ پس زمینه خاکستری روشن تر را نشان می‌دهد. • **Night** پس زمینه سیاه را نشان می‌دهد. • **Ocean** رنگ پس زمینه آبی را نشان می‌دهد.

Hide Side-menu and Show Side-menu	منوی درختی سمت چپ را نشان می‌دهد یا پنهان می‌کند.
Full Screen	نمایش در حالت تمام صفحه انجام می‌شود. جهت خارج شدن از این حالت بر روی **ESC** کلیک کنید.
استفاده از کنترل‌ها در ویجت	
Settings icon	تغییر تنظیمات ویجت. ویجت‌ها تنظیماتی مربوط به خود دارند. تنظیماتی مثل تعداد آیتم‌های قابل نمایش، بازه زمانی، ریفرش اینتروال و نوع چارت.
View Different Chart Types	برخی از ویجت‌ها تنظیماتی دارند که امکان انتخاب انواع چارت‌های مختلف را می‌دهند. تنظیماتی مانند **I/O** دیسک و **Top country** ویجت و ...
Hide or show a data type	برای ویجت‌هایی که انواع داده متفاوت را نمایش می‌دهند در نوار عنوان یک نوع دیتا را کلیک کرده تا آن دیتا در گراف نمایش داده شود و یا پنهان گردد.
Remove Widget icon	ویجت را از داشبورد شخصی سازی شده‌ای که از قبل تعریف گردیده است پاک مکینند.
Move widget	کلیک و درگ کردن یک ویجت در نوار ابزار جهت جابجا کردن آن به مکانی دیگر
Resize widget	در بالای سمت راست ویجت می‌توانید با کلیک و درگ کردن دکمه **resize** اندازه ویجت را تغییر بدهید.
View more details	برای نمایش دادن جزئیات دیتای ویجت‌ها کافی است نشانگر موس را در بالای ویجت نگه دارید.

برخی از ویجت‌ها دکمه‌هایی در پایین گراف دارند. با کلیک و درگ کردن دکمه‌ها دوره زمانی کوتاه تری قابل مشاهده است.	View a narrower time period
برای ویجت‌هایی که اطلاعات را بر روی نقشه نمایش می‌دهند از این ویژگی می‌توانید استفاده کنید. با استفاده از اسکرول موس می‌توانید سطح زوم را تغییر دهید.	Zoom in and out

شخصی سازی داشبورد NOC

هر ویجتی را بر روی داشبورد از قبل تعریف شده می‌توانیم اضافه کنیم. همچنین امکان جابجایی،تغییر سایز و پاک کردن ویجت‌ها وجود دارد. توجه داشته باشید که امکان تغییر نام یا پاک کردن یک داشبورد از قبل تعریف شده وجود ندارد. ریست کردن داشبورد هم به صورتی است که تنظیمات را به حالت پیش فرض تغییر می‌دهد.

Dashboard> Reset

می‌توانیم ویجت‌های مشابه را در زمان‌های متفاوت اضافه کرده و تنظیمات لازم را بر روی آنها انجام دهیم.

پیاده‌سازی یک داشبورد:

۱. در نوار ابزار بر روی Dashboard کلیک کنید و سپس Create New را بزنید.

۲. Name را انتخاب کنید. می‌توانید یک داشبورد خالی یا از یک Template استفاده نمایید. اگر From Template را انتخاب کنید، مشخص می‌کنید که کدام داشبورد از قبل تعریف شده بعنوان یک Template استفاده شود.

۳. بر روی OK کلیک کنید. داشبورد جدیدی در منوی درختی نمایش داده می‌شود.

نمایش Security Fabric در NOC :

۱. در فورتی‌گیت یک security fabric ایجاد نمایید.

۲. Security fabric را در فورتی آنالایزر اضافه کنید.

۳. به مسیر NOC> Dashboard> Select Security Fabric بروید. صفحه Add Device باز می‌شود.

٤. Security fabric که می‌خواهید در داشبورد NOC نمایش داده شود را انتخاب نمایید.

ویجت دلخواه را به داشبورد اضافه نمایید.

اضافه کردن یک ویجت:

١. داشبوردی که از قبل تعریف شده و یا شخصی سازی شده است را انتخاب کرده و ویجتی را به آن اضافه نمایید.

٢. بر روی Add Widget کلیک کرده تا منو باز شود سپس ویجتی را که می‌خواهید اضافه نمایید را مشخص کنید.

٣. بر روی دکمه + کلیک کنید تا ویجت‌ها اضافه شوند.

٤. وقتی اضافه کردن ویجت‌ها تمام شد، بر روی دکمه close کلیک کنید تا صفحه Add Widget بسته شود.

داشبوردهای NOC و Widget ها

NOC از داشبوردها و ویجت‌های از پیش تعریف شده زیر تشکیل شده است. امکان ایجاد داشبوردهای دلخواه و اضافه کردن هر نوع ویجتی وجود دارد.

مانیتور کردن وضعیت امنیتی

داشبورد مانتیور کردن وضعیت امنیتی شامل ویجت‌های زیر می‌باشد:

Top Threat Destination	**نقشه‌ای جهانی که بالاترین ترافیک شبکه را نمایش می‌دهد. با قرار دادن مکان نما بر روی نقاط داده دستگاه‌های مبدا و IP آدرس‌ها نمایش داده می‌شود. IP آدرس ها، مقصد، کشور، سطح تهدیدات و تعداد رخدادها نمایش داده می‌شود.**
Top Threat	**بالاترین تهدیداتی که بر روی شبکه قرار دارد نمایش داده می‌شود. مکان نما را بر روی نقاط داده قرار دهید تا تهدیدات را مشاهده نمایید. دسته‌بندی، سطح تهدیدات، امتیاز و تعدد رخدادها مشخص می‌گردد.** **رخدادهای زیر جزو تهدیدات می‌باشند:**

	• ریسک برنامه‌هایی توسط **Application Control** شناسایی می‌شوند. • رخدادهای نفوذی که توسط **IPS** شناسایی شده‌اند. • وب سایت‌های مخرب شناسایی شده‌اند. • **Malware** یا **botnet**هایی که توسط آنتی ویروس شناسایی شده‌اند.
Top Application	برنامه‌هایی که بالاترین میزان استفاده در شبکه را داشته‌اند با قراردادن مکان نما بر روی نقاط نام برنامه، سطح ریسک، دسته‌بندی، **session** ها، بایت‌های ارسالی و دریافتی نمایش داده می‌شود.
Indicators of Compromise	با قرار دادن نشانگر بر روی نقاط دیتا می‌توانید **IP** آدرس کاربر، نام هاست، گروه، نسخه **OS**، سطح تهدید و تعداد تهدیدات را مشاهده نمایید.
Top Endpoint Vulnerabilities	اطلاعاتی در مورد آسیب‌پذیری‌های کامپیوترهای کاربران که توسط فورتی کلاینت جمع آوری شده است مشخص می‌گردد. با قرار دادن موس بر روی نقاط دیتا آسیب‌پذیری‌ها قابل مشاهده است. مواردی مثل **IP** آدرس مبدا، گروه‌بندی
Top Sources	**IP** آدرس مبدایی که بالاترین ترافیک شبکه‌ای را دارد. **Session**های بلاک شده و یا رد شده، امتیازات تهدیدات و بایت‌های ارسال و دریافت شده مشخص می‌گردد.
Top Countries	بالاترین ترافیک شبکه‌ای بر اساس کشور، **session**های بلاک شده یا رد شده و بایت‌های ارسال و دریافت شده. این ویجت قابلیت نمایش به صورت نمودار درختی، چارت جبابی یا چارت میله‌ای را دارا می‌باشد. با پهنای باند یا تعداد **session** مرتب می‌شود.
Security Fabric Score Summary	جمع امتیازات و اقدامات پیشنهادی برای بهبود وضعیت می‌باشد.

Historical Security Fabric Scores	تغییرات بررسی امتیاز در طول زمان است.
Security Fabric Topology	نقشه‌ای توپولوژی که ساختار منطقی دستگاه‌های امنیتی را نمایش می‌دهد.
Top Dialup VPN	نقشه‌ای از جهان که دسترسی کاربران به شبکه را که از **SSL** یا **IPsec** بر اساس **VPN** تانل استفاده می‌کنند نمایش می‌دهد. با نگه داشتن اشاره‌گر موس بر روی نقاط داده نام کاربری یا **IP** آدرس، متصل شده از **IP** یا کشور، زمان اتصال و مدت اتصال و مقدار بایت ارسال و دریافت شده نمایش داده می‌شود.
VPN Site-to-Site	نقشه‌ای از جهان که نام **VPN** تانل‌ها با **IPsec** که به شبکه دسترسی دارد نمایش داده می‌شود. با نگه داشتن نشانگر موس بر روی نقاط داده **Site 2 Site** تانل، اتصال از **IP** آدرس، مدت زمان نمایش داده می‌شود.
FortiSandbox – Scanning Statistics	تعداد فایل‌های اسکن شده توسط فورتی سندباکس مشخص می‌گردد. این جدول فایل‌ها را بر اساس نوع مشخص می‌کند. با نگه داشتن نشانگر موس بر روی نقاط داده تعداد فایل‌ها از هر نوع نمایان می‌گردد.
FortiSandbox – Top Malicious & Suspicious File Users	کاربران و یا **IP** آدرس‌هایی که بالاترین تعداد فایل‌های مخرب و مشکوک را دارند بوسیله فورتی سندباکس شناسایی می‌شود. اگر نام کاربری و یا آواتار وجود داشته باشد در این جدول نمایش داده می‌شود در غیر اینصورت **IP** آدرس نمایش داده می‌شود. با نگه داشتن نشانگر موس بر روی نقاط داده تعداد فایل‌ها مشخص می‌گردد.

مانیتور کردن WiFi

این داشبورد شامل ویجت‌های زیر است:

Authorized Aps	نقشه‌ای که نام اکسس پوینت وای فای‌های موجود در شبکه را نمایش می‌دهد.
Top SSID	بالاترین **SSID**های مجاز که دسترسی **WiFi** بر روی شبکه برای آنها وجود دارد. با نگه داشتن نشانگر موس بر روی نقاط داده، **SSID** و بایت ارسال و دریافت شده نمایش داده می‌شود.
Top Rogue APs	بیشترین **SSID** از اکسس پوینت وای فای موجود در شبکه جهت دسترسی غیرمجاز به آن مشخص می‌گردد. با نگه داشتن نشانگر موس بر روی نقاط داده، **SSID** و کل زمان حضور آن نمایش داده می‌شود.

عملکرد سیستم

داشبورد عملکردی سیستم شامل ویجت‌های زیر است:

CPU & Memory Usage	وضعیت استفاده از CPU و Memory
Multi-Core CPU Usage	وضعیت استفاده از کورهای **CPU**
Insert Rate vs Receive Rate	تعداد لاگ‌های دریافت شده در مقایسه با تعداد لاگ‌های فعال که به دیتابیس وارد شده‌اند که دربرگیرنده نرخ ماکسیمم و مینیمم است. • نرخ دریافت: چه تعداد لاگ دریافت می‌شود.

• **نرخ ورود: چه تعداد لاگ از فعالیت‌ها وارد دیتابیس می‌شود.** **اگر نرخ ورود نسبت به نرخ دریافت لاگ بالاتر باشد، بنابراین دیتابیس بازسازی rebuilding می‌شود. Lag یعنی منتظر تعداد لاگ‌های ورودی باشیم.**	
تعداد لاگ‌های دریافتی در مقایسه با تعداد لاگ‌های ارسال شده به بیرون، شامل نرخ بیشینه و کمینه می‌باشد. • **نرخ دریافت: چه مقدار لاگ دریافت می‌شود.** • **نرخ فوروارد: چه مقدار لاگ به بیرون فوروارد می‌شود.**	Receive Rate vs Forwarding Rate
نرخ تراکنش دیسک (I/O per second)، Throughput (KB/s)، Utilization (%) . نرخ تراکنش و گراف Throughput نمایش دهنده ماکزیمم و مینیمم فعالیت‌های دیسک است.	Disk I/O

Log View

اطلاعات لاگ‌ها بوسیله دستگاه یا گروه لاگ مشاهده می‌گردد. وقتی عمل rebuild دیتابیس انجام می‌شود، این قسمت در دسترس نخواهد بود تا زمانی که بازسازی دیتابیس کامل انجام شود. بر روی لینک Show Progress کلیک کرده تا وضعیت rebuild شدن دیتابیس SQL را مشاهده بفرمایید.

وقتی ADOMها فعال می‌شوند، هر ADOM اطلاعات خود را دارد که در Log View نمایش داده می‌شود.

Log View لاگ‌ها را از بخش‌های آنالیز و آرشیو لاگ‌ها نمایش می‌دهد:

- لاگ‌های قدیمی و لاگ‌های لحظه‌ای موجود در Log View از لاگ‌های تحلیلی ایجاد می‌گردند.
- Log Browse لاگ‌ها را از هر دو حالت لاگ فایل‌های فعال و هر لاگ فایلی که فشرده شده باشد نمایش می‌دهد.

مدل‌های جمع آوری لاگ‌ها از هر دستگاه:

فورتی آنالایزر این امکان را دارد که از دستگاه‌های مختلف خانواده فورتی‌نت لاگ‌ها را جمع آوری نماید. در جدول زیر توضیحاتی در مورد جمع آوری انواع لاگ از هر دستگاه توسط فورتی آنالایزر داده می‌شود:

مدل دستگاه	مدل لاگ
FortiAnalyzer	**Event**
FortiAuthenticator	**Event**
FortiGate	**Traffic** **Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, DNS, Data Leak** **Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient** **Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi**
FortiCarrier	**Traffic, Event, GTP**
FortiCache	**Traffic, Event, Antivirus, Web Filter**
FortiClient	**Traffic, Event, Vulnerability Scan**
FortiDDoS	**Event, Intrusion Prevention**
FortiMail	**History, Event, Antivirus, Email Filter**
FortiManager	**Event**
FortiSandbox	**Malware, Network Alerts**
FortiWeb	**Event, Intrusion Prevention, Traffic**
Syslog	**Generic**

لاگ‌های مربوط به ترافیک

لاگ‌های ترافیک مسئول ثبت ترافیک‌های ورودی دستگاه فورتی‌گیت می‌باشند. وقتی ترافیکی وارد پالیسی‌های فایروال فورتی‌گیت می‌شود این مدل از لاگ با نام پالیسی لاگ فایروال شناخته می‌شود. پالیسی‌های فایروال تمام ترافیکی که سعی

در عبور از دستگاه فورتی‌گیت را دارند کنترل می‌کند. این روند کنترلی بین اینرفیس‌های فورتی‌گیت، زون‌ها و VLANها وجود دارد.

لاگ‌های امنیتی

لاگ‌های امنیتی تمام وضعیت آنتی ویروس، وب فیلترینگ، اپلیکیشن کنترل، ایمیل فیلترینگ، DLP، پویش آسیب‌پذیری‌ها و فعالیت‌های مربوط به VoIP را ثبت می‌کنند.

لاگ‌های DNS

لاگ‌های DNS فعالیت DNS بر روی دستگاه را ثبت می‌کنند.

لاگ‌های Event

لاگ‌های مربوط به ادمین‌ها و فعالیت‌های دستگاه مثل تغییرات در تنظیمات، لاگین ادمین یا رخدادهای مربوط به HA ثبت می‌شود. Event لاگ‌ها بسیار مهم هستند زیرا فعالیت‌های مربوط به دستگاه فورتی‌گیت را ثبت کرده که این فعالیت‌ها حاوی اطلاعات ارزشمندی در مورد چگونگی کارکرد دستگاه فورتی‌گیت می‌باشد.

پیام‌های لاگ

بوسیله دستگاه یا بوسیله گروه‌های لاگ می‌توانید اطلاعات مفید را مشاهده نمایید.

مشاهده لاگ‌ها با یک مدل لاگ مشخص

پیدا کردن لاگ‌های فورتی میل و فورتی وب در ADOMهای پیش فرض امکان پذیر می‌باشد.

مشاهده لیست پیام‌های لاگ:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

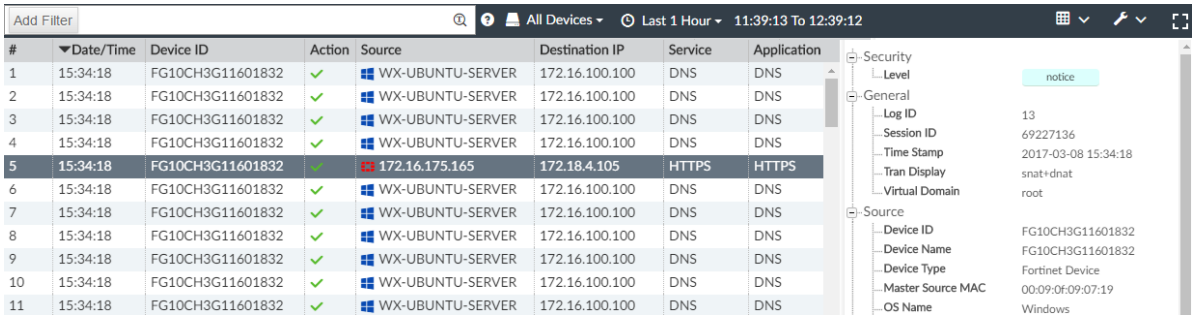
۲. به قسمت Log View بروید و نوع لاگ را از منوی درختی موجود انتخاب نمایید. لیست پیام‌های لاگ ورودی نمایش داده می‌شود.

مشاهده جزئیات پیغام‌های لاگ

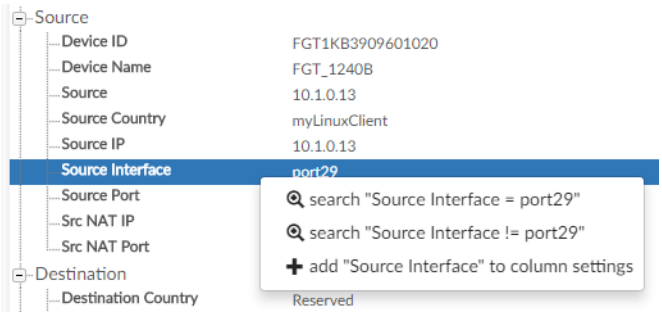
مشاهده جزئیات پیغام‌های لاگ:

۱. بر روی Log message دابل کلیک کنید یا log message را انتخاب و سپس بر روی Display Details کلیک نمایید.

پنجره جزئیات لاگ نمایش داده می‌شود در قسمت راست لیست پیغام لاگ، دسته‌بندی کامل در منوی درختی مشخص است.



پنجره جزئیات لاگ میانبری دارد که می‌توانید فیلترها را اضافه کرده و یک ستون را از حالت نمایش خارج کنید. بر روی فیلد لاگ راست کلیک کرده و یک آپشن را انتخاب نمایید.



سفارشی سازی ستون‌های نمایشی

ستون‌هایی که در لیست لاگ‌ها نمایش داده می‌شوند امکان مرتب‌سازی مجدد بر اساس نیاز کاربر را دارند.

سفارشی سازی ستون‌هایی که نمایش داده می‌شوند:

۱. در نوار ابزار log message، بر روی Column Settings کلیک و یک ستون را انتخاب نمایید تا نمایش داده شود و یا از لیست پنهان گردد.

ستون‌های نمایشی بسته به نوع دستگاه و نوع ورود متفاوت می‌باشند.

۲. برای اضافه کردن مابقی ستون‌ها بر روی More column در کادر محاوره‌ای Column Settings کلیک کرده و ستون‌ها را انتخاب نمایید تا نمایش داده شوند.

۳. جهت ریست کردن ستون‌ها و بازگشت آنها به حالت پیش فرض بر روی Reset to Default کلیک نمایید.

٤. بر روی OK کلیک کنید.

یک ستون لاگ در پنجره جزئیات Log وجود دارد بوسیله راست کلیک بر روی فیلد لاگ و انتخاب گزینه‌های Add یا Remove می‌توانید ستون‌ها را اضافه کرده یا حذف نمایید.

پیغام‌های لاگ را فیلتر کنیم

این قابلیت در اختیار شما است تا با استفاده از نوار ابزار یا بوسیله راست کلیک بر روی منو log messageها را فیلتر کنید.

به صورت پیش فرض فیلترها به حروف کوچک و بزرگ حساس نمی‌باشند. برای استفاده از فیلترهای case-sensitive کافی است به مسیر Tools> Case Sensitive بروید.

فیلترکردن log messageها با استفاده از فیلترهای موجود در نوار ابزار:

۱. به مسیری بروید که قصد دیدن لاگ‌ها را دارید.

۲. بر روی Add Filter کلیک کنید.

Regular search	بر روی **Add Filter** کلیک کرده و از لیست موجود فیلتری را انتخاب کنید. سپس یک مقدار انتخاب نمایید. فقط ستون‌های نمایش داده شده در لیست کشویی موجود می‌باشند.
Switching between regular search and advanced search	در انتهای سمت راست قسمت **Add Filter** بر روی آیکون **Switch to Advanced Search** کلیک کنید.
Advanced Search	در حالت **Advanced Search** معیارهای جستجو را انتخاب کنید.
Search operators and syntax	در انتهای سمت راست بر روی **Add Filter** کلیک کنید تا عملگرهای جستجو را مشاهده و صفحه **syntax**ها نمایش داده شود.
CLI string “freestyle” search	**config system sql** **config ts-index-field** **edit "FGT-traffic"** **set value** **"app,dstip,proto,service,srcip,user,utmaction"** **next** **end** **end**

۳. در قسمت Device list، یک دستگاه را انتخاب نمایید.

٤. در لیست زمان Time یک بازه زمانی مشخص نمایید.

برای فیلترکردن لاگ‌ها بر روی منو راست کلیک نمایید

در لیست پیغام لاگ، بر روی یک ورودی راست کلیک کرده و یک میعار فیلتر انتخاب نمایید. عبارت جستجو با آیکون ذره بین مشخص است. ورودی‌ها بر اساس مقادیر فیلترشده شما بازگردانده می‌شوند.

با توجه به ستون‌ها که مکان نمای شما در کدام یک از آنها قرار گرفته اند راست کلیک کرده از Log View استفاده نمایید تا مقادیر ستون بعنوان معیار فیلتر انتخاب شوند. این مقادیر حساس به متن بوده و فقط برای ستون‌های خاص در دسترس می‌باشند.

جستجو با عملگرها و syntax ها:

ترکیب	عملگر یا نماد
پیدا کردن ورودی‌های لاگ شامل تمام ترم‌های جستجو می‌باشد. برای مثال: **1. user=henry group=sales** **2. user=henry and group=sales**	And
1 .user=henry or srcip=10.1.0.15 **2. user=henry,linda**	Or
پیدا کردن ورودی لاگ‌هایی که NOT جمله قابل جستجو ما است. **-user=henry**	Not
پیدا کردن ورودی لاگی که بزرگتر یا کوچکتر از مقداری است که در یک رنج قرار دارد. این عملگر فقط برای مقادیری که دارای عدد صحیح می‌باشند کاربردی است. مانند **policyid>1 and policyid<10**	>, <
لاگ ورودی در یک مشخصه IP subnet یا یک رنج قرار می‌گیرد. **1 .srcip=192.168.1.0/24** **2 .srcip=10.1.0.1-10.1.0.254**	IP subnet/range search

Wildcard search	می‌توانید از **Wildcard** برای جستجو استفاده نمایید. **1 .srcip=192.168.1❊.** **2 .policyid=1❊** **3 .user❊=**

فیلترکردن پیام‌های لاگ فورتی کلاینت در ترافیک فورتی‌گیت:

برای فورتی‌کلاینت‌هایی که در دستگاه فورتی‌گیت ثبت شده‌اند امکان فلیترکردن لاگ در ترافیک ورودی فورتی‌گیت وجود دارد.

فیلترکردن log messageهای فورتی کلاینت

۱. به مسیر LogView> Traffic بروید.

۲. در قسمت Add Filter، عبارت .fct_devid=*. را تایپ کنید. لیستی از لاگ ترافیک‌های فورتی‌گیت که بوسیله فورتی کلاینت ایجاد شده نمایش داده می‌شود.

۳. در لیست Log message ، فورتی‌گیت را انتخاب نمایید تا در پنجره باز شده جزئیات را مشاهده کنید.

٤. تب فورتی کلاینت را انتخاب نمایید. بر روی ترافیک لاگ‌های فورتی کلاینت دابل کلیک کنید تا جزئیات را مشاهده نمایید.

تب فورتی کلاینت فقط در صورت در دسترس است که ترافیک لاگ‌های فورتی کلاینت برای فورتی‌گیت ارسال می‌شود.

مشاهده تاریخچه و لاگ‌های بلادرنگ

به صورت پیش فرض، LogView لاگ‌های مبتنی بر تاریخ را نمایش می‌دهد. حالت مشاهده دلخواه و چارت ساز فقط در log view موجود می‌باشند. برای مشاهده لاگ‌های لحظه‌ای یا بلادرنگ، در نوار ابزار به مسیر Tools> Real-time Log بروید.

برای بازگشت به قسمت مشاهده لاگ‌های قدیمی کافیست به مسیر Tools> Historical Log بروید.

مشاهده فرمت لاگ‌ها

به صورت پیش فرض، Log View فرمت لاگ‌ها را نمایش می‌دهد. Log View انتخابی شما بر روی گزینه‌های مشاهده شده موجود تاثیر می‌گذارد. امکان شخصی سازی ستون‌ها وقتی در حالت raw هستند وجود ندارد. برای مشاهده raw لاگ‌ها در لیست Log Message به مسیر Tools> Display Raw بروید. برای بازگشت به حالت قبلی کافیست Tools> Formatted Log را انتخاب نمایید.

سفارشی سازی

از Custom View در جهت ذخیره‌سازی تنظیمات فیلترینگ و دوره زمانی انتخاب شده استفاده می‌گردد.

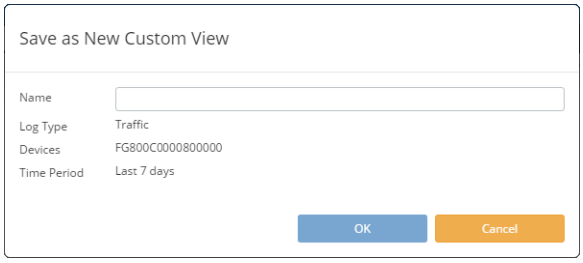
ساخت یک نمایش سفارشی سازی شده Custom View

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به قسمت Log View رفته و نوع لاگ را انتخاب نمایید.

۳. در پنجره content، بوسیله اضافه کردن فلیتر مورد نظر، مشخص کردن دستگاه‌ها و دوره زمانی مورد نیاز می‌توانید log view خود را شخصی سازی نمایید.

٤. در نوار ابزار بر روی Custom View کلیک نمایید.



۵. در فیلد Name، یک نام برای custom view خود انتخاب نمایید.

٦. بر روی OK کلیک نمایید. نمایش سفارشی سازی شده در قسمت Log View> Custom View نمایش داده می‌شود.

ویرایش صفحه سفارشی سازی شده:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Log View> Custom View بروید.

۳. در نوار ابزار، تنظیمات فلیتر را ویرایش کرده و سپس GO را بزنید.

٤. در نوار ابزار، بر روی Custom View کلیک نمایید.

٥. با کلیک بر روی Save تغییرات را ذخیره می‌کنیم.

٦. بر روی دکمه OK کلیک کنید.

مشاهده لاگ‌های یک صفحه سفارشی سازی شده:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید در ADOM درست قرار دارید.

۲. به مسیر Log View> Custom View بروید.

۳. بر روی نام صفحه سفارشی سازی شده کلیک راست کرده و گزینه View Traffic را انتخاب نمایید.

دانلود log messages

امکان دانلود لاگmessage ها به صورت یک فایل text و یا csv در کامپیوتر وجود دارد. شما لاگ‌ها را به صورت لحظه‌ای نمی‌توانید دانلود کنید.

لاگ messageها را دانلود کنید:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Log View بروید و نوع لاگ را انتخاب نمایید.

۳. در نوار ابزار بر روی Tools> Download کلیک نمایید.

٤. در پنجره باز شده Download Logs، تنظیمات مربوط به گزینه‌های دانلود را انجام دهید:

- از لیست فرمت فایل لاگ را انتخاب نمایید.

- برای فشرده‌سازی فایل دانلود شده، گزینه Compress با gzip را انتخاب کنید.
- اگر در نظر دارید فقط لاگ messageهای صفحه جاری را دانلود کنید، Current Page را انتخاب کنید. برای دانلود تمام صفحات در لیست لاگ مسیج‌ها گزینه All Pages را انتخاب کنید.

۵. بر روی Download کلیک کنید.

ایجاد کردن چارت ها

Log View دارای بخشی با نام Chart Builder می‌باشد که بوسیله آن می‌توانید جدول‌های سفارشی و دلخواه برای هر نوع لاگ مسیجی بسازید.

با Chart Builder جدول ایجاد کنید:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به قسمت Log View رفته و نوع لاگ را انتخاب نمایید.

۳. در نوار ابزار، بر روی Tools> Chart Builder کلیک نمایید.

٤. در پنجره محاوره‌ای باز شده با نام Chart Builder، تنظیمات جدول را انجام داده و بر روی Save کلیک کنید.

یک نام برای جدول انتخاب نمایید	نام
انتخاب کنید که کدام ستون‌ها شامل دیتایی باشند که بر اساس لاگ مسیج‌های نمایش داده شده در صفحه Log View است.	Columns
نحوه گروه‌بندی دیتاها را در نمودار انتخاب کنید.	Group By
نحوه سفارش اطلاعات را در نمودار انتخاب کنید.	Order By
نحوه مرتب‌سازی دیتاها را در نمودار انتخاب نمایید.	Sort
محدودیت‌ها نمایش داده می‌شوند.	Show Limit

Device	**نمایش دستگاه‌های انتخاب شده بر روی صفحه Log View**
Time Frame	**نمایش کادر زمانی انتخاب شده در صفحه Log View**
Query	**نمایش کوئری‌های ایجاد شده**
Preview	**پیش نمایشی از چارت نمایش داده می‌شود.**

گروه‌های لاگ

امکان گروه‌بندی دستگاه‌ها در Log Groups وجود دارد. شما به راحتی می‌توانید خلاصه‌ای از FortiView را مشاهده کنید، لاگ‌ها را ببینید، گزارش ایجاد کنید یا یک handler برای گروه‌بندی لاگ‌ها ایجاد کنید. گروه‌های لاگ مجازی بوده بنابراین آنها دیتابیس SQL نداشته یا فضای اضافی از دیسک اشغال نمی‌کنند.

در فورتی آنالایزر 5.0.6 و قبل از آن، این امکان وجود دارد که گروه‌های لاگ مربوط به یک دستگاه SQL دیتابیس خودشان را داشته باشند. این قابلیت در FortiAnalyzer 5.2 و قبل از آن وجود ندارد.

وقتی دستگاه را با VDOM هایش به لاگ گروه اضافه می‌کنید، تمام VDOMها به صورت خودکار اضافه می‌شوند.

گروه لاگ جدید بسازید:

۱. به مسیر Log View> Log Group بروید.

۲. در نوار ابزار بر روی Create New کلیک کنید.

۳. در کادر محاوره‌ای Create New Log، یک نام برای گروه لاگ انتخاب کرده و دستگاه‌ها را به گروه لاگ اضافه نمایید.

٤. بر روی OK کلیک کنید.

مرور لاگ

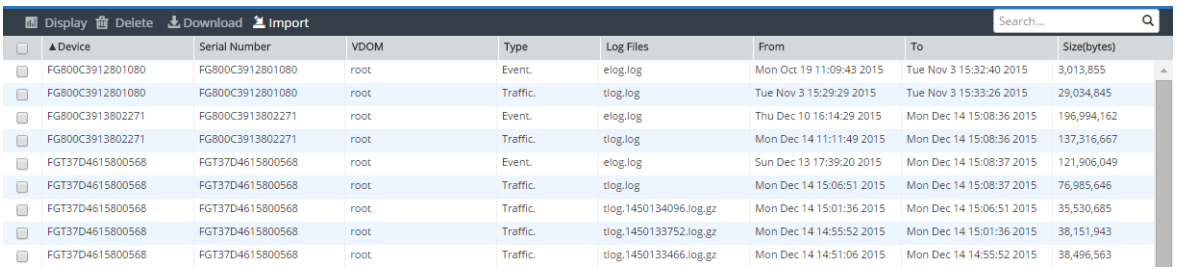
وقتی لاگ فایلی به بالاترین اندازه خود رسید یا به یک زمانبندی از قبل تعیین شده می‌رسد، فورتی آنالایزر بر اساس رول تعریف شده لاگ فایل را تغییر نام می‌دهد. نام فایل بر اساس فرم xlog.N.log که x حرفی است برای نشان دادن نوع ورودی و N یک نام غیرتکراری که متناظر با اولین زمان ورودی لاگ دریافت شده است.

Log Browse لاگ فایل‌هایی را نمایش می‌دهد که برای تمام دستگاه‌ها و خود فورتی آنالایزر ذخیره شده‌اند و می‌توانید در زمان فشرده‌سازی بر اساس زمانبندی تعیین شده این لاگ‌ها را فشرده نمایید.

لاگ فایل‌ها را مشاهده کنید:

۱. به مسیر Log View> Log Browse بروید.

۲. لاگ فایلی را انتخاب کرده و بر روی Display کلیک کنید تا لاگ فایل باز شده و log message در قالب مشخص شده نمایش داده شود.



Device	Serial Number	VDOM	Type	Log Files	From	To	Size(bytes)
FG800C3912801080	FG800C3912801080	root	Event.	elog.log	Mon Oct 19 11:09:43 2015	Tue Nov 3 15:32:40 2015	3,013,855
FG800C3912801080	FG800C3912801080	root	Traffic.	tlog.log	Tue Nov 3 15:29:29 2015	Tue Nov 3 15:33:26 2015	29,034,845
FG800C3913802271	FG800C3913802271	root	Event.	elog.log	Thu Dec 10 16:14:29 2015	Mon Dec 14 15:08:36 2015	196,994,162
FG800C3913802271	FG800C3913802271	root	Traffic.	tlog.log	Mon Dec 14 11:11:49 2015	Mon Dec 14 15:08:36 2015	137,316,667
FGT37D4615800568	FGT37D4615800568	root	Event.	elog.log	Sun Dec 13 17:39:20 2015	Mon Dec 14 15:08:37 2015	121,906,049
FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.log	Mon Dec 14 15:06:51 2015	Mon Dec 14 15:08:37 2015	76,985,646
FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450134096.log.gz	Mon Dec 14 15:01:36 2015	Mon Dec 14 15:06:51 2015	35,530,685
FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450133752.log.gz	Mon Dec 14 14:55:52 2015	Mon Dec 14 15:01:36 2015	38,151,943
FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450133466.log.gz	Mon Dec 14 14:51:06 2015	Mon Dec 14 14:55:52 2015	38,496,563

وارد کردن یک لاگ فایل

زمانی که بازیابی اطلاعات و یا بازخوانی دیتاها برای استفاده موقتی صورت می‌گیرد وارد کردن لاگ فایل‌ها بسیار کاربردی و مفید می‌باشد. برای مثال، اگر لاگ فایل‌های قدیمی از یک دستگاه را داشته باشید می‌توانید این لاگ‌ها را داخل دستگاه فورتی آنالایزر import کرده و گزارشات خود را بر اساس دیتاهای قدیمی ایجاد نمایید.

یک فایل لاگ را وارد کنیم:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Log View> Log Browse بروید و از نوار ابزار بر روی Import کلیک کنید.

۳. از لیست Device، دستگاهی را انتخاب کنید که قرار است لاگ‌ها به داخل آن وارد شود.

اگر گزینه Take From Imported File انتخاب شود، لاگ فایل باید شامل فیلدی با نام device_id باشد.

٤. لاگ فایل را کشیده و در داخل پنجره محاوره‌ای باز شده بیندازید یا بر روی Add Files کلیک کنید و مسیر فایل را مشخص کنید.

۵. OK کنید. پیامی ظاهر می‌شود که نشان می‌دهد آپلود آغاز شده اما اگر صفحه را ببندید فرآیند آپلود لغو می‌شود.

٦. OK کنید. زمان آپلود فایل با توجه به حجم فایل و سرعت اتصال شما متفاوت است.

بعد از آپلود شدن لاگ فایل، فورتی آنالایزر فایل را بررسی می‌کند.

- اگر فیلد device_id در آپلود لاگ فایل با دستگاه مطابقت نداشته باشد وارد کردن دیتاها Fail می‌شود. با کلیک بر روی Return می‌توانید تلاش مجددی را انجام دهید.
- اگر گزینه Take From Imported File را انتخاب کنید و دستگاه فورتی آنالایزر شما در لیست وجود نداشته باشد بعد از آپلود پیامی برای شما نمایش داده می‌شود. بر روی OK کلیک کنید تا لاگ فایل‌ها وارد شده و به صورت خودکار دستگاه به لیست دیوایس‌ها اضافه شود.

دانلود یک لاگ فایل

امکان دانلود یک لاگ فایل جهت ذخیره آن و همچنین استفاده از آن بعنوان یک بکاپ در خارج از دستگاه وجود دارد. دانلود شامل تمام لاگ فایل‌های ورودی می‌باشد.

دانلود کردن یک لاگ فایل:

۱. به مسیر Log View> Log Browse رفته و لاگ فایلی را که می‌خواهید دانلود کنید انتخاب نمایید.

۲. در نوار ابزار بر روی Download کلیک کنید.

۳. در کادر محاوره‌ای Download Log File(s)، تنظیمات دانلود را پیکربندی کنید:

- در لیست فرمت لاگ فایل، Native را انتخاب کرده و Text یا CSV را مشخص کنید.
- اگر تمایل دارید تا فایل را فشرده کنید گزینه Compress with gzip را انتخاب نمایید.

٤. بر روی Download کلیک کنید.

لاگ فایل‌ها را پاک کنید

حذف کردن لاگ فایل ها:

۱. به مسیر Log View> Log Browse بروید.

۲. یک یا چند فایل را انتخاب و Delete را کلیک کنید.

۳. جهت تایید بر روی OK کلیک کنید.

مدیریت رخدادها

مدیریت رخدادها تمام اتفاقات شکل گرفته را نمایش می‌دهد.

چطور ADOMها بر روی رخدادها تاثیر می‌گذارند

زمانی که ADOMها بر روی سیستم فعال می‌شوند، هر ADOM رخداد مربوط به خودش را داشته و لیستی از رخدادها ایجاد می‌گردد. جهت مشاهده Event Management قبل از هر کاری مطمئن شوید که در ADOM درست قرار دارید.

تعریف Event handlers

برای ایجاد Event Management می‌توانید از ایونت هندلر از پیش تعریف شده استفاده کنید. برای دستگاه‌های فورتی‌گیت و فورتی Carrier ایونت هندلر از قبل تعریف شده وجود دارد. برای سایر دستگاه‌ها، ایونت هندلر دلخواه را ایجاد نمایید.

لاگ‌های مورد استفاده برای ایونت ها

Event Management رخدادها را از لاگ‌های تحلیلی نمایش می‌دهد و در فرآیند لاگ‌های آرشیوی هیچگونه تاثیری ندارند.

ایونت هندلِر Event handlers

ایونت هندلرها تعریف می‌شوند تا مشخص کنیم کدام پیغام از لاگ‌ها بازگشایی شده و در event management نمایش داده شوند. یک ایونت هندلر را فعال کنید تا شروع به تولید رخدادها نماید. امکان پیکربندی ایونت هندلر برای

تولید رخدادهای یک دستگاه یا برای همه دستگاه‌ها وجود دارد. پیکربندی سیستم برای ارسال اخطارها به event handler امکان‌پذیر است. همچنین می‌توانید اخطارها را به یک آدرس ایمیل ارسال نمایید.

مدیریت Event Handlers

جهت مدیریت Event handlerها به مسیر زیر بروید:

Event Management> Event Handler List

گزینه	توضیحات
Create New	یک **Event Handler** جدید ایجاد می‌کنیم.
Edit	**Event Handler** انتخاب شده را ویرایش نمایید.
Delete	**Event Handler** انتخاب شده را پاک کنید. در نظر داشته باشید که امکان حذف ایونت هندلرهای از قبل تعریف شده وجود ندارد.
Clone	**Event Handler** انتخاب شده را کلون بگیرید.
Enable	**Event Handler** انتخاب شده را فعال نمایید.
Disable	**Event Handler** انتخاب شده را غیرفعال نمایید.
Collapse All / Expand All	ستون فیلترها را ببندید یا باز نمایید.
Show Predefined	**Handler** تعریف شده در لیست را نمایش/ مخفی نمایید.
Show Custom	**Handler** دلخواه در لیست را نمایش داده یا مخفی کنید.
Factory Reset	اگر در **Event Handler** تعریف شده تغییراتی ایجاد کردید آن را انتخاب کرده و به حالت تنظیمات کارخانه‌ای بازگردانید.

لیستی از ایونت هندلرهای از پیش تعریف شده

فورتی آنالایزر ایونت هندلرهای از پیش تعریف شده‌ای دارد که برای دستگاه‌های فورتی‌گیت و فورتی Carrier بوده و این امکان را به شما می‌دهد تا از رخدادهای ایجاد شده استفاده نمایید.

Event Handler	توضیحات
Antivirus Event	فعال سازی شده به صورت پیش فرض: • **Severity: Medium** • **Log Type: Traffic** • **Event Category: Antivirus** • **Group by: Virus Name** • **Log messages that match all connection:** • **Level Greater Than or Equal To Information** • **Generic Text Filter: virus!='' and virus!='N/A'**
App Ctrl Event	• **nabled by default** • **Severity: Critical** • **Log Type: Traffic** • **Event Category: Application Control** • **Group by: Application Name** • **Log messages that match any of the following conditions:** • **Application Category Equal To Botnet** • **Application Category Equal To Proxy**
Application Crashed Event	**Enabled by default** • **Severity: Medium** • **Log Type: Event Log**

	• **Event Category: System** • **Group by: Log Description** • **Log messages that match all conditions:** • **Log Description Equal To Application crashed** • **Level Greater Than or Equal To Warning**
Botnet Application Allowed by Application Control	**Disabled by default** • **Severity: Critical** • **Log Type: Application Control** • **Group by: Application Name** • **Log messages that match all of the following conditions:** ○ **Application Category Equal to Botnet** ○ **(action==pass or action==monitor)**
Botnet Application Blocked by Application Control	**Disabled by default** • **Severity: High** • **Log Type: Application Control** • **Group by: Application Name** • **Log messages that match all of the following conditions:** ○ **Application Category Equal to Botnet** ○ **Action Not Equal to Pass** ○ **Action Not Equal to Monitor**
Botnet C-and-C Allowed by IP-Reputation	**Disabled by default** • **Severity: High** • **Log Type: Application Control**

	• **Group by: Virus Name**
	• **Log messages that match all of the following conditions:**
	  ○ **Action Not Equal to Blocked**
	  ○ **logid==0202009248 or logid==0202009249**

Botnet C-and-C Blocked by DNS Filtering	**Disabled by default**
	• **Severity: Medium**
	• **Log Type: DNS**
	• **Group by: Message**
	• **Log messages that match all of the following conditions:**
	  ○ **Level Greater Than or Equal to Information**
	  ○ **logid==1501054600 or logid==1501054601**

Botnet C-and-C Blocked by IP-Reputation	**Disabled by default**
	• **Severity: Medium**
	• **Log Type: AntiVirus**
	• **Group by: Virus Name**
	• **Log messages that match all of the following conditions:**
	  ○ **Action Equal to Blocked**
	  ○ **logid==0202009248 or logid==0202009249**

Botnet Traffic Allowed by IPS	**Disabled by default** • **Severity: Critical** • **Log Type: IPS** • **Group by: Attack Name** • **Log messages that match all of the following conditions:**

	○ **Level Greater Than or Equal To Information** ○ **attack ~ Botnet and (action=='detected' or action=='pass session')**
Botnet Traffic Blocked by IPS	**Disabled by default** • **Severity: High** • **Log Type: IPS** • **Group by: Attack Name** • **Log messages that match all of the following conditions:** ○ **Level Greater Than or Equal To Information** ○ **attack ~ Botnet and (action!='detected' or action!='pass session')**
Conserve Mode	**Disabled by default** • **Severity: Critical** • **Log Type: Event** • **Event Category: System** • **Group by: Message** • **Log messages that match all conditions:** ○ **Log Description Equal To System services entered conserve mode**
DLP Event	**Disabled by default** • **Severity: Medium** • **Log Type: Traffic Log** • **Event Category: DLP** • **Group by: DLP Rule Name**

	○ **Log messages that match all conditions:** ○ **Security Action Equal To Blocked**
DNS Botnet C-and-C - High Severity	**Enabled by default** • **Severity: High** • **Log Type: DNS** • **Group by: Message** • **Log messages that match all conditions:** ○ **Level Equal To Warning** ○ **Generic Text Filter: botnetip!='' or botnetdomain!=''**
HA Failover	**Disabled by default** • **Severity: Medium** • **Log Type: Event Log** • **Event Category: HA** • **Group by: Log Description** ○ **Log messages that match any of the following conditions:** ○ **Log Description Equal To Virtual cluster move member** ○ **Log Description Equal To Virtual cluster member state moved**
Interface Down	**isabled by default** • **Severity: High** • **Log Type: Event Log** • **Event Category: System** • **Group by: Message** ○ **Log messages that match all conditions:**

	○ **Action Equal To interface-stat-change** ○ **Status Equal To DOWN**
Interface Up	**Disabled by default** • **Severity: Medium** • **Log Type: Event Log** • **Event Category: System** • **Group by: Message** ○ **Log messages that match all conditions:** ○ **Action Equal To interface-stat-change** ○ **Status Equal To UP**
IPS - Critical Severity	**Enabled by default** • **Severity: Critical** • **Log Type: IPS** • **Group by: Attack Name** ○ **Log messages that match all conditions:** ○ **Severity Equal To Critical**
IPS - High Severity	**Enabled by default** • **Severity: High** • **Log Type: IPS** • **Group by: Attack Name** ○ **Log messages that match all conditions:** ○ **Severity Equal To High**
Web Filter Event	**Enabled by default** • **Severity: Medium** • **Log Type: Traffic Log**

	• **Event Category: Web Filter**
	• **Group by: Category**
	• **Log messages that match any of the following conditions:**
	  ○ **Web Category Equal To Child Abuse**
	  ○ **Web Category Equal To Discrimination**
	  ○ **Web Category Equal To Drug Abuse**
	  ○ **Web Category Equal to Explicit Violence**
	  ○ **Web Category Equal to Extremist Groups**
	  ○ **Web Category Equal to Hacking**
	  ○ **Web Category Equal to Illegal or Unethical**
	  ○ **Web Category Equal to Plagiarism**
	  ○ **Web Category Equal to Proxy Avoidance**
	  ○ **Web Category Equal to Malicious Websites**
	  ○ **Web Category Equal to Phishing**
	  ○ **Web Category Equal to Spam URLs**

فعال سازی event handlers

برای هر دو حالت از پیش تعریف شده و دلخواه ابتدا باید event handler را فعال کرده تا بعد از آن رخدادها ایجاد گردند. در لیست ایونت هندلر ستون Name نمایش آیکون  برای فعال سازی ایونت هندلر بوده و آیکون  نشان از غیرفعال بودن آن دارد.

اگر تمایل دارید تا اخطارها را از ایونت هندلرهای از قبل تعریف شده دریافت نمایید، ایونت هندلر از پیش تعریف شده را ویرایش کرده و اخطارها را پیکربندی نمایید.

فعال سازی ایونت هندلرها:

۱. اگر از ADOM استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Event Management> Event Handler List بروید.

۳. یک یا چند ایونت هندلر را انتخاب نمایید و سپس بر روی More> Enable کلیک کرده و Enable را انتخاب نمایید.

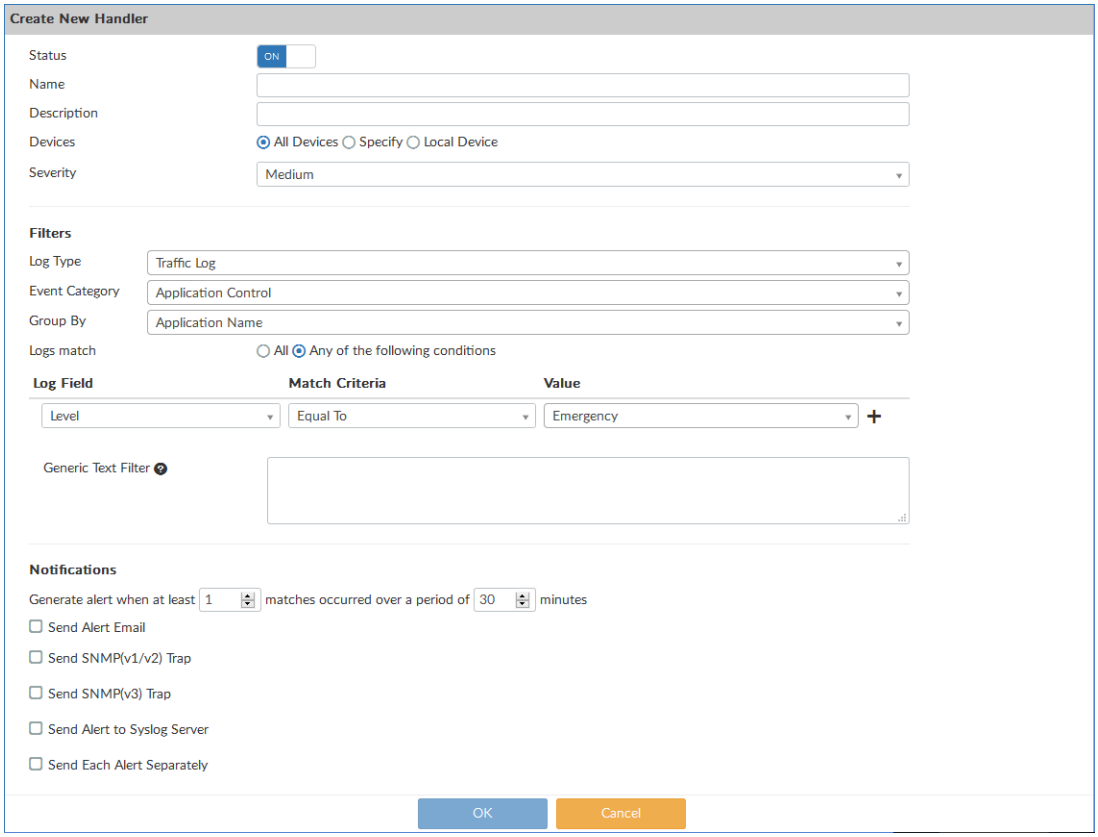
ایجاد ایونت هندلرهای دلخواه

ساختن یک ایونت هندلر جدید:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Event Management> Event Handler List بروید.

۳. در نوار ابزار، بر روی Create New کلیک کنید.



٤. بر اساس نیاز پیکربندی را انجام داده و بر روی OK کلیک کنید.

٥. با کلیک بر روی OK ایونت هندلر جدید ایجاد می‌شود.

ایجاد یک صفحه هندلر جدید

توضیحات زیر در مورد تنظیمات موجود در Create New Handler pane است.

فیلد	توضیحات
Status	فعال/غیرفعال کردن رخدادهای هندلر می‌باشد.
Name	اضافه کردن یک نام برای هندلر است.
Description	توضیحات در مورد ایونت هندلر می‌باشد.
Devices	انتخاب دستگاه‌هایی شامل:

	○ تمام دستگاه‌ها ○ مشخص شده: اضافه کردن دستگاه‌ها، کلیک بر روی آیکون **Add** ○ دستگاه داخلی
Severity	انتخاب **severity** از لیست که شامل موارد زیر می‌باشد: • **Critical** • **High** • **Medium** • **Low**
Filters	برای هندلر فیلترها را پیکربندی می‌کنید.
Log Type	وقتی دستگاه به صورت لوکال پیکربندی می‌شود می‌توانید لاگ فایل را از لیست انتخاب نمایید. امکان ایجاد تغییرات در **Log Type**، **Event Category**،**Group By** وجود ندارد.
Event Category	گروهی از ایونت هندلر انتخاب می‌گردد. موجودیت این بخش وابستگی به نوع پلتفرمی که انتخاب شده خواهد داشت.
Group By	چگونگی انتخاب گروه رخدادها مشخص می‌گردد.
Logs Match	انتخاب **All** یا **Any** بر اساس شرایط تعریف شده
Log Field	فیلد لاگ فیلتر شده از لیست انتخاب می‌گردد. موجودیت این گزینه وابستگی دارد به نوع لاگی که انتخاب شده است.
Match Criteria	از لیست معیار منطبق را انتخاب نمایید. گزینه‌های موجود بستگی دارد به فیلد لاگی که انتخاب شده است.
Value	مقداری از لیست و یا وارد کردن مقادیری در باکس نوشتاری انتخاب می‌شوند. گزینه‌های موجود بستگی دارد به فیلد لاگی که انتخاب شده است.

Add	فیلتر لاگ اضافه می‌گردد. وقتی دستگاه به صورت داخلی تنظیم می‌گردد این گزینه در دسترس نمی‌باشد. در این حالت فقط یک لاگ فیلتر موجود است.
Remove	حذف کردن فیلتر
Generic Text Filter	یک فیلتر نوشتاری عمومی وارد نمایید.
Notification	پیکربندی اخطارهای اعلام شده در هندلر در این بخش تنظیم می‌گردد.
Generate alert when at least n matches occurred over a period of n minutes	مقدار **threshold** برای ایجاد اخطار وارد نمایید. تعداد رخدادهای مربوط را وارد نمایید و مشخص کنید که در چند دقیقه باید برای ایجاد یک هشدار رخ دهد.
Send Alert Email	یک اخطار بوسیله ایمیل ارسال می‌گردد. پارامترهای ایمیل در داخل تنظیمات میل سرور مشخص می‌گردد.
Send SNMP community Trap	یک یا هر دو چک باکس انتخاب شده و مشخص نمودن **SNMP community** یا کاربر از لیست انتخاب شده.
Send Alert to Syslog Server	اخطار به **syslog** سرور ارسال می‌گردد. انتخاب **syslog** سرور از لیست انجام می‌شود.
Send Each Alert Separately	با انتخاب این گزینه هر اخطار به صورت مجزا ارسال می‌گردد.

فیلتر ایونت هندلرها

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Event Management> Event Handler List بروید.

۳. در نوار ابزار بر روی More> Show Predefined یا More> Show Custom کلیک نمایید تا event handler مورد نظر را فیلتر کنید.

جستجو ایونت هندلرها

جستجو کردن ایونت هندلرها:

۱. به مسیر Event Management> Event Handler List بروید.

۲. گزینه مورد نظر جهت جستجو را در فیلد مشخص شده تایپ کنید.

بازگردانی به تنظیمات کارخانه‌ای از طریق ریست کردن

امکان ایجاد تغییرات در ایونت هندلرهای از پیش تعریف شده بر اساس نیاز وجود دارد. در صورت درخواست می‌توانید ایونت هندلرهای از پیش تعریف شده را به تنظیمات کارخانه‌ای بازگردانید.

ریست ایونت هندلرهای از پیش تعریف شده:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Event Management> Event Handler بروید.

۳. مطمئن شوید که تیک گزینه Show Predefined خورده باشد.

٤. یک یا چند ایونت هندلر از پیش تعریف شده را انتخاب نمایید.

۵. بر روی More> Factory Reset کلیک نمایید تا تنظیمات به حالت پیش فرض کارخانه‌ای بازگردد.

امکان ریست و بازگشت به تنظیمات کارخانه‌ای از طریق صفحه Edit Handler هم وجود دارد.

رخدادها Events

بعد از تولید رخدادها توسط ایونت هندلرها، امکان مشاهده رخدادها به همراه جزئیاتشان برای شما فراهم می‌گردد. در قسمت Event Management> All Events رخدادها با نوع و شدتی که دارند در یک قالب گرافیکی نمایش داده می‌شوند. همچنین رخدادهایی که اخیرا به وقوع پیوستند در یک جدول نمایش داده می‌شوند.

در قسمت Event Management> Calendar رخدادها بوسیله ماه یا هفته در یک تقویم زمانی یا نمودار میله‌ای نمایش داده می‌شوند. وقتی ریبیلد SQL را انجام می‌دهید ممکن است مشاهده کامل لیست تاریخچه رخدادها وجود نداشته باشد. هرچند ممکن است همیشه رخدادهای لحظه‌ای را در لاگ‌ها مشاهده کنید. امکان مشاهده وضعیت بازسازی SQL بوسیله چک کردن وضعیت Rebuilding DB در Notification Center وجود دارد.

خلاصه رویدادها

- برای مشاهده خلاصه‌ای از رویدادها به مسیر زیر مراجعه کنید:

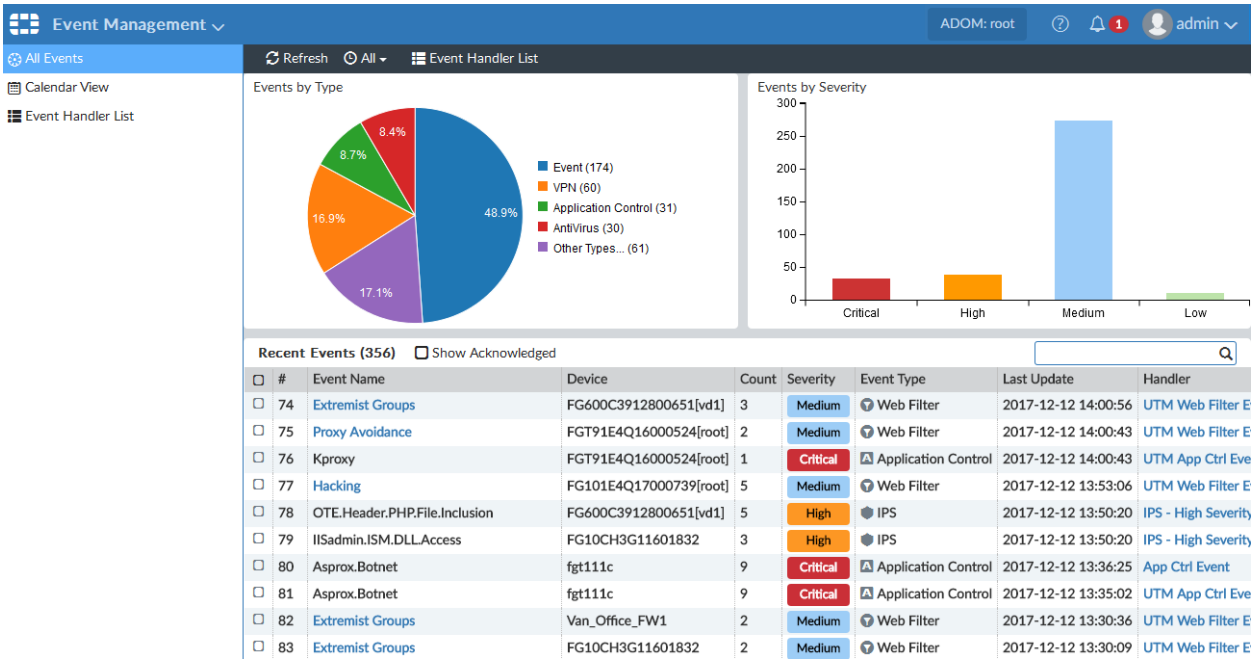
Event Management> All Events.

- برای بازخوانی دستی دیتاهای خلاصه شده ایونت‌ها بر روی Refresh کلیک نمایید.

این قابلیت وجود دارد که صفحه در بازه‌های زمانی مختلف به صورت خودکار بازخوانی شود.

- تغییر دوره زمانی نمایش، بر روی آیکون زمان کلیک کرده و یک بازه زمانی مشخص نمایید.
- برای مشاهده ایونت هندلرها بر روی Event Handler List کلیک کنید.

All Event نمایش دهنده تمام رویدادها و اتفاقات بر اساس نوع و شدت آنها در یک فرمت گرافیکی بوده و رویدادهای اخیر در یک فرمت جدولی ذخیره می‌شوند.



Event by Type	**رویدادها بر اساس نوع در یک نمودار دایره‌ای نمایش و سازماندهی می‌شوند.** • **برای مشاهده تعداد اخطارها و تعداد لاگ‌ها، مکان نما را بر روی بخشی از دایره قرار دهید.**

	• جهت مشاهده لیستی که فقط ایونت‌ها باseverity می‌باشند بر روی نوار چارت کلیک نمایید.
Events by Severity	ایونت‌ها در یک نمودار میله‌ای سازمان‌دهی شده بوسیله شدت رخدادها نمایش داده می‌شوند. • مشاهده تعداد اخطارها و تعداد لاگ‌ها، مکان نما را بر روی نمودار قرار دهید. • جهت مشاهده رویدادهایی که فقط شدت بالایی دارند بر روی نوار در چارت کلیک کنید.
Recent Event	نمایش دهنده رخدادها بر اساس مدت زمان انتخاب شده می‌باشد. • مرتب‌سازی بوسیله یک ستون، کلیک بر روی هدر ستون انجام می‌پذیرد. • ایونت‌های پذیرفته شده را شامل می‌گردد. • جستجو کردن در لیست، تایپ عبارت جستجو در قسمتی که مربوط به جستجو است. • برای ویرایش هندلر، بر روی المان هندلر کلیک نمایید. • برای مشاهده اطلاعات در مورد یک ایونت و اتفاقات مربوط به آن بر روی هایپرلینک Event Name کلیک نمایید. این گزینه فقط برای بعضی از ایونت‌ها موجود است. • برای مشاهده جزئیات رخدادها بر روی event line کلیک نمایید.

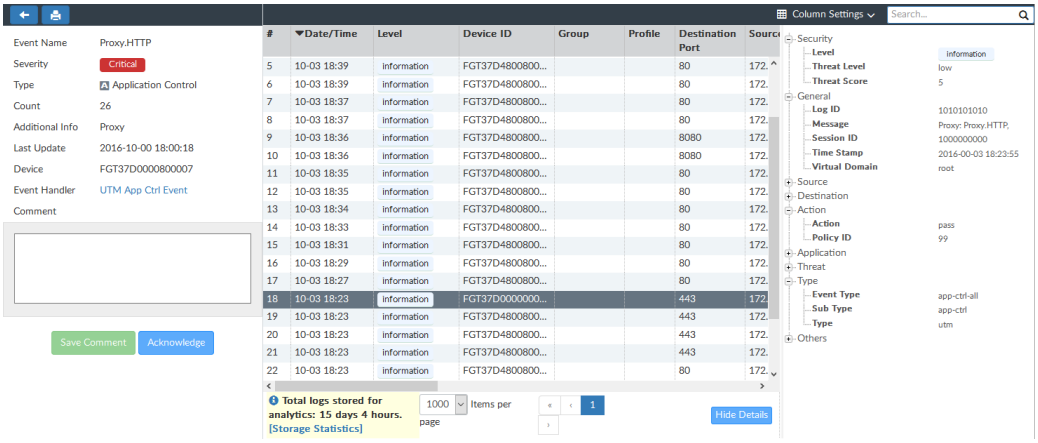
فیلتر لیست رخدادها

در قسمت‌های Event by Type و Events by Severity، بر روی یک المان کلیک کرده تا فقط ایونت‌هایی که شدت بالایی دارند نمایش داده شوند. لیست رخدادهایی که فیلتر شده‌اند نمایش دهنده اطلاعات مشابه و انتخابی در Recent Events لیست می‌باشند.

برای بازگشت به صفحه قبلی بر روی دکمه بازگشت کلیک کنید.

جزئیات رخداد

در قسمت Recent Events یا لیست رخدادهای فیلترشده، برای مشاهده جزئیات رخداد، بر روی خط ایونت دابل کلیک کنید تا جزئیات بیشتری را مشاهده نمایید.



صفحه جزئیات رخدادها شامل اطلاعاتی در مورد رخدادها و لیست تمامی لاگ‌ها می‌باشد. می‌توانید از رخدادها پرینت گرفته، اعلام آگاهی نمایید و یا توضیحی به یک رخداد اضافه نمایید.

- جهت تغییر دادن ستون‌های نمایشی بر روی Column Settings یا Column Settings> More Columns کلیک کنید.
- بر روی یک خط دابل کلیک کنید یا یک خط را انتخاب کرده و بر روی Display Details کلیک کنید. پنجره جزئیات مربوط به لاگ‌ها در گوشه سمت راست باز می‌شود و می‌توانید جزئیات بیشتری را مشاهده کنید.
- برای بازگشت به صفحه قبلی کافی است بر روی دکمه بازگشت کلیک کنید.

تصدیق وضعیت رخدادها Acknowledging events

آگاهی و پاک کردن رخداد از لیست اتفاقات اخیر در این قسمت انجام می‌گیرد.

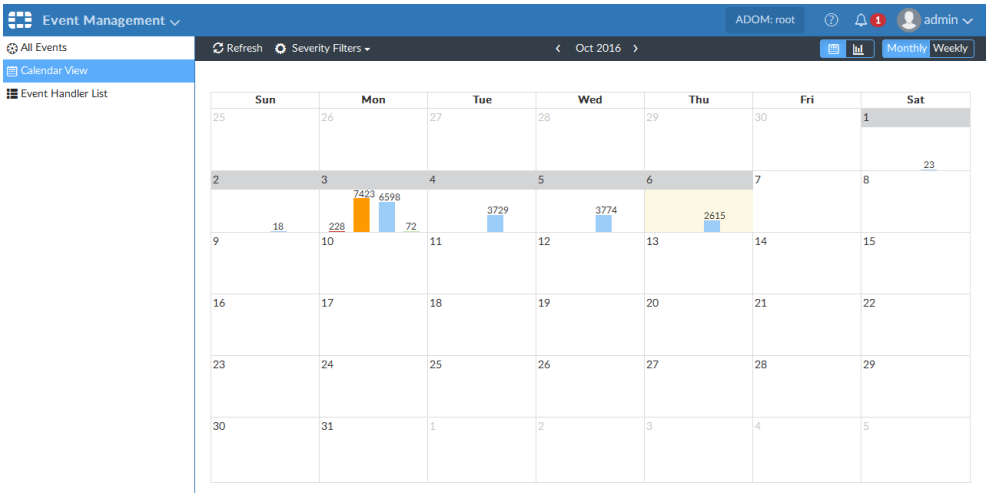
شناسایی رخدادها:

- در لیست رخدادهای اخیر، یک یا چند رخداد را انتخاب نمایید. سپس راست کلیک کرده و Acknowledge را انتخاب نمایید.

- در صفحه جزئیات رخداد، بر روی Acknowledge کلیک نمایید.

تقویم رویدادها

Calendar View رویدادها را با ماه یا هفته در تقویم و یا از طریق نمودار میله‌ای برای شما نمایش می‌دهد.

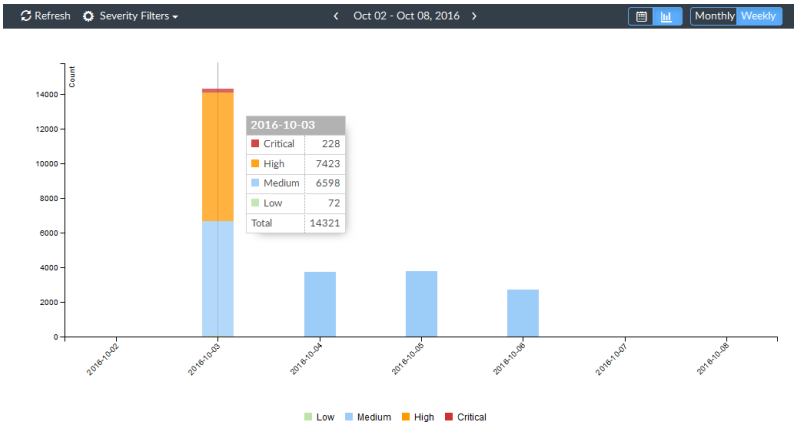


این قسمت فقط شامل رویدادهایی می‌شوند که severity مشخصی داشته باشند. بر روی Severity Filters کلیک کرده و سطح severity را انتخاب نمایید. به صورت پیش فرض سطوح بحرانی و بالاترین severityها موجود هستند.

با کلیک بر روی هر عنصر در هر قسمتی که مشاهده می‌کنید لیست رویدادهای فیلتر شده باز می‌شود.

با کلیک بر روی دکمه نمودار تقویم در نوار ابزار، تقویم نمایش داده می‌شود. نمایش تقویم به صورت ماهیانه حکایت از آن دارد که نمودار خطی وقایع بوسیله severity بر روی هر روز از ماه می‌باشد. نمایش به صورت هفتگی رخدادها برای هر ساعت از هر روز هفته را نشان می‌دهد. بر روی فلشی که در هر دو قسمت تقویم قرار دارد کلیک کنید تا به ماه یا هفته بعدی بروید.

با کلیک بر روی دکمه Bar Chart در نوار ابزار نمای نمودار میله‌ای را تغییر می‌دهید. نمودار میله‌ای نمایش دهنده یک سری دیتای انباشته شده می‌باشد که به صورت نمودار خطی عمودی در برابر زمان می‌باشند. حرکت نشانگر روی یک نوار نمایش دهنده تعداد لاگ‌های هر severity و کل آن روز است.



گزارشات

با استفاده از این قابلیت می‌توانید از لاگ‌های جمع آوری شده گزارش‌های دلخواه خود را تهیه نمایید.

- از گزارش‌های تعریف شده در سیستم استفاده نمایید. قالب‌های گزارشی از پیش تعریف شده، چارت‌ها و ماکروهای موجود جهت کمک به کاربران برای ساخت و ایجاد گزارش‌های جدید در نظر گرفته شده است.
- ایجاد و ساخت گزارش‌های دلخواه

فایل‌های گزارشی در فضای رزرو شده ذخیره می‌گردند تا دستگاه بتواند از آنها استفاده نماید.

وقتی عمل بازسازی SQL را انجام می‌دهید ، گزارشی در دسترس نیست تا زمانی که بازسازی تکمیل گردد. انتخاب لینک Show Progress وضعیت rebuild مجدد SQL را برای شما نمایش می‌دهد.

ADOMهایی که تحت تاثیر گزارشات قرار می‌گیرند

زمانی که ADOMها فعال هستند، هر ADOM گزارش‌ها، کتابخانه‌ها، تنظیمات پیشرفته و ... مخصوص به خود را دارد. قبل از انتخاب یا ایجاد یک گزارش مطمئن شوید که در ADOM درستی قرار دارید.

بعضی از گزارش‌ها فقط در ADOMهای فعال موجود می‌باشند. برای مثال ADOMها باید وجود داشته باشند تا امکان دسترسی به گزارش‌های فورتی کش، فورتی کلاینت، فورتی دی داس و ... وجود داشته باشد.

امکان ایجاد گزارش‌هایی برای دستگاه‌های مختلف در پیش فرض هر ADOM وجود دارد.

گزارش‌های از قبل تعریف شده ، قالب ها، چارت ها، ماکروها

برای ایجاد گزارش‌های مورد نیاز فورتی آنالایزر المان‌هایی موجود است که به شما در این زمینه کمک خواهد کرد.

گزارش از پیش تعریف شده	موقعیت در محیط گرافیکی	هدف
Reports	Reports> Report Definitions >All Reports	گزارش‌ها به صورت مستقیم یا با حداقل تنظیمات ممکن ایجاد می‌گردد. گزارش‌های از قبل تعریف شده در حقیقت قالب‌های گزارشی هستند که با تنظیمات حداقلی ایجاد شده‌اند.
Templates	Reports> Report Definitions> Templates	امکان ایجاد قالب‌ها به صورت مستقیم وجود دارد. قالب‌های گزارشی شامل چارتها، ماکروها و طرح‌بندی‌های مشخص از گزارش‌ها می‌باشند. یک قالب شامل تبِ **layout** یک گزارش ساخته شده است.
Charts	Reports> Report Definitions> Chart Library	امکان استفاده مستقیم وجود دارد. نمودارها را می‌توانید بر روی یک قالب گزارشی ایجاد نمایید. نمودارها مشخص کننده اطلاعات خارج شده از لاگ‌ها می‌باشند.
Macros	Reports> Report Definitions> Macro Library	امکان استفاده به صورت مستقیم یا ساخت بر روی قالب گزارشی که در حال ایجاد می‌باشید در تب **Layout** امکان پذیر می‌باشد. ماکروها مشخص کننده اطلاعات استخراج شده از لاگ‌ها می‌باشند.

لاگ‌های مورد استفاده گزارش ها

Reportsها جهت ایجاد گزارش‌های تحلیلی بکار برده می‌شوند اما لاگ‌های آرشیوی برای تولید گزارش‌ها استفاده نمی‌شوند.

چگونه نمودارها و ماکروها اطلاعات را از لاگ‌ها استخراج می کنند

گزارش‌ها شامل چارتها یا ماکروها هستند. هر جدول یا نمودار مرتبط با مجموعه‌ای از داده‌ها است. وقتی گزارشی ایجاد می‌شود، مجموعه دیتا مرتبط با هر جدول و ماکرو دیتاها را از لاگ‌ها استخراج می‌کند.

فورتی آنالایزر شامل تعدادی از چارت‌ها و ماکروهای از پیش تعریف شده می‌باشد. امکان تعریف جدول و ماکرو دلخواه وجود دارد.

چگونگی کارکرد auto-cache

زمانی که شما یک گزارش را ایجاد می‌کنید ممکن است چندین روز زمان صرف جمع آوری داده‌ها شود تا بتوانید گزارش را تولید نمایید. این زمان با بزرگ شدن مجموعه داده‌های شما بزرگتر می‌گردد. به جای قرار دادن مجموعه‌ای از داده‌ها در یک زمان جهت تهیه گزارش می‌توانید از قابلیت auto cache برای گزارش‌های فعال استفاده نمایید.

Auto-cache تنظیمی است که سیستم را به صورت خودکار hard cache را تولید می‌کند. Hcache یا Hard Cache به این معنی است که کش بر روی هارد باقی می‌ماند. Hcache بکار بردن matured دیتابیس جدول است. زمانی که پایگاه داده rolls به mature شده است. یعنی جدول دیگر رشد نخواهد کرد. جهت کوئری گرفتن از SQL از hcache استفاده می‌شود. Hcache نتایج موقت کوئری‌ها را به صورت matured از جدول دیتابیس و با روشی پیشرفته کش می‌کند. زمانی که این وضعیت برای یک گزارش بوجود می‌آید، بسیاری از مجموعه داده‌ها در حال سرهمبندی و مونتاژ می‌باشند و سیستم فقط نیاز به ادغام نتایج از hchaceها دارد. این روش باعث کاهش زمان ایجاد به صورت قابل ملاحظه‌ای می‌شود. پروسه auto-cache از منابع سیستمی استفاده می‌کند تا کش دیتابیس را ایجاد کرده و این خود باعث ایجاد یک فضای مخصوصی می‌شود تا نتایج کوئری را در آنجا قرار دهد. برای گزارش‌هایی که نیازمند یک زمان طولانی جهت ایجاد مجموعه‌ای از داده دارند باید Auto-cache فعال گردد.

تولید گزارش

برای ایجاد یک گزارش کافی است از قسمت گزارش‌های از پیش تعریف شده یا بوسیله گزارش دلخواه اقدام نمایید. تمام گزارش‌های از پیش تعریف شده و گزارش‌های دلخواه در قسمت:

Reports> Report Definitions> All Reports

لیست شده‌اند.

یک گزارش ایجاد کنیم:

۱. به مسیر Reports> Report Definitions> All Reports بروید.

۲. در پنجره content، یک گزارش از لیست انتخاب نمایید.

۳. به صورت دلخواه از نوار ابزار بر روی Edit کلیک نموده و تنظیمات موجود بر روی تب Settings and Layout را ویرایش نمایید.

٤. در نوار ابزار، بر روی Run Report کلیک کنید.

مشاهده گزارش‌های تکمیل شده

بعد از ایجاد گزارش‌ها به صورت کامل می‌توانید آنها را در مسیر زیر مشاهده کنید:

Reports> Generated Reports

یا

Reports> Report Definitions> All Reports

امکان خروجی گرفتن از گزارش‌ها در فرمتهای زیر وجود دارد:

HTML, PDF, XML, CSV

مشاهده کامل گزارش‌های تولید شده:

۱. به مسیر زیر مراجعه کنید:

Reports> Generated Reports

این بخش نمایش دهنده تمام گزارش‌های تولید شده برای بازه زمانی مشخص می‌باشد.

۲. امکان مرتب‌سازی لیست گزارش‌ها بوسیله تاریخ وجود دارد. بر روی Order by Time کلیک کنید. مرتب‌سازی لیست گزارشی بر اساس نام گزارش با کلیک کردن بر روی Order by Name میسر می‌شود.

۳. مسیری که قرار است گزارش در آنجا قرار بگیرد همراه با فرمتی که مایل هستید تا گزارش را مشاهده کنید انتخاب نمایید. برای مثال اگر تمایل دارید تا گزارش را در فرمت HTML مشاهده کنید بر روی لینک HTML کلیک نمایید.

گزارش‌های تکمیل شده را در All Reports مشاهده کنید:

۱. به مسیر زیر بروید:

Reports> Report Definitions> All Reports

۲. در لیست گزارش‌ها برای باز شدن گزارش بر روی آن دابل کلیک کنید.

۳. در تب View Report، مسیر گزارش به همراه فرمتی که قرار است با آن گزارش را مشاهده کنید انتخاب نمایید.

برای مثال، اگر تمایل دارید بازخوانی گزارش در حالت HTML باشد بر روی لینک HTML کلیک نمایید.

فعال سازی auto-cache

جهت ایجاد گزارش‌هایی که زمان زیادی جهت ساخت برای آنها صرف می‌شود می‌توانید این گزینه را فعال نمایید.
برای فعال سازی این قابلیت کافی است به مسیر زیر بروید:

Reports> Report Definitions> All Reports

و در ستون Cache Status وضعیت سیستم را مشاهده کنید.

فعال سازی auto-cache:

۱. به مسیر Reports> Report Definitions> All Reports بروید.

۲. از لیست، گزارش را انتخاب کرده و در نوار ابزار بر روی Edit کلیک نمایید.

۳. در تب Settings، تیک گزینه Enable Auto-cache را بزنید.

٤. بر روی Apply کلیک نمایید.

گروه‌بندی گزارش‌ها

اگر تعداد زیادی گزارش که شبیه به یکدیگر هستند را اجرا می‌کنید این امکان در اختیار شما گذاشته شده است تا بوسیله گروه‌بندی گزارش‌ها زمان بسیار زیادی را کاهش دهید و فرآیند ایجاد گزارش را بهبود ببخشید.

- کاهش تعداد جداول hcache
- بهبود در زمان انجام auto-cache
- بهبود زمان تنظیم گزارش

قدم ۱: پیکربندی گروهی گزارش ها

برای مثال، گزارش‌های گروهی با سرفصل‌هایی شامل security_Report بوسیله ID دستگاه و VDOM امکان پذیر است.

دستورات زیر را در محیط CLI وارد کنید:

```
config system report group
edit 0
set adom root
config group-by
edit devid
next
edit vd
next
end
set report-like Security_Report
next
end
```

- توجه داشته باشید که دستورات به حروف بزرگ و کوچک حساس می‌باشند.
- Group-by مقدار کنترلی است که چگونگی گروه‌بندی کش‌ها را بررسی می‌کند.
- جهت مشاهده گزارش، گروه‌بندی اطلاعات، دستورات زیر را در CLI وارد نمایید.

```
execute sql-report list-schedule <ADOM>
```

قدم۲: آماده سازی rebuild جداول hcache

برای آماده سازی و شروع، دستورات زیر را در محیط CLI وارد نمایید:

```
diagnose sql hcache rebuild-report <start-time> <end-time>
Where <start-time> and <end-time> are in the format: <yyyy-mm-dd hh:mm:ss>
```

بازیابی گزارش لاگ‌های تشخیصی

اولین باری که گزارشی را شروع می‌کنید، فورتی آنالایزر لاگی در مورد گزارش تولید شده ایجاد می‌کند. این لاگ که تشخیصی نامیده می‌شود در جهت رفع ایرادات و مسایل مربوط به عملکرد گزارش ایجاد شده است. برای مثال، اگر گزارش شما خیلی معمولی تولید شود، امکان استفاده از این لاگ در جهت بازبینی کارایی سیستم وجود دارد. همچنین می‌توانید بالاترین زمان تولید هر جدول را مشخص نمایید.

لاگ‌های تولید گزارش بازیابی:

۱. به مسیر Reports> Generated Report رفته و بر روی گزارش راست کلیک کرده و گزینه Retrieve Diagnostic را انتخاب نمایید.

۲. از یک ویرایشگر متنی جهت باز کردن لاگ استفاده نمایید.

گزارش‌های خودکار تولید شده

گزارش Cyber Threat Assessment به صورت خودکار تولید می‌شود. به صورت پیش فرض، گزارش در ساعت 3:00 AM هر دوشنبه اجرا می‌گردد. برای بدست آوردن اطلاعات بیشتر بر روی زمانبندی گزارش کلیک کنید.

این موضوع فقط بر روی فورتی آنالایزر یا ADOM جدید که ایجاد شده است تاثیر می‌گذارد.

گزارش‌های زمانبندی

۱. به مسیر Reports> Report Definitions> All Reports بروید.

۲. یک گزارش را انتخاب کرده و بر روی نوار ابزار Edit کلیک کنید.

۳. از روی نوار ابزار بر روی Settings کلیک نمایید.

٤. گزینه Enable Schedule را تیک زده و تنظیمات مربوط به زمانبندی را انجام دهید.

۵. بر روی Apply کلیک کنید.

ایجاد گزارش ها

از طریق قالب‌های گزارشی، کلون گرفتن و یا ویرایش گزارش‌های موجود یا از پیش تعریف شده می‌توان یک گزارش را ایجاد نمود.

ایجاد گزارش‌ها از طریق قالب‌های گزارشی:

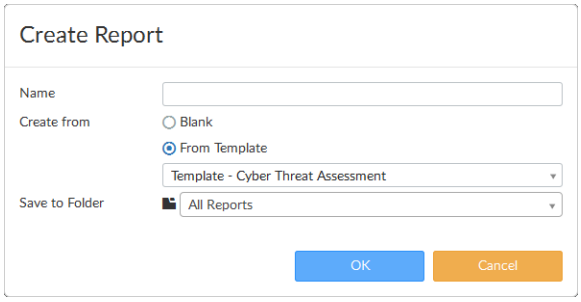
امکان ایجاد یک گزارش جدید از یک قالب وجود دارد. این قالب عموما از تب Layout از گزارش می‌باشد. این قالب متن، چارت‌ها و ماکروهایی که در گزارش استفاده می‌شوند را مشخص می‌کند. قالب گزارشی هیچ دیتایی ندارد و وقتی دیتا به گزارش اضافه می‌شود که شما آن را ایجاد می‌نمایید.

ساخت یک گزارش جدید از یک قالب:

۱. اگر از ADOM استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Report Definitions> All Report بروید.

۳. در نوار ابزار، بر روی Create New کلیک کنید. پنجره محاوره‌ای Create Report باز می‌شود.



٤. در قسمت Name، یک نام برای گزارش جدید تایپ نمایید.

۵. از قسمت From Template گزینه Create را برای ایجاد یک قالب انتخاب نمایید.

٦. از لیست، فولدر جدیدی که گزارش را ذخیره خواهد کرد انتخاب نمایید.

۷. OK را زده تا گزارش جدیدی ایجاد شود.

۸. در تب Settings تنظیمات مورد نیاز را پیکربندی نمایید. اگر امکان دارد برای فیلدها توضیحات بگذارید.

۹. به تب Layout بروید تا قسمت Layout گزارش را سفارشی سازی کنید.(این قسمت اختیاری می‌باشد)

۱۰. با کلیک بر روی Apply گزارش‌ها را ذخیره نمایید.

ایجاد گزارش‌ها بوسیله گرفتن کلون و یا ویرایش کردن

ساخت یک گزارش بوسیله Cloning و ویرایش:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست هستید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در پنجره content، از لیست گزارش را انتخاب و سپس بر روی Clone از نوار ابزار کلیک کنید.

٤. در پنجره محاوره‌ای Clone Report، یک نام تایپ کنید.

۵. فولدری که قرار است گزارش جدید در آن ذخیره شود را انتخاب نمایید.

٦. با کلیک بر روی OK گزارش جدید ساخته می‌شود.

۷. در تب Settings تنظیمات را بر اساس درخواست پیکربندی کنید.

۸. به صورت دلخواه به تب Layout بروید تا Layout گزارش‌ها و محتوا را سفارشی‌سازی نمایید.

۹. با کلیک بر روی Apply تغییرات را ذخیره نمایید.

ساخت گزارش بدون استفاده از قالب

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در نوار ابزار بر روی Create New کلیک کنید. پنجره Create New Report باز می‌شود.

٤. در فیلد Name، نامی را برای گزارش جدید انتخاب نمایید.

۵. گزینه Blank را انتخاب نمایید.

٦. از لیست فولدری که قرار است گزارش جدید در آنجا ذخیره شود را انتخاب نمایید.

۷. با انتخاب OK گزارش جدید ساخته می‌شود.

۸. در تبِ Setting، می‌توانید دوره زمانی برای گزارش مشخص نمایید. همچنین تعیین کنید که کدام دستگاه‌ها شامل گزارش‌های لاگ شوند.

۹. در تب Layout، می‌توانید جداول و ماکروهایی که شامل گزارش می‌شوند را مشخص نمایید.

۱۰. با کلیک بر روی Apply تغییرات ذخیره می‌شوند.

تنظیمات گزارش

گزینه‌های زیر در تبِ Settings وجود دارند:

فیلد	توضیحات
Time Period	**دوره زمانی که گزارش‌ها پوشش می‌دهند. زمانی را مشخص یا به دلخواه انتخاب نمایید. به صورت دستی شروع و پایین و زمان و ساعت را مشخص نمایید.**
Devices	**دستگاه‌هایی که شامل این گزارش‌ها می‌شوند. All Devices یا Specify را انتخاب کرده تا دستگاهی را مشخص نمایید. آیکون اضافه کردن را انتخاب نمایید تا دستگاه انتخاب گردد.**
Type	**گزینه Single Report یا Multiple Report را انتخاب نمایید. این گزینه در صورتی موجود است که چندین دستگاه انتخاب شوند.**
Enable Schedule	**فعال کردن قالب زمانبندی گزارش**
Enable Auto-Cache	**انتخاب پایگاه داده قبل از تولید گزارش در زمانی که داده‌ها موجود می‌باشند. این پروسه از منابعی که برای گزارش‌گیری می‌باشند استفاده می‌کند. غیرفعال کردن این گزینه برای گزارش‌های غیرقابل استفاده می‌باشد.**

فعال سازی زمانی مفید است که برای گزارش‌گیری نیاز به زمان کمتری دارید.	
زمان ارسال گزارش را انتخاب نمایید.	Generate PDF Report Every
تاریخ و زمانی برای شروع تولید فایل وارد نمایید.	Start time
تاریخ و زمانی برای پایان تولید فایل وارد نمایید.	End time
اعلان گزارش را فعال نمایید.	Enable Notification
از لیست پروفایل‌های خروجی را انتخاب یا بر روی **Create New** کلیک نمایید تا یک پروفایل جدید ساخته شود.	Output Profile

فیلترها از تنظیمات گزارشات

گزینه‌های زیر در تبِ Advanced Settings وجود دارند.

توضیحات	فیلد
زبان گرازش را انتخاب کنید.	Language
نتایج دسته‌بندی نشده را در سایر گروه‌ها قرار دهید.	Bundle rest into “others”
چاپ به صورت پرتره تنظیم می‌شود.	Print Orientation
تنظیم سطح **heading** برای جدول **heading** انجام می‌شود.	Chart Heading Level
فونت پیش فرض را تنظیم نمایید.	Default Font
ستون‌های مخفی را انتخاب نمایید.	Hide # Column
متن هدر و عکس آن انتخاب می‌شود. فورتی‌نت از عکس پیش فرض استفاده می‌کند اما می‌توانید از عکسی متفاوت استفاده نمایید.	Layout Header

Layout Footer	فوتر پیش فرض یا با انتخاب گزینه دلخواه می‌توانید فوتر مورد نظر خود را ثبت کنید.
Print Cover Page	کاوری را برای پرینت انتخاب نمایید.
Print Table of Contents	محتوای جدول را انتخاب نمایید.
Print Device List	لیست دستگاهی که قرار است چاپ شود را انتخاب نمایید.
Print Report Filters	چاپ فیلترهای اعمال شده به گزارش انتخاب می‌گردد.
Obfuscate User	جهت مخفی کردن اطلاعات کاربر در گزارش مورد استفاده قرار می‌گیرد.
Resolve Hostname	جهت شناسایی هاست‌ها در گزارش انتخاب می‌گردد.
Allow Save Maximum	مقادیری بین ۱-۱۰۰۰۰ برای بیشترین تعداد گزارش‌های ذخیره شده انتخاب می‌گردد.
Color Code	انتخاب رنگ مورد استفاده جهت شناسایی بر روی تقویم انتخاب می‌گردد. انتخاب کد رنگ از لیست جهت برنامه ریزی گزارش می‌باشد.

سفارشی سازی صفحات کاور گزارش

صفحه کاور گزارش فقط دربرگیرنده گزارش است. زمانی که از طریق تب Settings در Advanced Settings فعال می‌گردد.

وقتی این گزینه را فعال می‌کنید، صفحه کاور شخصی سازی می‌گردد تا توصیف کننده اطلاعاتی در زمینه گزارش باشد.

سفارشی‌سازی صفحه کاور گزارش:

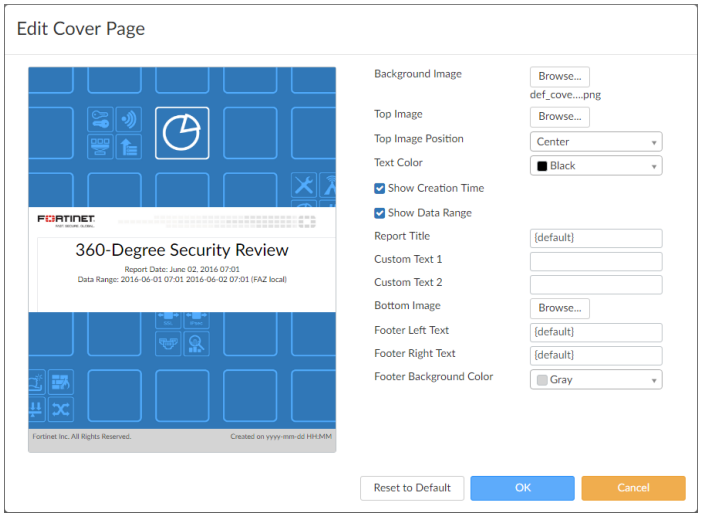
۱. اگر از ADOMها استفاده می‌نمایید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در پنجره موجود، از لیست گزارش را انتخاب نمایید و درنوار ابزار بر روی Edit کلیک کنید.

٤. تب Settings را انتخاب و سپس بر روی Advanced Settings کلیک کنید.

٥. تیک گزینه Print Cover Page را بزنید، سپس بر روی Customize کلیک کرده و بعد از آن پنجره Edit Cover Page باز می‌شود.



٦. تنظیمات زیر را پیکربندی کنید:

Background Image	**بر روی Browse کلیک کرده تا قسمت Choose an Image باز شود. تصویری را انتخاب کرده یا با کلیک بر روی Upload File تصویری را جستجو کنید سپس با کلیک بر روی OK تصویر را بعنوان پس زمینه به صفحه کاور اضافه نمایید.**
Top Image	**با کلیک بر روی Browse صفحه مربوط به choose an image باز می‌شود. عکسی را انتخاب کرده و یا بر روی Upload File کلیک نمایید تا یک عکس انتخاب شود سپس بر روی OK کلیک کنید تا عکس به بالای صفحه کاور اضافه شود.**

Top Image Position	**موقعیت عکس بالای صفحه از منو انتخاب می‌شود. یکی از گزینه‌های Left،Center و Right را انتخاب نمایید.**
Text Color	**از لیست رنگ نوشته را مشخص نمایید.**
Show Creation Time	**تاریخ چاپ گزارش بر روی کاور را مشخص نمایید.**
Show Data Range	**محدوده داده‌های چاپ شده در گزارش را بر روی کاور مشخص نمایید.**
Report Title	**عنوان پیش‌فرض را پذیرفته یا عنوان دیگری در فیلد Report Title انتخاب نمایید.**
Custom Text 1	**اگر علاقمند هستید تا متن دلخواهی داشته باشید فیلد Custom Text 1 را پر کنید.**
Custom Text 1	**اگر علاقمند هستید تا متن دلخواهی داشته باشید فیلد Custom Text 2 را پر کنید.**
Bottom Image	بر روی Browse کلیک نمایید تا صفحه Choose an Image باز شود. عکسی را برای بارگزاری انتخاب نمایید. سپس OK کرده تا عکس به بالای صفحه کاور منتقل شود.
Footer Left Text	برای چاپ کردن متن دلخواه در فوتر سمت چپ آن را وارد نمایید.
Footer Right Text	برای چاپ کردن متن دلخواه در فوتر سمت راست آن را وارد نمایید.
Footer Background Color	از لیست رنگ پس زمینه صفحه فوتر را انتخاب نمایید.
Reset to Default	با انتخاب این گزینه تنظیمات صفحه کاور به حالت پیش فرض بازمی‌گردد.

۷. برای ذخیره کردن تغییرات بر روی OK کلیک کرده و به تب Settings باز گردید.

گزارش‌های تب Layout

گزینه‌های زیر را می‌توانید در تب Layout مشاهده نمایید:

فیلد	توضیحات
Insert Chart or Edit Chart	برای وارد کردن جدول فورتی آنالایزر بر روی این گزینه کلیک نمایید. جداول با مجموعه داده‌هایی که از لاگ‌ها برای گزارشگیری خارج شده‌اند در ارتباط هستند. امکان ویرایش یک جدول بوسیله راست کلیک بر روی آن وجود دارد.
Insert Macro	ماکروها با دیتاست‌ها ارتباط دارند.
Image	با کلیک بر روی دکمه **Image** در نوار ابزار می‌توانید عکسی را در داخل **Layout** گزارش وارد نمایید. با راست کلیک بر روی یک عکس می‌توانید مشخصات عکس را ویرایش نمایید.
Table	اگر در **Layout** گزارش نیاز به جدول دارید می‌توانید با راست کلیک بر روی آن یک سلول یا ردیف یا ستون را ویرایش نمایید.
Insert Horizontal Line	جهت وارد کردن یک خط افقی بر روی این گزینه کلیک کنید.
Insert Page Break for Printing	وارد کردن یک صفحه برای پرینت گرفتن از آن بر روی این گزینه کلیک کنید.
Link	برای وارد کردن یک **URL** به یک متن یا اضافه کردن یک ایمیل آدرس می‌توانید از این گزینه استفاده نمایید.
Anchor	از طریق این گزینه می‌توانید یک **anchor** به طرح گزارش وارد نمایید.

Cut	برش یک قسمت از متن هنگامی که بخشی از آن را انتخاب می‌کنیم.
Copy	هنگامی که بخشی از متن را انتخاب می‌کنیم با استفاده از این قسمت می‌توانیم آن را را کپی نماییم.
Paste	چسباندن بخشی از متن توسط این بخش صورت می‌پذیرد.
Paste from Word	فرمت اصلی حفظ می‌شود. وقتی شما متنی را از **word** مایکروسافت **paste** می‌کنید فرمت آن حفظ می‌شود.
Undo	با استفاده از این دکمه به آخرین وضعیت بازمی‌گردید. از سوی دیگر با استفاده از دکمه‌های ترکیبی **CTRL+Z** می‌توانید این کار را انجام دهید.
Redo	با کلیک بر روی این دکمه به آخرین عمل انجام شده می‌روید. دکمه‌های ترکیبی **CTRL+Y** این کار را برای شما انجام می‌دهد.
Find	این قسمت شامل موارد زیر می‌باشد: • **Find What**: فیلدی است که کلمات یا عباراتی که درنظر داریم جستجو کنیم در آن وارد می‌کنیم. • **Match Case**: بررسی می‌کند که کلمات از لحاظ املایی و یا حروف بزرگ و کوچک مطابقت دارند یا خیر • **Match Whole word**: عملیات جستجو را به وجود تمام کلمه وارد شده محدود می‌کند. • **Match cycle**: هنگامی که ادیتور به انتهای داکیومنت رسید جستجو از ابتدای متن مجددا

ادامه پیدا کند. این آپشن به صورت پیش فرض مورد بررسی قرار می‌گیرد.	
این بخش شامل گزینه‌های زیر می‌باشد: • **Find What**: در فیلد تکست وقتی کلمه یا عبارتی را وارد می‌نمایید در نظر دارید تا آن را پیدا کنید. • **Replace With**: کلمه یا متنی که در فیلد متنی پیدا کرده‌اید جایگزین کلمه یا عبارتی می‌شود که در داکیومنت یافت شده است. • **Match Case**: عملیات جستجو را محدود می‌کند به کلمه‌ای که دیکته آنها با فیلد جستجو تطابق دارند. بدین معنی که جستجو به حروف بزرگ و کوچک حساس است. • **Match Whole word**: عملیات جستجو به کلمات کلیدی محدود می‌شود. • **Match cyclic**: بعد از رسیدن ادیتور به انتهای داکیومنت، جستجو ادامه پیدا کرده و از ابتدای متن این گزینه به صورت پیش فرض فعال است.	Replace
انتخاب این گزینه باعث می‌شود طرح همانند یک **template** ذخیره گردد.	Save as Template
از لیست فرمت پاراگراف را انتخاب می‌نمایید.	Paragraph Format
از لیست نام فونت انتخاب می‌گردد.	Font Name
از لیست سایز فونت را انتخاب می‌کنید.	Font Size
بولد بودن فونت انتخاب می‌گردد.	Bold

Italic	ایتالیک بودن فونت‌ها مشخص می‌گردد.
Underline	فونت در حالت زیرخط باشد.

فیلترکردن خروجی گزارش ها:

امکان فیلتر پیام‌های لاگ برای گزارشگیری وجود دارد. با تنظیم فیلترهای گزارش در یکی از قسمت‌های زیر:

- تب Settings بخش Filters
- تب Layout بخش Filters در کادر محاوره‌ای Insert Chart یا Chart Properties. برای باز کردن این صفحه بر روی Insert Chart یا Edit Chart کلیک کنید.

در بخش Filters، گزینه‌های زیر موجود می‌باشند.

فیلد	توضیحات
Log messages that match	فقط در تب **Settings** موجود می‌باشد. انتخاب **All** ، لاگ‌ها را بر اساس تمام حالت‌های اضافه شده فیلتر می‌نماید و انتخاب **any** لاگ‌ها را بر اساس تمام شرایط فیلتر می‌کند.
Add Filter	با کلیک بر روی این گزینه برای هر فیلتر، فیلد را انتخاب و عملگر را از لیست برمی‌گزینیم، سپس مقادیر مورد نیاز را وارد می‌کنیم.
LDAP Query	فقط در تب **Settings** موجود می‌باشد. با کلیک بر روی آن یک **LDAP** کوئری اضافه می‌شود و سپس **LDAP** سرور را انتخاب می‌کنیم.

مدیریت گزارش ها

با مراجعه به مسیر زیر امکان مدیریت گزارش‌ها برای شما فراهم گردیده است.

Reports> Report Definitions> All Reports

بعضی از گزینه‌ها به صورت دکمه بر روی نوار ابزار موجود می‌باشند. بعضی هم به صورت کلیک راست کار می‌کنند. بر روی یک گزارش راست کلیک کرده تا منو نمایش داده شود.

گزینه ها	توضیحات
Create New	**یک گزارش جدید ایجاد نمایید.**
Edit	**گزارش انتخاب شده را ویرایش کنید.**
Delete	**گزارش انتخاب شده را پاک کنید.**
Clone	**از گزارش انتخاب شده کلون بگیرید.**
Run report	**گزارشی را ایجاد نمایید.**
Folder	**سازمان‌دهی گزارش‌ها در داخل یک فولدر**
Import	**وارد کردن گزارش از کامپیوتر**
Export	**از یک گزارش به کامپیوتر گزارش بگیرید.**
Show Scheduled Only	**فیلترکردن لیستی که شامل گزارش‌هایی می‌شوند که بر اساس زمانبندی در حال اجرا می‌باشند.**

سازمان‌دهی گزارش‌ها در فولدرها

امکان ساخت و ایجاد پوشه‌ها جهت سازمان‌دهی گزارشات وجود دارد.

گزارش‌ها را در فولدرها سازمان‌دهی کنید:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در نوار ابزار بر روی Folder کلیک کنید و گزینه Create New Folder را انتخاب نمایید.

٤. یک نام و مکانی را برای فولدر در نظر بگیرید و بر روی OK کلیک کنید. حالا در لیست گزارش‌ها فولدر دیده می‌شود.

در این فولدر امکان ساخت، کلون گرفتن و وارد کردن گزارش‌ها وجود دارد.

وارد و خارج کردن گزارش ها:

امکان جابجا کردن گزارش‌ها بین دستگاه‌های مختلف فورتی آنالایزر وجود دارد. گزارشی را از دستگاه خروجی گرفته و در کامپیوتر خود ذخیره نمایید همان طور که مشاهده می‌کنید فایل با پسوند dat. ذخیره می‌شود. امکان وارد کردن این گزارش به دستگاه فورتی آنالایزر دیگر وجود دارد.

خروجی گرفتن از گزارش ها:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در پنجره content، گزارشی را انتخاب کنید یا از نوار ابزار More> Export را انتخاب نمایید تا فایل را در کامپیوتر ذخیره کنید.

وارد کردن گزارش‌ها:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> All Reports بروید.

۳. در پنجره باز شده، از نوار ابزار بر روی More> Import کلیک کنید. کادر محاوره‌ای Import Report باز می‌شود.

٤. فایل گزارش را در داخل کادر محاوره‌ای باز شده بیندازید(درگ و دراپ کنید) یا بر روی Browse کلیک کرده و مسیری که فایل در درون کامپیوتر شما می‌باشد را مشخص نمایید.

۵. یک فولدر انتخاب نمایید تا گزارش‌ها در درون آن ذخیره شود.

٦. بر روی OK کلیک کنید تا گزارش‌ها وارد شوند.

قالب گزارشی

بدلیل اینکه عملگرهای cut،copy،paste عملگرهایی هستند که نیاز به دسترسی کلیپ بورد دارند بعضی از مرورگرهای اینترنتی آنها را بلاک می‌کنند به همین دلیل قبل از بلاک از شما پرسیده می‌شود که آیا این موارد مورد نیاز است؟ حتما با موارد پیشنهادی موافقت کنید تا بتوانید از این عملگرها استفاده نمایید.

یک قالب گزارشی تعریف کننده کاراکترها و ماکروهایی است که در ریپورت وجود دارد.

امکان استفاده از آیتم‌های زیر جهت ساخت یک قالب گزارشی وجود دارد:

- تکست
- عکس
- جدول
- جداولی که به دیتاست بازگشت داده می‌شود.
- ماکروهایی که به دیتاست بازگشت داده می‌شود.

دیتاست‌ها برای جداول و ماکروهایی مشخص می‌شوند که هنگامی گزارشی ایجاد می‌شود این دیتا برای لاگ‌های تحلیلی مورد استفاده قرار بگیرد. امکان ساخت جداول و ماکروهای دلخواه برای قالب‌های گزارشی مورد استفاده وجود دارد.

ساخت قالب‌های گزارشی:

با ذخیره کردن یک گزارش به صورت یک تمپلیت گزارشی یا کلا با ساخت یک تمپلیت جدید می‌توانید قالب‌های گزارشی ایجاد نمایید.

ایجاد یک قالب گزارشی:

۱. اگر از ADOMها استفاده می‌نمایید مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> Templates بروید.

۳. در نوار ابزار بر روی Create New کلیک نمایید.

٤. گزینه‌های زیر را تنظیم نمایید:

a. نام

b. توضیحات

c. دسته‌بندی

۵. از نوار ابزار برای وارد کردن، فرمت تکست‌ها و گرافیک‌های تمپلیت استفاده می‌کنیم. به خصوص، استفاده از Insert Chart و Insert Macro برای وارد کردن جداول و ماکروها در قالب کاربرد دارد.

٦. بر روی OK کلیک نمایید.

حالا قالب جدید در لیست نمایش داده می‌شود.

ایجاد یک قالب جدید با استفاده از ذخیره‌سازی یک گزارش:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر زیر بروید

Reports> Report Definitions> All Reports

۳. در پنجره باز شده، گزارش را از لیست انتخاب نمایید و از نوار ابزار بر روی Edit کلیک کنید.

٤. در تب Layout، از نوار ابزار بر روی دکمه Save As Template کلیک کنید.

۵. در کادر محاوره‌ای Save as Template، گزینه‌های زیر را تنظیم و سپس بر روی OK کلیک کنید.

a. نام

b. توضیحات

c. گروه‌بندی

قالب جدید در لیست قالب‌ها نمایش داده می‌شود.

مشاهده گزارش‌های نمونه‌ای برای قالب‌های گزارشی از قبل تعریف شده

برای مشاهده گزارش‌های نمونه:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Report> Report Definitions> Templates بروید.

۳. در پنجره باز شده بر روی لینک HTML یا PDF کلیک کرده تا نمونه قالب را مشاهده کنید.

مدیریت قالب‌های گزارشی

این امکان وجود دارد تا تمپلیت‌های گزارشی را از طریق آدرس Reports> Report Definitions> Templates مدیریت نمایید. بعضی از گزینه‌ها به صورت دکمه بر روی نوار ابزار وجود دارند. بعضی دیگر با راست کلیک بر روی منو فعال می‌شوند.

گزینه ها	توضیحات
Create New	**قالبی برای گزارش ایجاد می‌شود.**
Edit	**ویرایش قالب گزارشی، توسط این گزینه امکان ویرایش قالب‌های گزارشی وجود دارد. قالب‌های گزارشی از قبل ایجاد شده امکان ویرایش ندارند.**
View	**نمایش تنظیمات قالب‌های گزارشی که از قبل تعریف شده‌اند. امکان کپی کردن المان‌ها از گزارش به کلیپ بورد وجود دارد.**
Delete	**قالب‌های گزارشی انتخاب شده پاک می‌شوند. امکان پاک کردن گزارش‌های از قبل تعریف شده وجود ندارد.**
Clone	**از قالب گزارشی انتخاب شده کلون گرفته می‌شود.**
Rename	**قالب گزارشی انتخاب شده را تغییر نام می‌دهیم.**

لیست قالب‌های گزارشی

هنگامی که گزارش جدیدی ایجاد می‌کنید فورتی آنالایزر شامل قالب‌های گزارشی می‌باشد که می‌توانید از آنها استفاده نمایید. فورتی آنالایزر برای دستگاه‌های مجزا قالب‌های جدایی ایجاد می‌کند.

قالب‌های گزارشی از مسیر زیر قابل دسترس می‌باشند:

Reports> Report Definitions> Templates

Chart Library

از کتابخانه جداول برای ایجاد، ویرایش و مدیریت جداول استفاده می‌کنیم.

ایجاد کردن جداول

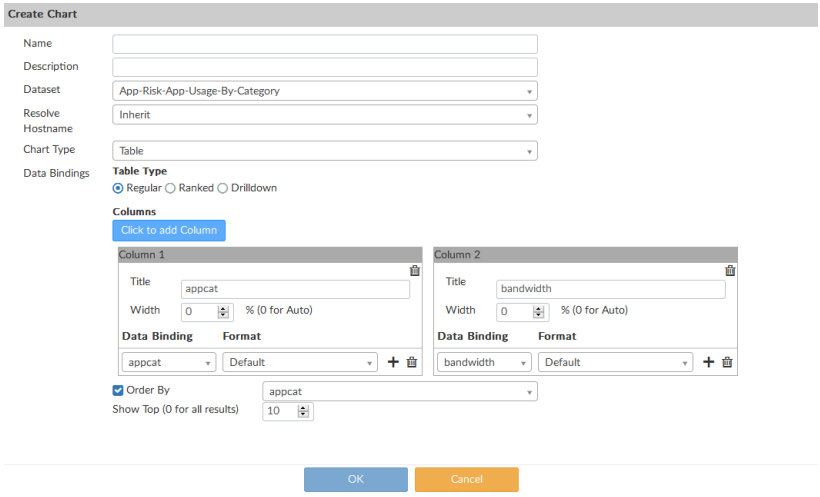
جداول را با استفاده از Log View Chart Builder می‌توانید ایجاد نمایید.

ایجاد جداول:

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> Chart Library بروید.

۳. از نوار ابزار بر روی Create New کلیک نمایید.



٤. تنظیمات جدول جدید را انجام دهید. جدول زیر در مورد هر کدام از تنظیمات توضیحاتی می‌دهد.

Name	**برای جدول نامی را انتخاب نمایید.**
Description	**برای جدول توضیحی وارد نمایید.**
Dataset	**یک دیتاست از لیست انتخاب نمایید. این گزینه به تنظیمات بر اساس نوع دستگاه بستگی دارد.**
Resolve Hostname	**یکی از گزینه‌های Inherit، Enabled، Disabled انتخاب نمایید.**

Chart Type	انتخاب نوع گراف از لیست: جدول، میله‌ای، دایره‌ای، خطی و ... این انتخاب بقیه موارد را تحت تاثیر قرار می‌دهد.
Data Binding	نوع نمودار انتخاب شده به نوع دیتا وابستگی زیادی دارد.
Table	
Table Type	انتخاب حالت‌های: **Regular, Ranked, Drilldown**
Add Column	انتخاب یا اضافه کردن یک ستون برای جدول معمولی تا ۱۵ ستون امکان پذیر است. جداول **Ranked** سه ستون دارند. جداول **Drilldown** سه ستون دارند.
Columns	تنظیمات ستون باید به صورت زیر انجام پذیرد: • **Column Title**: تیتری برای ستون وارد نمایید. • **Width**: وارد کردن عرض ستون به صورت درصدی. • **Data Binding**: انتخاب مقدار از لیست. گزینه‌های متفاوت بستگی به انتخاب **Dataset** دارند. • **Format**: مقداری از لیست انتخاب شود. • **Add Data Binding**: اضافه کردن داده‌ها به ستون. هر ستون حداقل باید یک دیتا را شامل

شود. بالاترین مقدار متفاوت به نوع جدول بستگی دارد.	
آنچه باید سفارش داده شود را انتخاب نمایید.	Order By
وارد کردن مقدار عددی فقط اولین آیتم نمایش داده می‌شود. سایر آیتم‌ها به بقیه موارد متصل می‌شود.	Show Top
یک مقدار عددی وارد نمایید. فقط آیتم اولیه نمایش داده می‌شود. این گزینه فقط برای جداول **Drilldown** وجود دارد.	Drilldown Top

مدیریت نمودارها

امکان مدیریت نمودارها از آدرس Reports> Report Definitions> Chart Library فراهم می‌شود. بعضی از گزینه‌ها به صورت دکمه بر روی نوار ابزار موجود می‌باشند و بعضی دیگر از طریق کلیک راست بر روی منو موجود هستند. با راست کلیک بر روی نمودار نمایش داده می‌شود.

توضیحات	گزینه ها
یک نمودار جدید ایجاد می‌کنید.	Create New
ویرایش چارت، چارت‌های ایجاد شده را ویرایش می‌کنید. امکان ویرایش چارت‌های از قبل تعریف شده وجود ندارد.	Edit
تنظیمات مربوط به چارت‌های از قبل تعریف شده نمایش داده می‌شود. امکان ویرایش یک چارت از قبل تعریف شده وجود ندارد.	View
چارت‌های انتخابی حذف می‌شوند. امکان حذف چارت از قبل تعریف شده وجود ندارد.	Delete
از چارت انتخاب شده کلون گرفته می‌شود.	Clone

Import	یک چارت از دستگاه دیگر وارد نمایید.
Export	از چارت‌های فورتی آنالایزر خروجی گرفته می‌شود.
Show Predefined	چارت‌های از قبل تعریف شده نمایش داده می‌شوند.
Show Custom	نمایش نمودارهای دلخواه انجام می‌شود.
Search	جستجو بر اساس نام نمودار صورت می‌پذیرد.

نمایش مجموعه داده‌های مرتبط با نمودارها

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Report Definitions> Chart Library بروید.

۳. نموداری را انتخاب کرده و از نوار ابزار بر روی View کلیک نمایید.

٤. در پنجره View Chart، نام مرتبط با دیتاست را پیدا کرده و در فیلد Dataset وارد نمایید.

٥. به مسیر Reports> Report Definitions> Datasets بروید.

٦. در قسمت Search box، نامی را برای دیتاست تایپ نمایید.

۷. دیتاست یافته شده را انتخاب کرده و از نوار ابزار بر روی View کلیک کنید تا نمایش داده شود.

کتابخانه ماکرو

از کتابخانه ماکرو برای ایجاد، ویرایش و مدیریت ماکروها استفاده می‌شود.

ساخت و ایجاد ماکروها

فورتی آنالایزر شامل تعدادی ماکرو از قبل ایجاد شده می‌باشد. امکان ساخت ماکروهای جدید وجود دارد. همچنین می‌توانید از ماکروها کلون گرفته و آن دسته که وجود دارند را ویرایش نمایید.

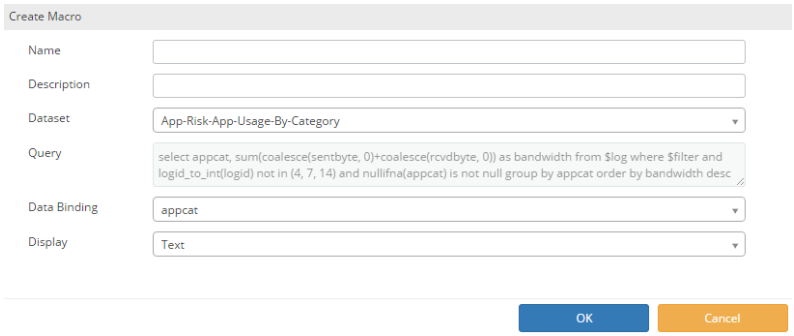
ماکروهای از قبل تعریف شده برای دیتاست‌های مشخص استفاده می‌شوند.

در حال حاضر ماکروها در فورتی‌گیت و فقط ADOMهای فورتی carrier پشتیبانی می‌شوند.

ماکروی جدیدی ایجاد نمایید:

۱. اگر از ADOM استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Report Definitions> Macro Library بروید و بر روی Create New کلیک کنید. پنجره Create Macro نمایش داده می‌شود.



۳. اطلاعات مورد نیاز برای ساخت ماکرو جدید به شرح زیر می‌باشد.

Name	برای ماکرو یک نام وارد نمایید.
Description	توضیحاتی برای ماکرو وارد نمایید.
Dataset	از لیست دیتاستی را انتخاب نمایید. این گزینه به نوع دستگاه مرتبط است.
Query	نمایش وضعیت کوئری برای دیتاست انتخابی می‌باشد.
Data Binding	دیتاست‌ها بسته به نوع انتخاب داده متفاوت می‌باشند.
Display	انتخاب مقدار از لیست

٤. بر روی OK کلیک کنید. ماکرو جدید در لیست ماکروهای موجود نمایش داده می‌شود.

مدیریت ماکروها

امکان مدیریت ماکروها از طریق آدرس Reports> Report Definitions> Macro Library وجود دارد.

گزینه	توضیحات
Create New	ماکرو جدید ایجاد نمایید.
Edit	ماکروی انتخابی را ویرایش نمایید. ماکرویی که ساخته شده است امکان ویرایش را دارا می‌باشد اما ماکروهایی که از قبل وجود داشته‌اند ویرایش نمی‌شوند.
View	تنظیمات ماکرو انتخاب شده نمایش داده می‌شود. ماکرو از قبل تعریف شده امکان ویرایش ندارد.
Delete	ماکرو انتخاب شده حذف می‌گردد.
Clone	از ماکروهای انتخاب شده کلون گرفته می‌شود.
Show Predefined	ماکروهای از قبل تعریف شده نمایش داده می‌شوند.
Show Custom	ماکروهای دلخواه نمایش داده می‌شوند.
Search	اجازه جستجوی ماکروها از طریق نام داده می‌شود.

مشاهده دیتاست‌های مربوط به ماکروها

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Report> Reports Definitions> Macro بروید.

۳. یک ماکرو انتخاب نمایید. بر روی View کلیک کنید. می‌توانید ماکرو را ویرایش کنید.

٤. در صفحه View Macro یا Edit Macro، نامی که مرتبط با دیتاست می‌باشد را جستجو نمایید.

۵. به مسیر Reports> Report Definitions> Dataset بروید.

٦. در قسمت Search یک نام برای دیتاست مورد جستجو وارد نمایید.

۷. بر روی دیتاست دابل کلیک کرده تا آن را مشاهده کنید.

دیتاسِت ها

از صفحه دیتاست‌ها برای ایجاد، ویرایش و مدیریت مربوط به آنها استفاده می‌شود.

ساخت دیتاست ها

دیتاست‌ها در فورتی آنالایزر دیتاها را از لاگها جمع آوری می‌کنند و این امر سبب مانیتورینگ راحت آنها می‌شود. نمودارها و ماکروها به دیتاست‌ها ارجاع داده می‌شوند.

ایجاد دیتاست جدید:

۱. اگر از ADOMها استفاده می‌کنید مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Report Definitions> Dataset بروید و بر روی Create New کلیک کنید. پنجره Create Dataset نمایش داده می‌شود.

۳. برای ایجاد دیتاست جدید اطلاعات درخواستی را وارد نمایید.

Name	**یک نام برای دیتاست وارد نمایید.**
Log Type	**نوع لاگ را از لیست انتخاب کنید.**
Query	**کوئری SQL که برای دیتاست استفاده می‌کنید را وارد نمایید.**
Variables	**برای اضافه کردن متغییر بر روی دکمه Add کنید.**
آزمودن کوئری‌ها با دستگاه‌های دلخواه در بازه‌های زمانی مختلف	
Time Period	**از لیست استفاده نمایید تا یک بازه زمانی مشخص کنید. وقتی custom انتخاب می‌شود زمان و تاریخ شروع را وارد و سپس تاریخ و زمان خاتمه را مشخص نمایید.**
Devices	**دستگاه‌های مورد نظر خود را انتخاب کنید تا کوئری مربوط به SQL مجددا اجرا شود. با کلیک بر روی select device امکان اضافه کردن چندین و چند دستگاه وجود دارد.**

قبل از ذخیره کردن تنظیمات دیتاست می‌توانید کوئری‌های SQL را تست نمایید.	Test

٤. بر روی Test کلیک نمایید.

نتیجه کوئری برای شما نمایش داده می‌شود. اگر نتیجه ناموفق باشد یک پیغام خطا ظاهر می‌شود.

٥. بر روی OK کلیک نمایید.

مشاهده پرس و جوی SQL برای موجود بودن دیتاست

١. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

٢. به مسیر Reports> Report Definitions> Datasets بروید.

٣. نشانگر موس را بر روی لیست دیتاست قرار دهید. وضعیت کوئری SQL برای شما نمایش داده می‌شود. همچنین امکان باز کردن دیتاست و مشاهده فیلد Query وجود دارد.

مدیریت دیتاست ها

با مراجعه به قسمت Reports> Report Definitions> Dataset امکان مدیریت دیتاست‌ها وجود دارد. بعضی از آپشن‌ها به صورت دکمه در نوار ابزار هستند و بعضی دیگر با راست کلیک کردن بر روی منو قابل دسترسی می‌باشند.

توضیحات	گزینه
یک دیتاست جدید ایجاد می‌شود.	Create New
دیتاست انتخابی ویرایش می‌شوند. امکان ویرایش دیتاست‌های از پیش تعریف شده وجود ندارد.	Edit
دیتاست انتخابی حذف می‌شود.	Delete
از دیتاست انتخاب شده کلون گرفته می‌شود.	Clone
دیتاست‌های انتخاب شده تایید می‌شوند.	Validate
دیتاست‌های سفارشی تایید می‌شوند.	Validate All Custom

Search	نام یک دیتاست را جستجو می‌کنید.

پروفایل‌های خروجی

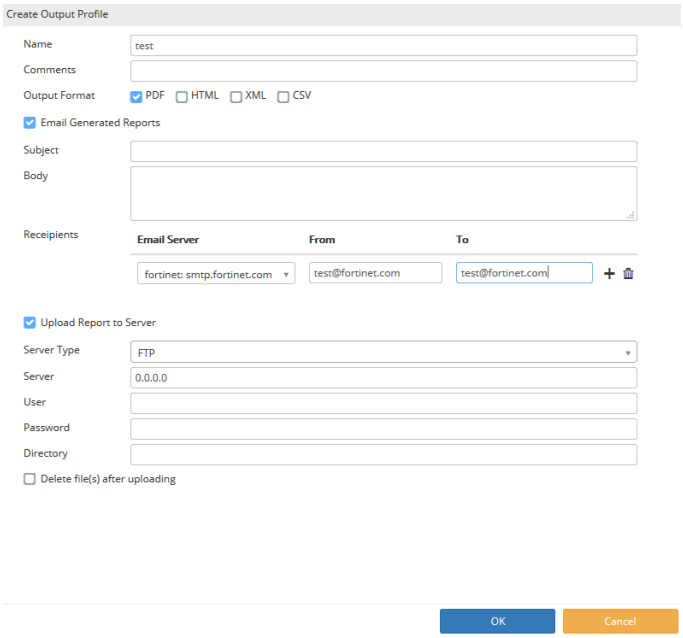
پروفایل‌های خروجی به شما این امکان را می‌دهد تا آدرس‌های ایمیل را تعریف کرده و گزارش‌های تولید شده را ارسال نمایید. هنگامی که ایجاد شد، یک پروفایل خروجی می‌تواند برای یک گزارش مشخص شود.

ساخت پروفایل‌های خروجی

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Advanced> Output Profile بروید.

۳. بر روی Create New کلیک کنید. پنجره Create Output Profiles نمایش داده می‌شود.



٤. اطلاعات زیر را وارد کرده و بر روی OK کلیک کنید.

Name	یک نام انتخاب نمایید.
Comments	توضیحی در نظر بگیرید. این گزینه کاملا اختیاری می‌باشد.
Output Format	فرمت گزارش تولید شده را انتخاب نمایید.

Email Generated Reports	گزارش‌های تولید شده ایمیل شوند.
Subject	موضوعی برای گزارش ایمیل انتخاب کنید.
Body	متنی برای ایمیل مشخص نمایید.
Recipient	میل سرور را انتخاب کرده و لیست آدرس‌ها را مشخص کنید. با کلیک بر روی **Add** می‌توانید چندین گیرنده را انتخاب نمایید.
Upload Report to Server	گزارش‌های تولید شده بر روی یک سرور آپلود می‌شود.
Server Type	از لیست **FTP**،**SFTP**، **SCP** انتخاب می‌گردد.
Server	**IP** آدرس سرور را وارد نمایید.
User	نام کاربری را وارد نمایید.
Password	کلمه عبور را وارد نمایید.
Directory	فولدری که قرار است گزارش‌ها در آن ذخیره شود را مشخص نمایید.
Delete file(s) after uploading	بعد از انتقال گزارش‌ها به سرور مشخص شده پاک می‌شوند.

مدیریت پروفایل‌های خروجی

امکان مدیریت پروفایل‌های خروجی از طریق رفتن به مسیر Reports> Advanced> Output Profiles وجود دارد.

گزینه	توضیحات
Create New	یک پروفایل خروجی جدید ایجاد کنید.
Edit	پروفایل خروجی انتخاب شده را ویرایش نمایید.
Delete	پروفایل خروجی انتخاب شده را حذف کنید.

زبان‌های گزارش

هنگامی که در نظر دارید گزارشی را ایجاد کنید می‌توانید زبان را انتخاب نمایید. امکان اضافه کردن زبان‌های جدید به همراه نام و توضیحات مربوط به زبان را تغییر دهید. امکان ویرایش زبان‌های از قبل تعریف شده وجود ندارد.

زبان‌های گزارش از پیش تعریف شده

فورتی آنالایزر شامل زبان‌های از پیش تعریف شده زیر می‌باشد:

- انگلیسی
- فرانسوی
- ژاپنی
- کره ای
- پرتغالی
- چینی
- اسپانیایی

متغییرهای زبانی را اضافه نمایید

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درست قرار دارید.

۲. به مسیر Reports> Advanced> Language بروید.

۳. از نوار ابزار بر روی Create New کلیک کنید.

٤. در پنجره New Language یک نام و توضیحی برای زبان وارد و سپس OK کنید.

یک متغییر زبانی جدید ایجاد می‌گردد.

مدیریت زبان‌های گزارش

با مراجعه به مسیر Reports> Advanced> Language امکان مدیریت زبان گزارش‌ها برای شما وجود دارد.

توضیحات	گزینه
گزارش متغییر زبانی را ایجاد نمایید.	Create New
جزئیات مربوط به زبان گزارش را مشاهده نمایید.	View
زبان گزارش انتخاب شده را ویرایش نمایید.	Edit
زبان گزارش انتخاب شده را حذف کنید.	Delete

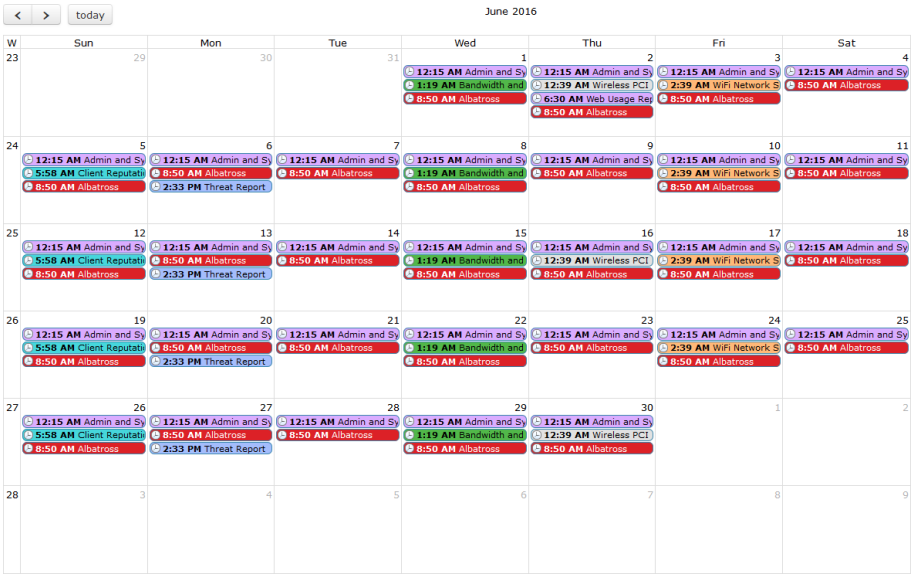
گزارش تقویم

از این نوع گزارش در جهت مشاهده تمام گزارش‌هایی که زمانبندی شده‌اند می‌توانید استفاده نمایید. در این مدل گزارش امکان ویرایش یا غیرفعال کردن برنامه‌های آینده وجود دارد. همچنین حذف و یا دانلود کامل گزارش‌ها وجود دارد.

مشاهده گزارش‌های زمانبندی شده

۱. اگر از ADOMها استفاده می‌کنید، مطمئن شوید که در ADOM درستی قرار دارید.

۲. به مسیر Reports> Advanced> Report بروید.



۳. با قرار دادن نشانگر موس بر روی تقویم نام وارد شده، وضعیت و نوع دستگاه در گزارش زمانبندی شده نمایش داده می‌شود.

٤. بر روی گزارش ایجاد شده کلیک کنید تا دانلود شود.

۵. بر روی زمانبندی گزارش کلیک و سپس به تب Settings بروید.

٦. فلش سمت چپ یا راست در بالای صفحه را کلیک کنید تا Report Calendar مشاهده گردد. برای تغییر در ماه نمایش داده شده بر روی Today کلیک کنید تا مجددا به ماه جاری بازگردید.

مدیریت زمابندی گزارش

امکان مدیریت زمانبندی گزارش از طریق آدرس Reports> Advanced> Report Calendar وجود دارد.

۱. در قسمت Report Calendar، راست کلیک کرده و گزینه Edit را انتخاب نمایید.

۲. در تب Settings از گزارش‌هایی که باز هستند گزارش برنامه ریزی مربوط را ویرایش نمایید.

غیرفعال کردن گزارش زمانبندی:

در قسمت Report Calendar، بر روی یک ورودی تقویم راست کلیک کنید و بعد گزینه Disable را انتخاب نمایید. تمام زمانبندی‌های نمونه گزارش از تقویم حذف می‌شوند و فقط گزارش تکمیل شده در تقویم باقی می‌ماند.

حذف یا دانلود یک گزارش کامل شده:

در Report Calendar، بر روی ورودی تقویم قدیمی راست کلیک کرده و سپس گزینه Delete یا Download را انتخاب نمایید.

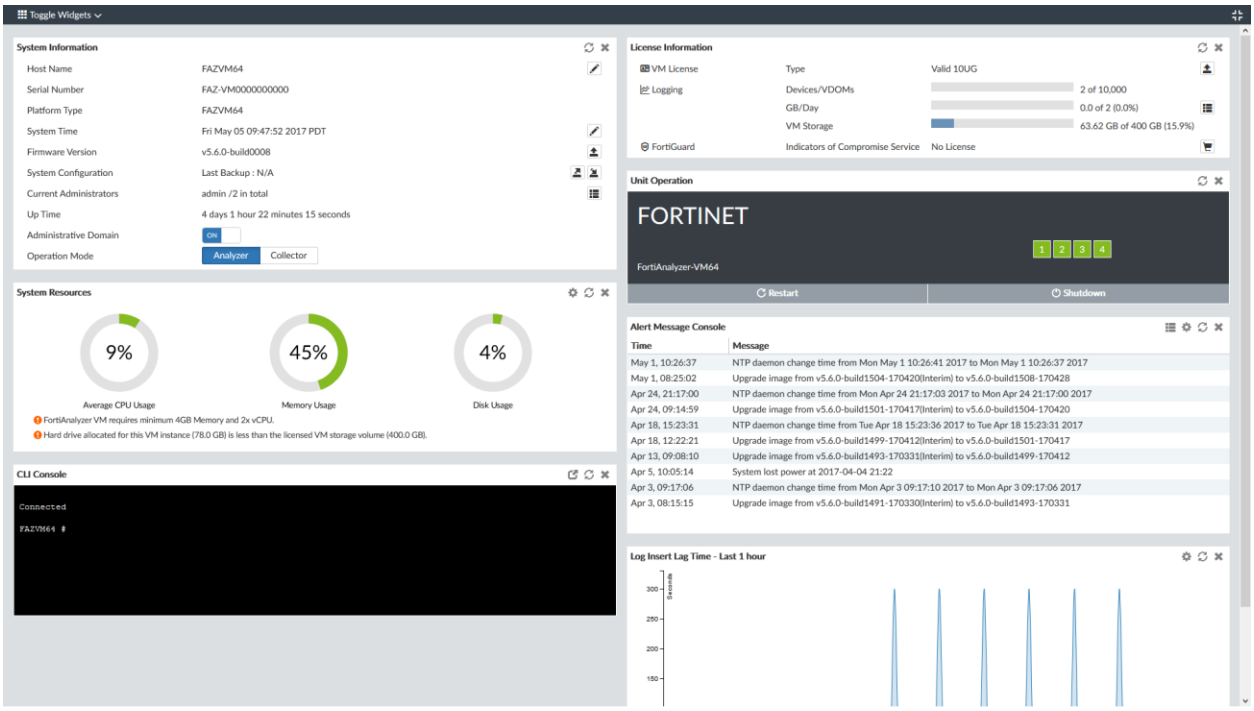
گزارش تکمیل شده متناظر پاک یا دانلود می‌شود. گزارش‌هایی که در وضعیت Finished قرار دارند امکان دانلود آنها وجود دارد. گزارش‌هایی که در وضعیت pending هستند امکان پاک کردن را نخواهند داشت.

تنظیمات سیستمی

در این قسمت امکاناتی وجود دارد که شما گزینه‌های سیستمی را برای دستگاه فورتی آنالایزر مدیریت نمایید.

داشبورد

داشبورد حاوی ویجت‌هایی است که کارایی و وضعیت کلی سیستم را نمایش می‌دهند. در این قسمت امکان انجام تنظیمات ابتدایی سیستم وجود دارد. داشبورد ویجتی با نام CLI دارد که از طریق آن می‌توانید از command line استفاده نمایید.



ویجت‌های زیر موجود می‌باشند:

ویجت	توضیحات
System Information	اطلاعات پایه‌ای سیستم نمایش داده می‌شود. مواردی مثل زمان **UP** بودن سیستم و نسخه فریمور دستگاه. امکان فعال/غیرفعال کردن دامین ادمین و تنظیم مُد عملیاتی دستگاه از این قسمت وجود دارد. از طریق این ویجت می‌توانید دستگاه را به صورت دستی بروزرسانی نمایید.
System Resources	وضعیت مصرف **CPU**،**Memory** و هارددیسک را به صورت بلادرنگ و تاریخچه‌ای نمایش داده می‌شود.
License Information	نشان دهنده بیشترین تعداد دستگاهی است که می‌توانید به فورتی آنالایزر متصل کنید. از طریق این ویجت امکان آپلود کردن دستی لایسنس برای سیستم‌های مجازی وجود دارد.

Unit Operation	وضعیت پورت‌های متصل شده به دستگاه فورتی آنالایزر نمایش داده می‌شود. همچنین امکان خاموش کردن یا ریستارت کردن دستگاه فورتی آنالایزر وجود دارد.
CLI Console	پنجره ترمینال باز شده و به شما اجازه داده می‌شود تا دستگاه را پیکربندی نمایید. امکان انجام تنظیمات به صورت مستقیم از طریق محیط **CLI** بر روی دستگاه وجود دارد.
Alert Message Console	پیام‌های هشدار برای دستگاه‌های متصل به فورتی آنالایزر را نمایش می‌دهد.
Log Receive Monitor	لاگ‌های دریافتی بدون وقفه قابل مشاهده می‌باشند. امکان مشاهده دیتا بر اساس دستگاه یا بر اساس نوع لاگ وجود دارد.
Insert Rate vs Receive Rate	نمایش دهنده لاگ‌های وارد شده و نرخ دریافت آنها می‌باشد. وقتی فورتی آنالایزر در حالت کالکتور مُد است این قابلیت مخفی می‌باشد. در حالت دیتابیس **SQL** این قابلیت غیرفعال می‌باشد.
Log Insert Lag Time	برای پردازش لاگ‌ها دیتابیس چند ثانیه درگیر است. وقتی فورتی آنالایزر در حالت کالکتور است این گزینه مخفی بوده و در حالت دیتابیس **SQL** این قسمت غیرفعال است.
Receive Rate vs Forwarding Rate	وقتی لاگ فوروارد تنظیم می‌شود فورتی آنالایزر با چه سرعتی لاگ‌ها را دریافت می‌کند. این ویجت نمایش دهنده نرخ ارسال لاگ‌ها به سرور تنظیم شده می‌باشد.

Disk I/O	**میزان استفاده دیسک نمایش داده می‌شود. نرخ جابجایی یا خروج دیتا بر اساس درصد بر زمان می‌باشد.**

شخصی سازی داشبورد

داشبورد سیستمی فورتی آنالایزر امکان شخصی سازی را داشته و شما به راحتی می‌توانید مشخص نمایید که کدام یک از ویجت‌ها نمایش داده شود و در کدام قسمت از صفحه قرار گیرد و سایز یک ویجت چه اندازه‌ای باشد. با انتخاب دکمه Full Screen می‌توانید به صورت تمام صفحه وضعیت را نمایش دهید.

مراحل	اقدام
جابجایی ویجت‌ها بوسیله کلیک و درگ کردن آنها از نوار ابزار امکان پذیر است.	Move a Widget
انتخاب toggle widget از نوار ابزار و بعد ویجتی که نیاز دارید را انتخاب نمایید.	Add a Widget
از title بار بر روی آیکون close کلیک نمایید.	Delete a widget
برای ویجت‌هایی با آیکون ویرایش امکان دلخواه‌سازی وجود دارد.	Customize a widget
از نوار ابزار گزینه Reset Default را انتخاب می‌کنیم. داشبورد به حالت تنظیمات پیش فرض باز می‌گردد.	Reset the dashboard

ویجت اطلاعات سیستم

ویجت System information اطلاعات مربوط به سیستم را نمایش می‌دهد و وابسته به مدل فورتی آنالایزر و تنظیمات دستگاه می‌باشد.

Hostname	**شناسایی نامی که به دستگاه فورتی آنالایزر تخصیص داده شده است. با کلیک بر روی نام هاست می‌توانید اسم آن را تغییر بدهید.**

Serial Number	شماره سریال دستگاه فورتی آنالایزر است. سریال نامبر برای هر دستگاه بی‌همتا (بی‌مانند) بوده و با تغییر و یا بروزرسانی فریمور تغییری نمی‌کند. سریال نامبر برای شناسایی دستگاه هنگام اتصال به سرورهای فورتی گارد مورد استفاده قرار می‌گیرد.
Platform Type	نمایش دهنده پلتفرم فورتی آنالایزر می‌باشد.
System Time	زمان کنونی دستگاه بر اساس ساعت داخلی می‌باشد. بر روی دکمه تغییر ساعت کلیک نمایید.
Firmware version	شامل شماره نسخه و بیلد نامبر فریمور نصب شده بر روی دستگاه می‌باشد. برای آپدیت فریمور باید آخرین نسخه را از سرویس پشتیبانی دانلود نمایید.
System Configuration	تاریخ آخرین بکاپ سیستم می‌باشد. با کلیک بر روی دکمه **backup** از تنظیمات سیستمی در قالب یک فایل نسخه پشتیبان تهیه می‌گردد. با کلیک بر روی دکمه **restore** فایل تنظیمات بر روی سیستم بازگردانده می‌شود. امکان جابجایی تنظیمات بر روی مدل دیگری از فورتی آنالایزر با استفاده از **CLI** وجود دارد.
Current Administration	ادمین‌هایی که به دستگاه متصل هستند نمایش داده می‌شوند. با کلیک بر روی **Session** کنونی جزئیات تمام لاگ‌ها مشخص می‌گردد.
Up Time	مدت زمانی که از آخرین روشن شدن یا ریستارت شدن دستگاه فورتی آنالایزر میگذرد.
Administrative Domain	فعال بودن **ADOM**ها برای شما نمایش داده می‌شود.

Operation Mode	**حالت عملیات فعلی فورتی آنالایزر را نمایش می‌دهد. برای تغییر کافی است مُد دیگری را انتخاب نمایید.**

تغییر نام هاست

نام دستگاه در قسمت‌های مختلفی مورد استفاده قرار می‌گیرد.

- نام دستگاه در ویجت System Information بر روی داشبورد ظاهر می‌شود.
- در CLI سیستم مورد استفاده قرار می‌گیرد.
- در نام SNMP سیستم مورد استفاده قرار می‌گیرد.

در محیط CLI اگر دستور get system status را تایپ نمایید نام کامل دستگاه برای شما نمایان می‌شود. هرچند، اگر نام بیشتر از ١٦ کاراکتر باشد در محیط CLI و یا سایر قسمت‌ها به صورت خلاصه شده نشان داده می‌شود. نام بدین صورت نمایش داده می‌شود که از انتها با یک تیلدا مشخص می‌شود.

تغییر دادن نام هاست:

١. به مسیر System Settings> Dashboard بروید.

٢. در ویجت System Information، بر روی دکمه ویرایش نام هاست کلیک نمایید تا فیلد Host Name نمایش داده شود.

٣. در قسمت Host Name نام جدید هاست را تایپ نمایید.

نام جدید هاست می‌تواند تا ٣٥ کاراکتر طول داشته باشد و در برگیرنده US-ASCII، اعداد، زیرخط ها، فاصله‌ها باشد. اجازه استفاده از کاراکترهای خاص و فاصله‌ها را ندارید.

٤. برای تغییر نام هاست بر روی چک مارک کلیک نمایید.

تنظیمات زمان سیستم

امکان تنظیمات زمان سیستم به صورت خودکار یا دستی وجود دارد. تنظیمات خودکار از طریق شبکه و با استفاده از پروتکل NTP صورت می‌پذیرد. برای امکانات کاربردی دستگاه مثل زمابندی ها، لاگ‌ها، SSL و .. حتما باید زمان سیستم دقیق باشد.

تنظیمات زمان و تاریخ:

۱. به مسیر Dashboard> System Settings بروید.

۲. در ویجت System Information بر روی دکمه ویرایش Time کلیک کرده و وارد قسمت System Time شوید.

۳. پیکربندی تنظیمات زیر به صورت دستی یا همگام با دستگاه فورتی آنالایزر از طریق NTP سرور انجام می‌شود.

System Time	تاریخ و ساعت دستگاه بر اساس زمانی که در ساعت سیستم وارد شده است نمایش داده می‌شود.
Time Zone	**منطقه زمانی مشخص می‌گردد.**
Update Time By	**انتخاب Set time تا به صورت دستی زمان تنظیم شود یا همگام سازی با NTP سرور صورت پذیرد.**
Set Time	**تاریخ و ساعت به صورت دستی تنظیم می‌گردد.**
Select Date	**تنظیم تاریخ از تقویم یا به صورت دستی در فرمت YYYY/MM/DD انجام می‌شود.**
Select Time	**زمان را انتخاب نمایید.**
Synchronize with NTP Server	**به صورت خودکار همگام سازی تاریخ و ساعت انجام پذیرد.**
Sync Interval	**چند بار در دقیقه همگام سازی با سرور NTP صورت پذیرد.**
Server	**آدرس IP یا نام دامین NTP سرور را وارد نمایید. با کلیک بر روی دکمه + سرورهای بیشتری اضافه می‌شوند.**

٤. بر روی تیک Apply کلیک کنید تا تغییرات ذخیره شوند.

بروزرسانی فریمور سیستم

برای در اختیار داشتن آخرین امکانات به همراه کمترین مشکلات فریمور فورتی آنالایزر خود را بروزرسانی نمایید.

از تنظیمات و دیتابیس خود قبل از تغییرات نسخه پشتیبان تهیه نمایید. تغییر فریمور به نسخه‌های قدیمی یا ناسازگار ممکن است سبب ریست تنظیمات و بازگشت دیتابیس به حالت پیش فرض شود. این کار سبب از بین رفتن دیتاها خواهد شد.

بروزرسانی فریمور

۱. فریمور را که پسوندی به اسم .out دارد از customer service فورتی دانلود نمایید.

۲. به مسیر System Settings> Dashboard بروید.

۳. در ویجت System Information در فیلد Firmware Version بر روی Upgrade Firmware کلیک کنید پنجره Firmware Upload باز می‌شود.

٤. فایل را داخل پنجره باز شده درگ کرده یا با استفاده از دکمه Browse آن را انتخاب نمایید.

۵. بر روی OK کلیک کنید. بر روی دستگاه شما ایمیج فریمور آپلود می‌شود و پیام تاییدی مبنی بر موفقیت آمیز بودن بروزرسانی دریافت خواهید کرد.

به صورت دلخواه می‌توانید پروسه آپدیت فریمور را از طریق TFTP و یا FTP از طریق دستورات زیر انجام دهید:

```
execute restore image {ftp | tftp} <file path to server> <IP ofserver> <username on server> <password>
```

٦. مرورگر را ریفرش کرده و مجددا به دستگاه لاگین کنید.

۷. ماژول Device Manager را اجرا کنید و مطمئن شوید که تمام سوابق اضافه شده به دستگاه در لیست موجود باشد.

۸. سایر قابلیت‌های دستگاه را اجرا کرده و مطمئن شوید همه چیز به درستی کار می‌کند.

تهیه نسخه پشتیبان از سیستم

فورتی به ادمین‌ها توصیه اکید می‌کند که از دستگاه فورتی آنالایزر به صورت منظم بکاپ تهیه کرده و فایل‌های بکاپ را بر روی کامپیوتر خود نگهداری کنند.این کار سبب می‌شود زمانی که دستگاه با مشکل مواجه می‌شود در سریعترین زمان ممکن آن را به حالت قبلی بازگردانده و کمترین تاثیر را بر روی شبکه داشته باشد. قبل از انجام هرتغییری از تنظیمات فورتی آنالایزر بکاپ تهیه نمایید. قبل از بروزرسانی فریمور دستگاه حتما از تنظیمات نسخه پشتیبان تهیه نمایید.

تهیه نسخه پشتیبان از تنظیمات دستگاه

۱. به مسیر System Settings> Dashboard بروید.

۲. در ویجت system information، بر روی دکمه بکاپ کلیک کنید. دیالوگ باکس Backup System باز می‌شود.

۳. اگر می‌خواهید بکاپ‌هایی که تهیه می‌کنید رمزنگاری شود بخش Encryption را تیک بزنید سپس کلمه عبور را تایپ نمایید. توجه داشته باشید که حداکثر کلمه عبور می‌تواند ٦٣ کاراکتر باشد.

٤. با انتخاب دکمه OK بکاپ بر روی کامپیوتر شما قرار می‌گیرد.

بازیابی تنظیمات

برای بازیابی تنظیمات دستگاه فورتی آنالایزر می‌توانید از دستور العمل زیر استفاده نمایید:

۱. به مسیر System Settings> Dashboard بروید.

۲. در ویجت System Information بر روی دکمه restore کلیک نمایید پنجره Restore System باز می‌شود.

۳. تنظیمات زیر را انجام داده و OK کنید. از طریق دکمه Browse می‌توانید بکاپ فایلی را که قصد بازیابی دارید انتخاب نمایید. اگر برای فایل پسوردی انتخاب کردید آن را تایپ نمایید. تیک مربوط به بازنویسی IP کنونی را بزنید و تنظیمات را بازیابی کنید.

جابجایی تنظیمات

امکان جالبی که در فورتی آنالایزر وجود دارد این است که شما می‌توانید از یک مدل فورتی آنالایزر بکاپ گرفته و سپس با استفاده از CLI و FTP، SCP و یا SFTP تنظیمات را به سایر مدل‌های فورتی آنالایزر جابجا کنید. اگر در هنگام

بکاپ‌گیری از تنظیمات کلمه عبور انتخاب کرده‌اید برای منتقل کردن تنظیمات به سایر دستگاه‌ها باید کلمه عبور را وارد نمایید.

جابجایی تنظیمات فورتی آنالایزر

۱. در یک مدل از فورتی آنالایزر به مسیر System Settings> Dashboard بروید.

۲. از سیستم بکاپ بگیرید.

۳. در سایر مدل‌های فورتی آنالایزر به مسیر System Settings> Dashboard بروید.

٤. در ویجت کنسول CLI، دستور زیر را وارد نمایید:

```
execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user><password>[cryptpasswd]
```

تنظیمات حالت کاربری

فورتی آنالایزر در دو حالت عملیاتی فعالیت می‌کند: ۱. آنالایزر ۲. حالت کالکتور

وقتی در حالت کالکتور کار می‌کنید دیتابیس SQL به صورت پیش فرض غیرفعال است.

تغییر حالت کاربری

۱. به مسیر System Settings> Dashboard بروید.

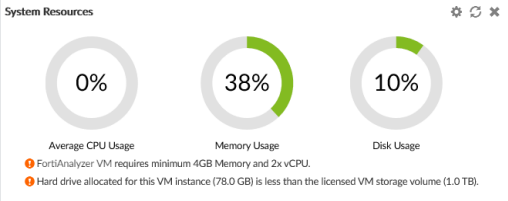
۲. در ویجت System Information از فیلد Operation Mode قسمت Analyzer یا Collector را انتخاب نمایید.

۳. بعد از انجام تغییرات در حالت کاربری بر روی دکمه OK کلیک کنید تا موارد اعمال گردد.

ویجت منابع سیستمی

ویجت منابع سیستمی نمایش دهنده وضعیت استفاده از CPU ها، مموری و هارددیسک می‌باشد. اطلاعات منابع سیستمی به صورت لحظه‌ای یا به صورت تاریخچه‌ای قابل مشاهده می‌باشد. امکان مشاهده میانگین یا مصرف CPU به صورت تک و انحصاری هم وجود دارد.

در VM ها، اگر تعداد CPUهای تخصیص داده شده و یا مموری در نظر گرفته شده و یا فضای هارد دیسک درنظر گرفته خیلی پایین باشد پیام‌های اخطاری نمایش داده می‌شود. این پیام‌ها در لیست اعلان‌ها نیز نمایان می‌شود.

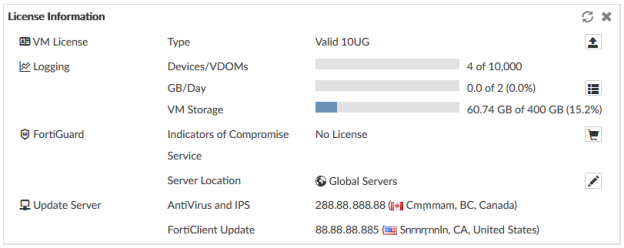


در تغییر وضعیت از حالت لحظه‌ای به دیتاهای تاریخچه‌ای (قدیمی)، از ویجت نوار ابزار بر روی Edit کلیک نمایید. Historical یا Real-time را انتخاب کنید، سایر گزینه‌های مورد نیاز را ویرایش کرده و سپس بر روی OK کلیک کنید.

برای مشاهده مصرف CPU به صورت اختصاصی از نمایش Real-Time بر روی نمودار CPU کلیک نمایید. برای بازگشت به نمای استاندارد مجددا بر روی نمودار کلیک کنید.

ویجت اطلاعات لایسنس

ویجت اطلاعات لایسنس نمایش دهنده تعداد دستگاه‌های متصل شده به فورتی آنالایزر می‌باشد.



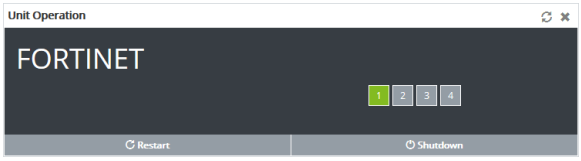
VM License	اطلاعات و وضعیت لایسنس VM نمایش داده می‌شود.
Logging	
Device/VDOM	**تعداد کل دستگاه‌ها و VDOMهایی که لایسنس داشته و به فورتی منیجر متصل شده‌اند نمایش داده می‌شود.**
GB/Day	**لاگ‌هایی که بر اساس گیگابایت بر روز باقی می‌ماند و مورد استفاده فورتی آنالایزر قرار می‌گیرند. با کلیک بر روی details می‌توانید لاگ‌های مورد استفاده در ٦ روز اخیر را مشاهده نمایید.**

VM Storage	مقدار فضای **VM** که مورد استفاده قرار گرفته یا باقی مانده است. این فیلد فقط برای **VM** فورتی آنالایزر موجود است.
VM Storage	مقدار فضای **VM** که استفاده شده یا باقی مانده است. این فیلد فقط برای **VM** فورتی آنالایزر موجود است.
FortiGuard	
Indicators of Compromise Service	وضعیت لایسنس‌ها وقتی در نظر دارید تا لایسنسی را خریداری کنید با کلیک بر روی دکمه **purchase** می‌توانید به قسمت **Customer service & support** فورتی‌نت متصل شوید.
Secure DNS Server	وضعیت لایسنس **SDNS** سرور نمایش داده می‌شود. یک لایسنس را می‌توانید بارگذاری کنید.
Server Location	مکان سرورهای فورتی گارد، به صورت کلی یا فقط **US** را مشخص می‌کنید. با کلیک بر روی **edit** می‌توانید موقعیت مکانی را ویرایش نمایید. تغییر دادن موقعیت مکانی سبب ریستارت شدن فورتی آنالایزر می‌شود.
Update Server	
Antivirus and IPS	**IP** آدرس و موقعیت فیزیکی آپدیت سرورهای **IPS** و **Antivirus** مشخص می‌شود.
FortiClient Update	**IP** آدرس و موقعیت فیزیکی سرور بروز رسان **FortiClient** مشخص می‌شود.

ویجت عملیاتی

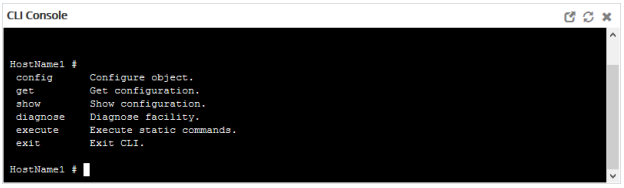
این ویجت به صورت گرافیکی وضعیت هر پورت را نمایش می‌دهد. نام پورت و وضعیت پورت با استفاده از رنگ مشخص می‌گردد. نشانگر سبز یعنی پورت متصل است. نمایشگر خاکستری یعنی پورت متصل نیست.

با قرار دادن کرسر موس بر روی پورت، پاپ آپی نمایش داده می‌شود که نام کامل اینترفیس می‌باشد.IP آدرس، Netmask، وضعیت لینک، سرعت اینترفیس و مقدار دیتای دریافت/ ارسال در همین قسمت نمایش داده می‌شود.



ویجت کنسول CLI

با کمک این ویجت می‌توانید در محیط گرافیکی از CLI استفاده نمایید و همین امر سبب می‌شود نیازی به telnet و یا SSH وجود نداشته باشد. ویجت CLI Console زمانی در مرورگر شما اجرا می‌شود که مرورگر از جاوا اسکیریپت پشتیبانی کند. وقتی از ویجت CLI استفاده می‌کنید در اصل با دسترسی ادمین در محیط گرافیکی لاگین می‌کنید. با تایپ کردن دستورات آنها را اجرا کرده یا می‌توانید دستورات را copy و paste کنید.



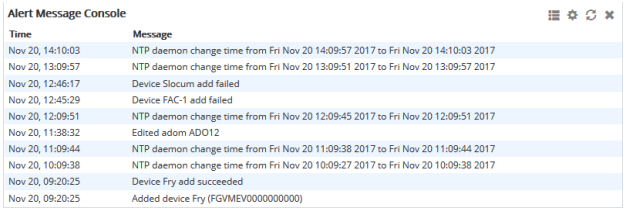
با کلیک بر روی Detach در ویجت نوار ابزار می‌توانید یک پنجره مجزا باز کنید.

پیام‌های اخطار ویجت کنسول

ویجت کنسولِ Alert Message بر اساس لاگ‌های دریافتی پیام‌های اخطار مربوط به فورتی آنالایزر و دستگاه‌های متصل به آن را نمایش می‌دهد.

پیام‌های اخطار کمک شایانی در پیدا کردن رخدادهای سیستمی بر روی دستگاه شما می‌کند. این رخدادها می‌تواند تغییرات در فریمور و اتفاقات شبکه‌ای مثل شناسایی حملات باشد. هر پیام نشانگر تاریخ و زمان رخداد می‌باشد.

پیام‌های اخطاری توسط ایمیل، syslog و یا SNMP قابل دریافت هستند.



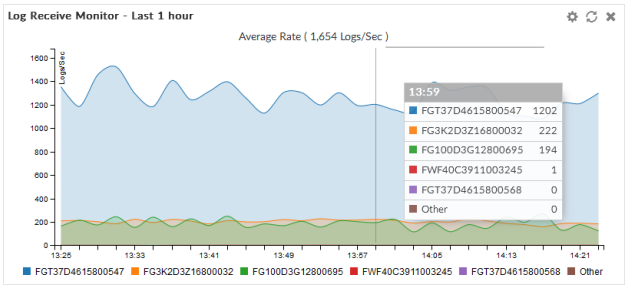
از نوار ابزار ویجت بر روی Edit کلیک کنید تا Alert Message Console Settings را مشاهده کنید، تعداد ورودی‌های ویجت و فاصله ریفرش را مشخص نمایید.

برای مشاهده لیست کامل پیام‌های اخطار، بر روی Show More کلیک کنید. ویجتی از لیست به صورت کامل نمایش داده می‌شود. برای پاک کردن لیست بر روی Delete All Message کلیک نمایید. با کلیک بر روی Show Less به حالت قبلی بازمی‌گردید.

ویجت مانیتور لاگ دریافتی

ویجت Log Receive Monitor میزان دریافت لاگ در زمان مشخص توسط فورتی آنالایزر را نمایش می‌دهد. لاگ دیتا بوسیله نوع لاگ یا دستگاه نمایش داده می‌شود.

وقتی موس را بر روی نقطه‌های روی گراف نگه میدارید تعداد دقیق لاگ‌های دریافت شده در زمان مشخص نمایش داده می‌شود. با کلیک بر روی نام دستگاه یا نوع لاگ می‌توانید آنها را از گراف اضافه یا حذف نمایید.

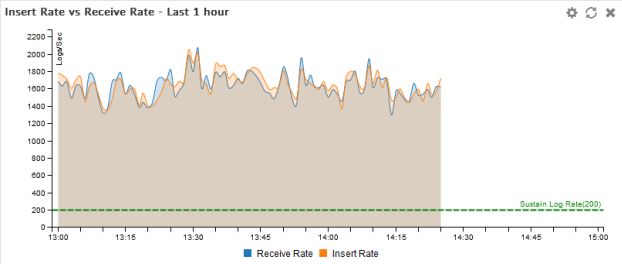


ویجت مقایسه‌ای بین نرخ درج با نرخ دریافت

- Log Receive rate: چه مقدار لاگ دریافت می‌شود.
- Log insert rate: چه مقدار لاگ به صورت اکتیو در دیتابیس درج می‌شود.

اگر نرخ درج لاگ خیلی بالاتر از نرخ دریافت لاگ باشد، دیتابیس در حال بازسازی است. تاخیر تعداد لاگ‌ها سبب انتظار برای درج دیتا می‌شود.

مکان نما را بر روی یک نقطه از نمودار قرار بدهید تا عدد دقیق لاگ‌های دریافتی و درج شده را در یک زمان مشخص مشاهده نمایید. با کلیک بر روی Receive Rate یا Insert Rate دیتاهای آنها از گراف پاک می‌شود. با کلیک بر روی Edit می‌توانید فاصله‌های زمانی نشان داده شده در گراف را تنظیم نمایید.

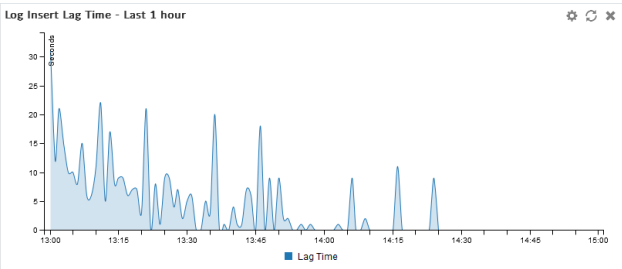


در شرایطی که دستگاه در حالت کالکتور فعال شده و دیتابیسSQL غیرفعال است این قابلیت پنهان می‌باشد.

ویجت تاخیر زمانی درج لاگ

ویجت Log Insert Lag Time نمایش دهنده مقدار زمانی است که دیتابیس لاگ‌ها را پردازش می‌کند.

با کلیک بر روی آیکون Edit در نوار ابزار ویجت تنظیم فاصله زمانی نشان داده شده است.

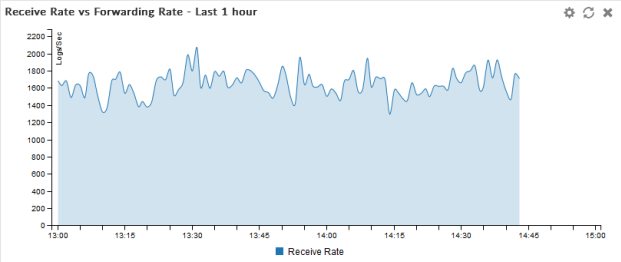


در شرایطی که دستگاه در حالت کالکتور فعال شده و دیتابیسSQL غیرفعال است این قابلیت پنهان می‌باشد.

ویجت مقایسه نرخ دریافت و ارسال

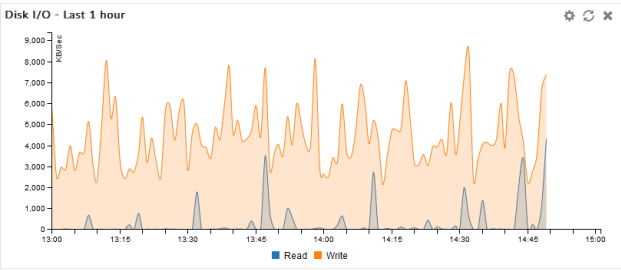
ویجت Receive Rate vs Forwarding Rate سرعتی که در آن فورتی آنالایزر لاگ‌ها را دریافت می‌کند نمایش داده می‌شود. وقتی log forwarding تنظیم می‌شود، ویجت سرعت ارسال لاگ برای هر سروری که تنظیم شده را نشان می‌دهد.

با کلیک بر روی آیکون ویرایش در ویجت نوار ابزار می‌توانید دوره زمانی را مشخص نمایید.



ویجت I/O دیسک

این ویجت نمایش دهنده میزان مصرف دیسک بر اساس درصد، سرعت تراکنش ها(درخواست/ ثانیه) یا میزان توان عملیاتی(درخواست ها/ ثانیه) است. در نوار ابزار ویجت بر روی آیکون ویرایش کلیک کرده تا چارت نمایش داده شده انتخاب شود حال دوره زمانی و فاصله ریفرش را مشخص کنید.

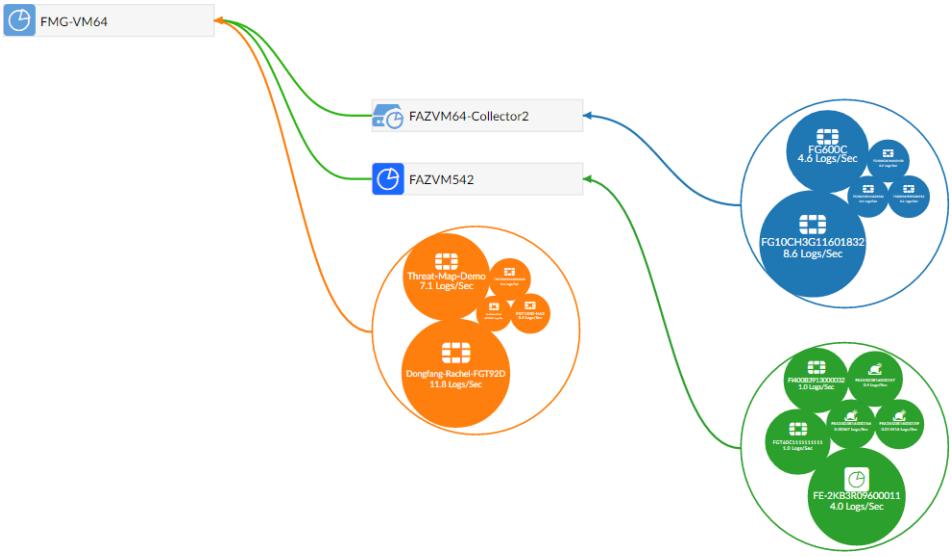


توپولوژی لاگین

پنجره Logging Topology توپولوژی دستگاه‌ها در حالت security Fabric را نشان می‌دهد. با کلیک کردن، نگه داشتن یا درگ کردن می‌توانید محتویات این قسمت را تنظیم نمایید. همچنین می‌توانید با دابل کلیک یا اسکرول کردن اندازه زوم صفحه را تغییر دهید.

الگوی بصری نمایش داده شده می‌تواند برای نمایش فقط دستگاه‌های فورتی آنالایزر یا تمام دستگاه‌های موجود در شبکه یا فقط ترافیک عبوری مورد استفاده قرار گیرد.

با نگه داشتن مکان نما بر روی یک دستگاه می‌توانید اطلاعاتی در مورد دستگاه بدست آورید. این اطلاعات شامل IP آدرس‌ها، نام دستگاه و یا با راست کلیک کردن بر روی دستگاه و انتخاب گزینه View Related Log به صفحه Log View بروید.



صادر کردن گواهی Certificate

فورتی آنالایزر گواهینامه امنیتی را بر اساس اطلاعات وارد شده شما ایجاد می‌نماید. بعد از ایجاد گواهینامه درخواستی آن را بر روی کامپیوتر خود دانلود کرده و سپس به CA سرور ارسال می‌نماید.

گواهینامه‌های داخلی برای سرورهای خاصی صادر می‌شوند و اغلب برای یک شبکه داخلی پیشرفته مورد استفاده قرار می‌گیرند.

روت CA سرتیفیکیت‌ها خیلی شبیه به Certificateهای داخلی می‌باشند هرچند به محدوده وسیع‌تری از سیستم‌ها اعمال می‌شوند.

CRL شامل لیستی است از سرتیفیکیت‌هایی است که لغو شده و مدت زمان زیادی است که مورد استفاده قرار نمی‌گیرند. این لیست شامل سرتیفیکت‌هایی است که منقضی شده ، دزدیده شده و ... می‌باشد. اگر گواهینامه صادر شده شما در این لیست باشد امکان استفاده از آن وجود ندارد. CRL توسط CA نگهداری می‌شود که سرتیفیکیت را صادر می‌کند و دربرگیرنده تاریخ و زمان می‌باشد. همچنین دنباله‌ای از اعداد که اطمینان حاصل شود شما آخرین نسخه را دارید.

گواهینامه داخلی Local Certificate

فورتی آنالایزر یک certificate درخواستی بر پایه اطلاعاتی وارد شده جهت شناسایی دستگاه ایجاد می‌کند. بعد از اینکه سرتیفیکیت درخواستی را ایجاد کردید، آن را دانلود کرده و سپس برای CA ارسال نمایید.

همچنین قسمت Certificate این امکان را برای شما فراهم می‌کند تا سرتیفیکیت‌ها را export و یا Import کرده و مشاهده نمایید.

فورتی آنالایزر یک سرتیفیکت داخلی پیش فرض با نام Fortinet_Local دارد.

امکان مدیریت سرتیفیکت‌های داخلی از طریق System Settings> Certificates> Local Certificates وجود دارد. بعضی از گزینه‌ها در نوار ابزار موجود می‌باشند و بعضی دیگر با راست کلیک بر روی منو قابل دستیابی هستند.

ساخت Local Certificate

۱. به مسیر System Settings> Certificated> Local Certificates بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید. پنجره Generate Certificate Signing Request باز می‌شود.

۳. اطلاعات را بر اساس نوع درخواست پر کرده و بر روی OK کلیک نمایید.

Certificate Name	نام سرتیفیکیت
Subject Information	**مدل ID را از لیست انتخاب نمایید:** • **Host IP: اگر دستگاه IP آدرس ثابت دارد انتخاب نمایید. اگر IP پابلیک دارد انتخاب نمایید.** • **Domain Name: اگر دستگاه یک IP آدرس داینامیک دارد و سرویس DDNS را دنبال می‌نماید در این قسمت انتخاب نمایید. در فیلد Domain Name نام دامنه را وارد نمایید.** • **Email: آدرس ایمیلی را مشخص نمایید. در فیلد ایمیل آدرس آن را وارد کنید.**
Optional Information	
Organization Unit	**نام دپارتمان را وارد نمایید. امکان وارد کردن OUها نهایتا ۵ سری وجود دارد. برای اضافه یا حذف کردن OUها کافیست بر روی + یا – کلیک کنید.**

Organization	نام قانونی کمپانی یا سازمان را وارد نمایید.
Locality	نام شهر یا شهرکی که دستگاه در آنجا قرار دارد.
State/Province	نام استانی که دستگاه در آنجا قرار دارد.
Country	انتخاب کشوری که دستگاه در آنجا نصب شده است.
Email Address	ایمیل آدرس ارتباطی را وارد نمایید.
Subject Alternative Name	برای زمانی که سرتیفیکیت معتبر است یک یا چند جایگزین وارد نمایید. نام‌ها را بوسیله کاما از یکدیگر تفکیک کنید. یک نام می‌تواند: • E-mail address • IP address • URI • DNS name • Directory name
Key Type	نوع کلید می‌تواند به صورت **RSA** یا **Elliptic Curve** باشد.
Key Size	از منو اندازه کلید را مشخص نمایید. این گزینه تنها در شرایطی فعال است که نوع کلید در حالت **RSA** قرار گرفته باشد.
Curve Name	نام **Curve** را از لیست انتخاب نمایید. این گزینه تنها در شرایطی فعال است که مدل کلید در حالت **Elliptic Curve** قرار داشته باشد.
Enrollment Method	روش ثبت نام اولیه بر اساس فایل تنظیم شده است.

سرتیفیکیت داخلی را وارد نمایید

وارد کردن سرتیفیکیت داخلی:

۱. به مسیر System Settings> Certificates> Local Certificates بروید.

۲. بر روی Import کلیک کنید. کادر محاوره مربوط به Import باز می‌شود.

۳. اطلاعات درخواست شده را بر اساس توضیحات جدول تکمیل نمایید.

Type	**از لیست نوع سرتیفیکیت را مشخص نمایید:** **Local Certificate, PKCS #12 Certificate, Certificate.**
Certificate File	**بر روی Browse کلیک کنید. محل قرارگیری سرتیفیکیت بر روی کامپیوتر خود را مشخص نمایید. همچنین می‌توانید فایل را در داخل کادر محاوره‌ای باز شده درگ و دراپ نمایید.**
Key File	**بر روی Browse... کلیک کنید و key فایل را از روی کامپیوتر خود آدرس دهی نمایید یا در کادر محاوره‌ای درگ، دراپ نمایید.**
Password	**کلمه عبور مربوط به سرتیفیکیت را وارد نمایید. این گزینه فقط در شرایطی موجود است که مدل سرتیفیکیت PKCS#12 باشد.**
Certificate Name	**نام سرتیفیکیت را وارد کنید. این گزینه فقط در شرایطی موجود است که مدل سرتیفیکیت PKCS#12 باشد.**

حذف سرتیفیکیت داخلی

حذف کردن سرتیفیکیت داخلی:

۱. به مسیر System Settings> Certificates> Local Certificates بروید.

۲. سرتیفیکیت/ سرتیفیکیت‌هایی که تصمیم به حذف آنها را دارید انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک کنید یا با راست کلیک کردن گزینه Delete را انتخاب نمایید.

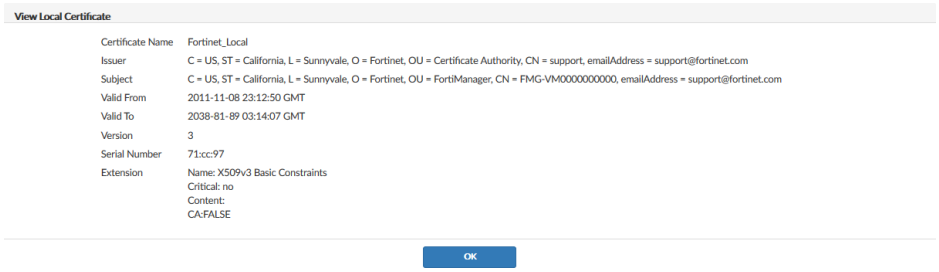
٤. بر روی OK در کادر تایید کلیک کرده تا سرتیفیکیت‌های انتخابی حذف گردد.

جزئیات سرتیفیکیت‌های داخلی را مشاهده نمایید

مشاهده جزئیات سرتیفیکیت‌های داخلی:

۱. به مسیر System Settings> Certificates> Local Certificates بروید.

۲. سرتیفیکیت‌هایی که درنظر دارید جزئیات آنها را مشاهده نمایید انتخاب و از نوار ابزار گزینه View Certificate Detail را بزنید.



۳. با زدن دکمه OK به قسمت لیست سرتیفیکت‌ها بازمی‌گردید.

دانلود سرتیفیکیت‌های داخلی

سیرتیفیکیت داخلی را دانلود نمایید:

۱. به مسیر System Settings> Certificates> Local Certificates بروید.

۲. سرتیفیکیتی که قصد دانلود آن را دارید انتخاب نمایید.

۳. از نوار ابزار بر روی Download کلیک و سرتیفیکیت را بر روی کامپیوتر خود ذخیره نمایید.

CA Certificate

فورتی آنالایزر CA certificate پیش فرضی با نام Fortinet_CA دارد. در این زیرمنو می‌توانید عملیات حذف کردن، وارد کردن، مشاهده کردن و دانلود کردن سرتیفیکیت را انجام دهید.

وارد کردن CA سرتیفیکیت

CA سرتیفیکیت را وارد نمایید:

۱. به مسیر System Settings> Certificates> CA Certificates بروید.

۲. از نوار ابزار بر روی Import کلیک کنید. کادر محاوره‌ای Import باز می‌شود.

۳. بر روی Browse... کلیک و فایل سرتیفیکیت را از داخل کامپیوتر خود مشخص و یا از طریق درگ و دراپ داخل کادر محاوره‌ای وارد نمایید.

٤. با کلیک بر روی OK سرتیفیکیت را وارد کنید.

جزئیات CA Certificate را مشاهده نمایید

جزئیات CA Certificate را مشاهده نمایید:

۱. به مسیر System Settings> Certificates> CA Certificates بروید.

۲. سرتیفیکیت‌هایی که تمایل دارید جزئیاتی در مورد آنها بدانید را انتخاب نمایید.

۳. از نوار ابزار View Certificate Detail را کلیک نمایید. صفحه View CA Certificate برای شما باز می‌شود.

٤. با انتخاب OK به لیست CA certificate بازمی‌گردید.

CA سرتیفیکیت‌ها را دانلود نمایید

CA سرتیفیکیت‌ها را دانلود کنید:

۱. به مسیر System Settings> Certificates> CA Certificates بروید.

۲. سرتیفیکیتی که قصد دانلود آن را دارید انتخاب نمایید.

۳. از نوار ابزار بر روی Download کلیک و سرتیفیکیت را در کامپیوتر خود ذخیره نمایید.

CA سرتیفیکیت‌ها را حذف نمایید

حذف کردن CA سرتیفیکیت ها:

۱. به مسیر System Settings> Certificates> CA Certificates بروید.

۲. سرتیفیکیت/ سرتیفیکیت‌هایی که تمایل به حذف آنها را دارید انتخاب نمایید.

۳. از نوار ابزار بر روی Delete کلیک کرده و آن را انتخاب کنید.

٤. جهت تایید بر روی OK کلیک کنید.

توجه داشته باشید که Fortinet_CA حذف نمی‌گردد.

لیست سرتیفیکیت باطل شده

هنگامی که درخواستی برای پذیرش سرتیفیکیت شخصی یا گروه برای نصب بر روی یک کلاینت داده می‌شود امکان دریافت روت سرتیفیکیت و CRL لیست فسخ سرتیفیکیت از CA صادر شده وجود دارد.

CRL لیستی است شامل سرتیفیکیت‌هایی که باطل شده و مدت زمان زیادی است که قابل استفاده نمی‌باشند. این لیست حاوی مواردی مانند منقضی شده، دزدیده شده یا سرتیفیکیت‌هایی که به هر دلیلی با مشکلاتی مواجه شده‌اند می‌باشد. اگر سرتیفیکیت شما در این لیست باشد پذیرفته نخواهد شد. CRLها توسط CAهایی نگهداری می‌شوند که سرتیفیکیت‌ها را صادر کرده‌اند. این موارد شامل زمان و تاریخ هستند. وقتی CRL بعدی صادر می‌شود یک توالی عددی به همراه خود دارد که کمک می‌کند شما مطمئن شوید بالاترین نسخه فعلی در اختیارتان است.

وارد کردن یک CRL

یک CRL را وارد نمایید:

۱. به مسیر System Settings> Certificates> CRL بروید.

۲. از نوار ابزار بر روی Import کلیک کنید. کادر محاوره‌ای Import باز می‌شود.

۳. بر روی Browse... کلیک کرده و فایل CRL را از کامپیوتر خود مسیریابی کنید یا با استفاده از درگ و دراپ به داخل کادر محاوره‌ای کار را انجام دهید.

٤. برای وارد کردن CRL بر روی OK کلیک نمایید.

مشاهده یک CRL

مشاهده کردن یک CRL:

۱. به مسیر System Settings> Certificates>CRL بروید.

۲. CRL که می‌خواهید جزئیاتی در مورد آن بدانید را انتخاب نمایید.

۳. از نوار ابزار بر روی View Certificate Detail کلیک نمایید، صفحه Result باز می‌شود.

٤. برای بازگشت به لیست CRL بر روی OK کلیک کنید.

حذف CRL

یک CRL را حذف نمایید:

۱. به مسیر System Settings> Certificates> CRL بروید.

۲. CRL یا CRLهایی که درنظر دارید حذف نمایید را انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک کنید و سپس گزینه Delete را انتخاب نمایید.

٤. جهت تایید بر روی OK کلیک کنید تا CRL یا CRLهای انتخابی حذف گردند.

ارسال لاگ

امکان ارسال لاگ‌ها از یک دستگاه فورتی آنالایزر به دستگاه فورتی آنالایزر دیگر و یا یک syslog سرور یا Common Event Format (CEF) سرور وجود دارد.

کلاینت دستگاه فورتی آنالایزر است که لاگ‌ها را به سایر دستگاه‌ها ارسال می‌کند. سرور دستگاه فورتی آنالایزر، syslog سرور یا CEF می‌باشد که لاگ‌های ارسال شده را دریافت می‌کند.

علاوه بر ارسال لاگ‌ها به سایر دستگاه‌ها، کلاینت نسخه‌ای از لاگ‌ها را برای خود نگهداری می‌کند. کپی داخلی لاگ‌ها در بحث دیتا پالیسی تنظیم می‌شود و در مورد لاگ‌های آرشیوی صدق می‌کند.

برای مشاهده یک شماتیک کلی و گرافیکی از تنظیمات لاگ‌های فورورد شده و همچنین جزئیات دستگاه به مسیر System Settings> Logging Topology بروید.

طریقه کار

دو حالت از فوروارد لاگ در فورتی آنالایزر پشتیبانی می‌شود: فوروارد به صورت پیش فرض و aggregation

فورواردینگ

لاگ‌ها به صورت لحظه‌ای یا با زمان خیلی کم دریافت می‌شوند. فایل‌های ارسال شده حاوی: DLP فایل‌ها، فایل‌های آنتی‌ویروسی که قرنطینه شده‌اند و پکت‌های کپچر شده IPS می‌باشند.

این روش می‌تواند در حالت گرافیکی و یا از طریق خط فرمان تنظیم گردد.

تجمیع

فورتی آنالایزر لاگ‌ها را از دستگاه‌ها دریافت و در زمان‌های مشخص آنها را جمع آوری می‌کند.

فورتی آنالایزر از ارسال لاگ‌ها به صورت تجمیع شده پشتیبانی می‌کند. Syslog و CEF با دستورات زیر پیکربندی می‌شوند:

log-forward

log-forward-service

پیکربندی ارسال لاگ

حالت فوروارد فقط بر روی کلاینت پیکربندی می‌گردد. نیازی به انجام تنظیمات بر روی سرور وجود ندارد. در حالت تجمیع پذیرش لاگ‌ها بر روی فورتی آنالایزر باید فعال شوند.

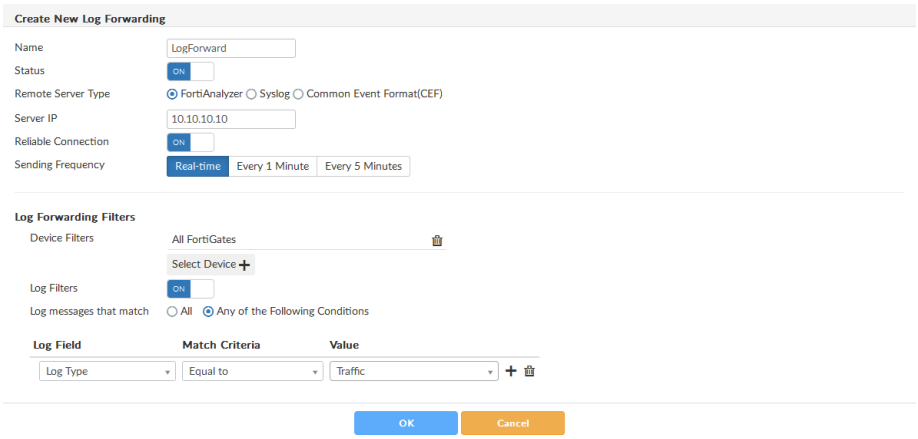
حالت ارسال

حالت ارسال می‌تواند در محیط گرافیکی تنظیم شود و نیازی به زدن دستور خاصی بر روی سرور نمی‌باشد.

انجام تنظیمات بر روی کلاینت:

۱. به مسیر System Settings> Log Forwarding بروید.

۲. بر روی نوار ابزار Create New کلیک کرده صفحه مربوط به Create New Log Forwarding باز می‌شود.



۳. اطلاعات را بر اساس توضیحات جدول زیر وارد می‌کنیم.

Name	برای سرور ریموت یک نام انتخاب می‌کنیم.
Status	با انتخاب حالت **on** ارسال لاگ را فعال کرده و با انتخاب **off** ارسال لاگ را غیرفعال می‌کنیم.
Remote Server Type	نوع سرور ریموتی که قرار است لاگ‌ها را برای آن بفرستید مشخص نمایید.
Server IP	**IP** آدرس ریموت سرور را وارد نمایید.
Server Port	شماره پورت سرور را وارد نمایید. به صورت پیش‌فرض: **514**
Reliable Connection	فعال کردن این گزینه در شرایطی که از **TCP** کانکشن استفاده می‌نمایید. غیرفعال کردن در شرایطی که از **UDP** استفاده می‌کنید. اگر لاگ‌ها را به سمت **Syslog** یا **CEF** سرور ارسال می‌کنید قبل از روشن کردن مطمئن شوید این گزینه پشتیبانی می‌شود.
Sending Frequency	زمان ارسال لاگ به سمت سرور را مشخص نمایید.
Log Forwarding Filters	
Device Filter	بر روی **Select Device** کلیک نمایید. سپس دستگاهی که قرار است لاگ آن ارسال شود را انتخاب نمایید.

Log Filter	**تنظیمات فیلتر لاگ‌هایی که ارسال می‌شوند در این قسمت صورت می‌پذیرد.**
Enable Excisions	**این گزینه فقط وقتی موجود است که سرور پاک شده یک syslog یا CEF سرور است.** **روشن کردن فیلتر تنظیمات بر روی لاگ‌هایی که فوروارد می‌شوند.**

دستگاه‌هایی که لاگ‌ها را برای دستگاه فورتی آنالایزر دیگری ارسال می‌کنند به عنوان سروری که ثبت نشده است به لیست اضافه می‌گردند.

حالت تجمیع

این حالت فقط از طریق محیط CLI امکان پیکربندی دارد. حالت تجمیع در لیست GUI وجود ندارد اما لاگ را با شماره ID ارسال می‌کند.

از دستور زیر استفاده نمایید تا مشاهده کنید لاگ‌های ارسالی از چه ID نامبرهایی استفاده می‌کنند:

```
get system log-forward
```

پیکربندی سرور:

۱. اگر لازم است، ادمین جدیدی ساخته که پروفایل Super_User دارد.

۲. قسمت log aggregation را فعال کرده و اگر لازم است quota دیسک را با استفاده از دستورات زیر پیکربندی کنید:

```
config system log-forward-service
        set accept-aggregation enable
        set aggregation-disk-quota <quota>
end
```

پیکربندی کلاینت:

۱. خط فرمان ارسال لاگ را باز نمایید:

```
        config system log-forward
```

۲. برای ساخت یا ویرایش ارسال لاگ خط زیر را وارد نمایید:

```
edit <log forwarding ID>
```

۳. حالت لاگ فوروارد را بر روی aggregation قرار دهید:

```
set mode aggregation
```

٤. نام و IP آدرس سرور را مشخص نمایید:

```
set server-name <string<
set server-ip <xxx.xxx.xxx.xxx>
```

٥. نام کاربری و کلمه عبور ادمین سرور را وارد نمایید:

```
set agg-user <string>
set agg-password <string>
```

٦. در صورت لزوم، زمان aggregation از ۰ تا ۲۳ ساعت را تنظیم نمایید.(پیش فرض: ۰)

```
set agg-time <integer>
```

۷. در انتها جهت اعمال تغییرات دستور زیر را وارد نمایید:

```
End
```

مدیریت ارسال لاگ

در حالت ارسال لاگ سرور وارد شده امکان ویرایش و حذف با استفاده از هر دو حالت گرافیکی و دستوری وجود دارد. در حالت تجمیعی سرور ورودی می‌تواند فقط با استفاده از CLI مدیریت شود. ورودی‌ها با استفاده از CLI قابلیت فعال یا غیرفعال شدن را ندارند.

فعال/غیرفعال کردن سرور ارسال لاگ:

۱. به مسیر System Settings> Log Forwarding بروید.

۲. بر روی سرور وارد شده دابل کلیک کنید، سپس راست کلیک کرده و Edit را انتخاب نمایید. پنجره Edit Log Forwarding باز می‌شود.

۳. تنظیم وضعیت در حالت Off یعنی غیرفعال کردن و تنظیم به صورت On یعنی فعال نمودن شرایط است. در حالت disable فقط نام سرور قابلیت ویرایش دارد.

٤. با کلیک بر روی Ok تغییرات اعمال می‌شود.

ویرایش سرور ارسال لاگ با استفاده از محیط CLI:

١. خط فرمان را باز کنید:

```
config system log-forward
```

٢. ورودی که از آن ID ،برای ارسال لاگ استفاده می‌کند را وارد نمایید:

```
edit <log forwarding ID>
```

٣. تنظیمات را بر اساس درخواست ویرایش کنید.

٤. برای اعمال تغییرات دستور زیر را وارد نمایید:

```
End
```

حذف سرور ارسال کننده لاگ:

١. به مسیر System Settings> Log Forwarding بروید.

٢. ورودی که درنظر دارید حذف نمایید را انتخاب کنید.

٣. از نوار ابزار بر روی Delete کلیک نمایید.

٤. با کلیک بر روی OK کادر محاوره‌ای تایید جهت حذف باز می‌شود و سرورهای انتخاب حذف می‌گردد.

مدیریت Fetcher

لاگ fetcher برای بدست آوردن مجدد لاگ‌های آرشیوی از یک فورتی آنالایزر به دیگری استفاده می‌شود. این کار به ادمین اجازه می‌دهد تا گزارش‌ها و صف‌ها را بر خلاف دیتاهای قدیمی اجرا کرده و برای تجزیه و تحلیل‌های قابل استناد و قانونی استفاده شود.

Fetching فورتی آنالایزر برای پرس و جو از سرور فورتی آنالایزر و بدست آوردن دیتا لاگ‌ها برای یک دستگاه مشخص و در دوره زمانی بر اساس متغییرهای مشخص شده مورد استفاده قرار می‌گیرد. بعد از اینکه دیتا بدست آمد، ایندکس گذاری شده و مورد استفاده قرار می‌گیرد تا تجزیه و تحلیل مناسب بر روی آن انجام گیرد.

Fetching لاگ بر روی دو دستگاه فورتی آنالایزر اجرا می‌شود که فریمورهای یکسانی دارند. یک دستگاه فورتی آنالایزر می‌تواند یک سرور و یا یک کلاینت را fetch نماید. البته توجه داشته باشید که امکان انجام هر دو رول در یک زمان توسط تمام دستگاه‌های فورتی آنالایزر متفاوت است.

مراحل اولیه برای fetch کردن لاگ‌های موجود:

۱. روی کلاینت یک fetching Profile ایجاد می‌کنیم.

۲. روی کلاینت، برای سرور درخواست fetch را ارسال می‌کنیم.

۳. اگر بار اولی است که با پروفایل انتخابی میخواهیم لاگ‌ها را fetch کنیم یا اگر هر گونه تغییری در دستگاه‌ها ایجاد شده دستگاه‌ها و ADOMها با سرور همگام می‌شوند.

٤. بر روی سرور، درخواست را مرور کرده سپس آنها را تایید یا رد کنید.

٥. پروسه Fetch کردن فورتی آنالایزر را مانیتور کنید.

٦. بر روی کلاینت، قبل از استفاده از دیتایی که fetch شده است تا زمان بازسازی دیتابیس صبر کنید.

پروفایل‌های Fetch شده

برای Fetch کردن پروفایل‌ها امکان مدیریت از تب Profiles در قسمت زیر وجود دارد:

System Settings> Fetcher Management

پروفایل‌ها امکان ایجاد، ویرایش و حذف بنا به درخواست را دارند. در لیست نام پروفایل نمایش داده می‌شود همان طور که IP آدرس سرور Fetcher موجود است.

ایجاد کردن یک پروفایل fetch جدید:

۱. بر روی کلاینت به مسیر System Settings> Fetcher Management بروید.

۲. تب Profiles را انتخاب کرده، سپس بر روی Create New کلیک کنید. سپس کادر محاوره‌ای Create New Profile برای شما باز می‌شود.

۳. تنظیمات زیر را اعمال نمایید و جهت ایجاد پروفایل OK کنید

Name	**یک نام برای پروفایل وارد نمایید.**
Server IP	**IP آدرس fetch سرور را وارد نمایید.**
User	**نام کاربری ادمینی که بر روی fetch سرور دسترسی دارد را وارد نمایید.**
Password	**کلمه عبور ادمین را وارد کنید.**

ویرایش پروفایل fetch :

۱. به مسیر System Settings> Fetching Management بروید.

۲. بر روی یک پروفایل دابل کلیک کنید، بر روی یک پروفایل راست کلیک کرده سپس Edit را انتخاب نمایید یا پروفایلی را انتخاب کرده و از نوار ابزار بر روی Edit کلیک نمایید. کادر محاوره‌ای Edit Profile باز می‌شود.

۳. تنظیمات درخواستی را ویرایش و سپس جهت اعمال تغییرات بر روی OK کلیک نمایید.

حذف پروفایلی که fetch شده است

۱. به مسیر System Settings> Fetching Management بروید.

۲. پروفایلی که می‌خواهید حذف نمایید را انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک کنید.

٤. از کادر محاوره‌ای تایید بر روی OK کلیک کنید تا پروفایل/ پروفایل‌های انتخابی حذف گردد.

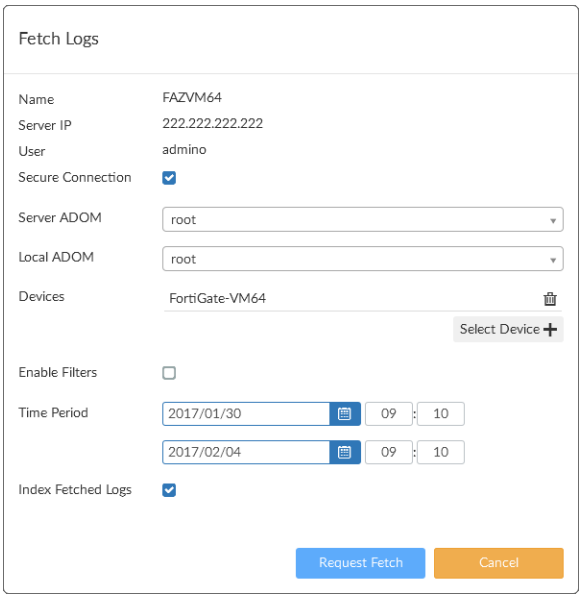
درخواست‌های Fetch

Fetch request لاگ‌های آرشیو شده درخواستی را از سرور fetch که در پروفایل انتخاب شده را می‌گیرد. وقتی درخواستی ایجاد می‌شود، لاگ‌های fetch شده باید مشخص گردند. یک ADOM بر روی fetch کلاینت باید مشخص شده یا اگر نیاز است مورد جدیدی ایجاد گردد.

درخواست fetch را ارسال کنیم:

۱. بر روی fetch کلاینت به مسیر System Settings> Fetcher Management رفته و تب Profiled را انتخاب کنید.

۲. پروفایل را انتخاب کرده و سپس از نوار ابزار بر روی Request Fetch کلیک کنید، کادر محاوره‌ای Fetch Logs باز می‌شود.



۳. تنظیمات زیر را پیکربندی کرده و سپس بر روی Request Fetch کلیک نمایید.

درخواست برای سرور fetch ارسال می‌شود. وضعیت درخواست در تب Session قابل مشاهده است.

Name	نامی که برای **Fetch** سرور مشخص کرده‌اید نمایش داده می‌شود.
Server IP	**IP** آدرسی که برای **Fetch** سرور خود مشخص کرده‌اید نمایش داده می‌شود.
User	نام کاربری ادمین سرور نمایش داده می‌شود.
Secure Connection	**SSL** کانکشن مورد استفاده را انتخاب کرده تا **fetch** لاگ‌ها از سرور جابجا شوند.
Server ADOM	**ADOM** روی سروری که لاگ‌ها از آن **Fetch** می‌شوند را انتخاب نمایید. فقط یک **ADOM** در یک زمان می‌تواند **Fetch** شود.
Local ADOM	**ADOM** روی کلاینت را انتخاب نمایید زمانی که لاگ‌ها دریافت می‌شوند. از لیست **ADOM** موجود را انتخاب نمایید یا **ADOM** جدیدی ساخته بوسیله وارد کردن یک نام در فلیدی که مشخص شده است.
Devices	اضافه کردن دستگاه‌هایی که لاگ‌ها از آنها **Fetch** می‌شوند. تا ۲۵۶ دستگاه امکان اضافه شدن را دارد. بر روی **Select Device** کلیک کنید، دستگاه‌ها را از لیست انتخاب نمایید و سپس **OK** کنید.
Enable Filters	فعال سازی فلیترها را انتخاب کرده تا لاگ‌های **fetch** شده امکان فلیترشدن را داشته باشند.
Time Period	پیام‌های لاگ **Fetch** شده را بر اساس زمان و تاریخ مشخص نمایید.
Index Fetch Logs	این قسمت اگر انتخاب شود لاگ‌های **Fetch** شده در دیتابیس **SQL** ایندکس می‌شوند.

همگام‌سازی دستگاه‌ها و ADOM ها

اگر برای بار اولی است که کلاینت از دستگاه لاگ‌ها را fetch می‌کند یا اگر تغییراتی از آخرین fetch صورت گرفته پس دستگاه‌ها و ADOMها باید با سرور همگام‌سازی شوند.

همگام‌سازی دستگاه‌ها و ADOM ها:

۱. بر روی کلاینت، به مسیر System Settings> Fetcher Management رفته و تب Profiles را انتخاب نمایید.

۲. پروفایل را انتخاب کرده و از نوار ابزار بر روی Sync Devices کلیک نمایید. پنجره The Sync Server ADOM & Devices باز می‌شود روند پیشرفت را برای شما نمایش می‌دهد.

وقتی اولین همگام‌سازی به انتها می‌رسد، امکان تایید تغییرات روی کلاینت وجود دارد. برای مثال، بوسیله پروفایل در ADOM مشخص دستگاه‌های جدید اضافه شده‌اند.

درخواست پردازش

بعد از کلاینت fetching یک درخواست fetch ایجاد می‌شود، این درخواست بر روی fetch سرور لیست شده و در قسمت Received Request در تب Sessions از پنجره Fetcher Management قرار می‌گیرد. این بخش از قسمت اعلانات سیستم هم در دسترس خواهد بود.

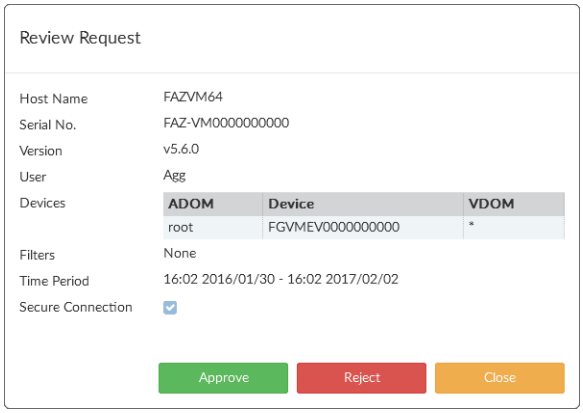
درخواست fetch می‌تواند پذیرفته یا رد شود.

پردازش درخواست fetch:

۱. به مسیر اعلانات اصلی سیستم در GUI بروید و بر روی درخواست fetch کلیک نمایید و یا به تب Sessions در قسمت System Settings> Fetcher Management بروید.

۲. از قسمت Received Request درخواست را پیدا کنید. از نوار ابزار بر روی Expand All کلیک کنید. وضعیت درخواست در حالت Waiting for Approval می‌باشد.

۳. با کلیک بر روی Review می‌توانید درخواست را بازنگری کنید. صفحه Review Request باز می‌شود.



٤. با کلیک بر روی گزینه Approve درخواست پذیرفته می‌شود یا با کلیک بر روی Reject درخواست رد می‌شود.

اگر درخواست ارسال شده پذیرفته شود، سرور لاگ‌های درخواستی را جمع آوری می‌کند و آنها را برای کلاینت ارسال می‌نماید. اگر درخواست رد شود، وضعیت آن در لیست به حالت Rejected on برای هر دو حالت کلاینت و سرور می‌رود.

مانیتور کردن fetch

مراحل درخواست fetch امکان مانیتور شدن در دو حالت کلاینت و سرور را دارا است.

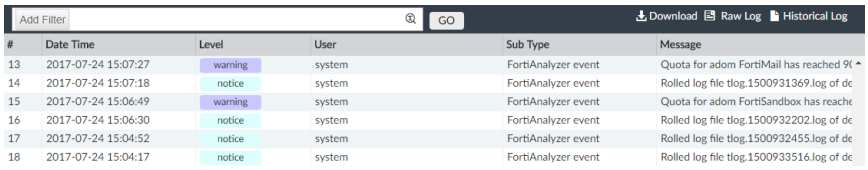
به مسیر System Settings> Fetcher Management بروید و تب Sessions را انتخاب کرده تا مراحل fetch را مانیتور نمایید. Session fetch امکان توقف لحظه‌ای با استفاده از pause و بازگشت مجدد با resume و یا دکمه cancel جهت ملغی کردن مراحل را دارد.

یکبار که لاگ fetching تکمیل می‌شود وضعیت تغییر کرده و به حالت done می‌رود و درخواست ثبت شده می‌تواند از طریق Delete پاک شود. کلاینت لاگ‌ها را در داخل دیتابیس ایندکس می‌کند. ممکن است مدت زمان زیادی طول بکشد تا کلاینت لاگ‌های fetch شده را ایندکس‌گذاری کرده و امکان آنالیز دیتا ایجاد شود. نوار وضعیت پیشرفت روند کار را در GUI نمایش می‌دهد. برای بدست آوردن اطلاعات بیشتر بر روی آن کلیک کرده تا باز شود. قابلیت‌های لاگ و گزارش به صورت کامل وجود ندارند تا زمانی که rebuilding به صورت کامل انجام شود.

لاگ رخدادها

پنجره Event Log لاگ‌های ممیزی از اتفاقات صورت گرفته توسط کاربران بر روی فورتی آنالایزر را جمع‌آوری می‌کند. به شما این امکان داده می‌شود تا پیام‌ها ذخیره شده در حافظه و یا هارددیسک دستگاه را مشاهده نمایید. جهت جستجو در لاگ‌ها و دانلود آنها در کامپیوتر خود می‌توانید از فیلترها استفاده نمایید.

به مسیر System Settings> Event Log رفته تا لیست لاگ‌های داخلی را مشاهده نمایید.



گزینه‌های زیر موجود می‌باشند:

Add Filter	**لاگ رخدادها بر اساس سطح لاگ، کاربر، sub type یا پیام فیلتر می‌شوند.**
Download	**لاگ رخدادها به صورت CSV یا فرمت نرمال در کامپیوتر دانلود می‌شوند.**
Raw Log / Formatted Log	**بر روی Raw Log کلیک کنید وضعیت لاگ‌ها در حالت raw قابل مشاهده باشد. با کلیک بر روی Formatted Log آنها را در قالب یک جدول مشاهده می‌نمایید.**
Historical Log	**با کلیک بر روی این گزینه لیست لاگ‌های مبتنی بر تاریخ را مشاهده کنید.**
Back	**با کلیک بر روی این گزینه به حالت مشاهده معمولی بازمی‌گردید.**
View	**فایل‌های لاگ انتخابی قابل رویت هستند. با راست کلیک کردن بر روی منو می‌توانید این گزینه را مشاهده نمایید.**

Delete	لاگ فایل انتخاب شده با این گزینه حذف می‌گردد. این امکان با راست کلیک بر روی منو قابل دسترسی است.
Clear	لاگ فایل‌های انتخابی پاک می‌شوند. این گزینه از طریق راست کلیک بر روی منو در دسترس است.
Type	از لیست نوع را انتخاب می‌کنید. • **Event Log** • **FDS Upload Log**
Search	جستجو در لاگ‌ها با وارد کردن یک عبارت انجام می‌شود.
Partition	مرور صفحه‌های لاگ‌ها و تنظیم تعداد لاگ‌هایی که در هر صفحه نمایش داده می‌شوند.

اطلاعات زیر نشان داده شده است:

#	عدد لاگ است.
Date Time	زمان و تاریخ ایجاد لاگ فایل می‌باشد.
Level	سطح لاگ: Debug Error Information Critical Notification Alert Warning Emergency
User	
Sub Type	**The log sub-type:** System manager event HA event FG-FM protocol event Firmware manager event Device configuration event FortiGuard service event Global database event FortiClient manager event

	Script manager event FortiMail manager event Web portal event Debug I/O log event Firewall objects event Configuration change event Policy console event Device manager event VPN console event Web service event Endpoint manager event FortiAnalyzer event Revision history event Log daemon event Deployment manager event FIPS-CC event Real-time monitor event Managed devices event Log and report manager event
Message	**جزئیات لاگ‌ها نمایش داده می‌شود.**

فیلتر کردن لاگ رخدادها

لاگ رخدادها با استفاده از Add Filter در نوار ابزار فیلترگذاری می‌شود.

فیلترگذاری خلاصه شده Fortiview با استفاده از نوار ابزار:

۱. مشخص کردن فیلترها در Add Filter.

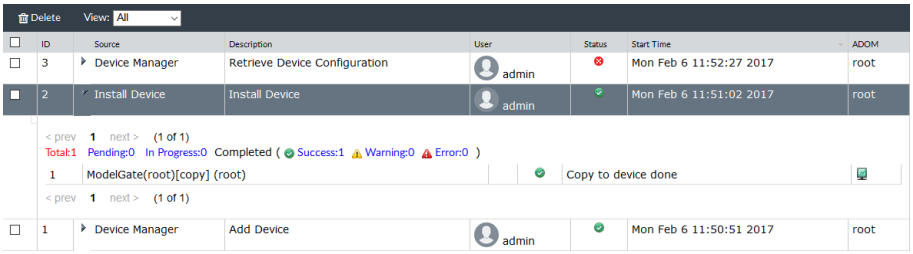
- جستجوی منظم: summary view را انتخاب نمایید. بر روی Add Filter کلیک کنید فیلتری را از لیست انتخاب نمایید و سپس مقداری را برای آن مشخص نمایید. با انتخاب NOT مقدار فیلتر را منفی می‌کنید. در یک زمان می‌توانید چندین فیلتر اعمال کنید و با گزینه or آنها را به هم متصل کنید.
- جستجوی پیشرفته: با کلیک بر روی آیکون switch to advanced Search وارد قسمت جستجوی پیشرفته می‌شوید و در این حالت معیارهای جستجوی خود را تایپ می‌کنید و با کلیک بر روی آیکون Switch to Regular به حالت جستجوی معمولی باز می‌گردید.

۲. با کلیک بر روی GO فلیترها را اعمال می‌کنید.

مانیتور وظایف

از طریق این قسمت می‌توانید وضعیت کارها را مشاهده و از انجام آنها مطلع شوید.

به مسیر System Settings> Task Monitor رفته تا وظایف را مشاهده کنید.



گزینه‌های زیر موجود می‌باشد:

Delete	**کار/کارهای انتخابی از لیست حذف می‌گردد.**
View	**بر اساس وضعیت کار امکان مشاهده آن از لیست وجود دارد.**
Expand Arrow	**در ستون source آیکون مربوط به باز شدن لیست را انتخاب کرده تا کارهای مربوط به این تیکت نمایش داده شود.**
Group Error Devices	**انتخاب Group Error Devices جهت ایجاد گروهی از دستگاه‌هایی که مشکل دارند. همچنین اجازه داده‌می‌شود تا نصب مجدد به آسانی بر روی دستگاه‌های مشکل‌دار صورت پذیرد.**
History	**انتخاب آیکون history برای مشاهده جزئیات کارها در پنجره جدید کاربرد دارد.**
Pagination	**صفحات وظایف را مرور کنید و تعداد کارهایی را که در هر صفحه نشان داده شده تنظیم کنید.**
ID	شماره شناسایی هر کار می‌باشد.

Source	کدام کار انجام شده است. با کلیک بر روی expand امکان مشاهده جزئیات هر وظیفه و دسترسی به دکمه تاریخچه موجود می‌باشد.
Description	ماهیت وظایف مشخص می‌گردد. اتفاقات مشخصی که با این کار به‌وقوع پیوسته است نمایش داده می‌شود.
User	کاربر/ کاربرانی که این وظایف را انجام داده‌اند.
Status	وضعیت کار: • Done: با موفقیت انجام شده است. • Error: ناموفق انجام شده است. • Canceled: کاربر کار را لغو کرده است. • Canceling: کاربر در حال متوقف کردن کار است. • Aborted: فورتی آنالایزر انجام این کار را متوقف کرده است. • Aborting: فورتی آنالایزر در حال متوقف کردن این کار می‌باشد. • Running: در حال پردازش می‌باشد. در این وضعیت یک نوار درصد نمایش داده می‌شود. • Pending: در حال انتظار • Warning: اخطار
Start Time	زمانی که کار شروع شده است.
ADOM	ADOM با یک کار در ارتباط است.
History	با کلیک بر روی دکمه history می‌توانید جزئیات کار را مشاهده کنید.

SNMP

با فعال سازی SNMP بر روی دستگاه امکان ارسال وضعیت فورتی آنالایزر برای کامپیوتر امکان‌پذیر می‌گردد. این کار باعث می‌شود فورتی آنالایزر با استفاده از یک SNMP منیجر مانیتور شود.

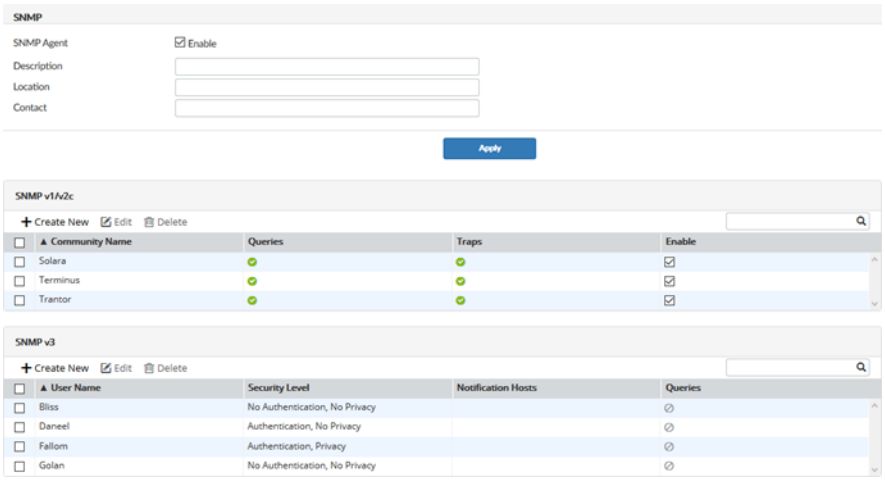
SNMP از دو بخش تشکیل شده است. SNMP Agent که Trapها را ارسال می‌کند. SNMP Manager که وظیفه رصد کردن موارد ارسالی را برعهده دارد. SNMP در فورتی آنالایزر به صورت read-only پیاده‌سازی شده و با نسخه‌های v1 و v2 و v3 سازگاری کامل دارد. در حالت read-only دستگاه trapها را دریافت می‌کند و تغییری صورت نمی‌گیرد.

SNMP Agent

SNMP Agent وظیفه دارد SNMP ترپ‌های ایجاد شده بر روی سیستم فورتی آنالایزر را به یک مانیتورینگ SNMP منیجر که در SNMP community آن تعریف شده ارسال کند. به صورت کلی یک SNMP منیجر برنامه‌ای بر روی کامپیوتر است که امکان خواندن SNMP ترپ‌ها و ایجاد گزارش‌ها یا گراف‌ها را از آنها دارد.

SNMP منیجر می‌تواند سیستم فورتی آنالایزر را مانیتور کرده تا تعیین کند اگر رخداد بحرانی به‌وقوع پیوست توضیحات و اطلاعات تماس برای این فورتی آنالایزر قسمتی از اطلاعات SNMP منیجر باشد. این اطلاعات زمانی مفید است که SNMP منیجر وضعیت دستگاه را مانیتور می‌کند.

به مسیر System Settings> Advanced> SNMP برای تنظیم SNMP agent بروید.



اطلاعات و تنظیمات زیر موجود می‌باشد:

SNMP Agent	با انتخاب **SNMP agent** آن را فعال نمایید. وقتی این گزینه فعال شود، ترپ‌های **SNMP** به فورتی آنالایزر ارسال می‌شود.
Description	**به صورت دلخواه، برای فورتی آنالایزر توضیحاتی وارد می‌کنیم.**
Location	**به صورت دلخواه، موقعیت فیریکی دستگاه را بر اساس نیاز خود وارد نمایید.**
Contact	**به صورت دلخواه، اطلاعات شخصی که وظیفه انجام تغییرات را دارد وارد نمایید.**
SNMP v1/2c	**لیست SNMP v1/v2 که به تنظیمات فورتی آنالایزر اضافه شده است.**
Create New	**با انتخاب گزینه Create New می‌توانید SNMP community اضافه نمایید. اگر SNMP agent انتخاب نشده باشد این بخش غیرفعال است.**
Edit	**ویرایش کاربر SNMP انتخاب شده انجام می‌پذیرد.**
Delete	**کاربر SNMP انتخاب شده را حذف می‌کند.**
User Name	**نام کاربری برای کاربر SNMP v3 مشخص می‌شود.**
Security Level	**سطح امنیتی کاربر SNMP v3 مشخص می‌شود.**
Security Level	**اعلانات هاست به کاربر SNMPv3 اختصاص داده می‌شود.**
Queries	**وضغیت کوئری SNMP برای هر کاربر SNMP نمایش داده می‌شود.**

SNMP v1/2c communities

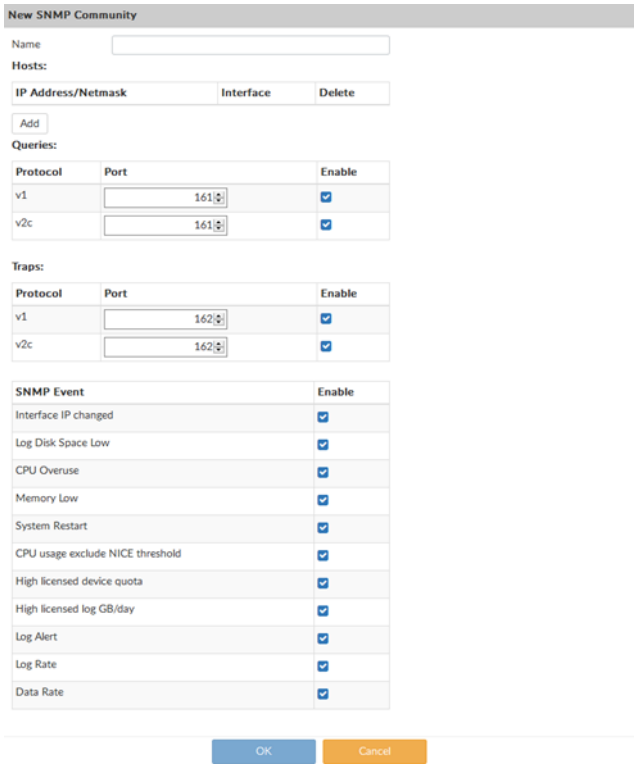
SNMP communityگروهبندی تجهیزات است که برای اهداف ادمین‌های شبکه مورد استفاده قرار می‌گیرد. فورتی آنالایزر باید طوری تنظیم شود که حداقل به یک SNMP community تعلق داشته باشد. بنابراین SNMP community منیجری که از SNMP ترپ‌ها پرس و جو می‌کند موارد را دریافت می‌نماید.

هر community برای SNMP Trapها می‌تواند تنظیمات متفاوتی داشته باشد. همچنین امکان پیکربندی به صورتی که وقایع متفاوت مانیتور شود وجود دارد. این امکان وجود دارد که IP آدرس‌ها طوری اضافه شوند که هشت عدد هاست برای هر community ترپ‌های مربوط به SNMP دیوایس‌ها را دریافت نماید.

ایجاد یک SNMP community جدید

۱. به مسیر System Settings> Advanced> SNMP رفته و مطمئن شوید که SNMP agent فعال است.

۲. در قسمت SNMP v1/v2c ، از نوار ابزار بر روی Create New کلیک کنید. پنجره New SNMP Community باز می‌شود.



۳. تنظیمات زیر را انجام داده سپس بر روی OK کلیک کنید.

Name	یک نام برای شناسایی SNMP community وارد نمایید. این نام بعدا قابل ویرایش نیست.
Hots	لیستی از هاست‌هایی برای مانیتور سیستم‌ها که با تنظیمات انجام شده در SNMP Community مورد استفاده قرار می‌گیرند. وقتی SNMP community ساخته می‌شود. هیچ هاستی در آن وجود ندارد. با انتخاب add یک ورودی جدید که SNMP آن broadcast می‌شود ایجاد می‌گردد.
IP Address/Netmask	IP آدرس و netmask مربوط به SNMP منیجر را وارد نمایید. به صورت پیش فرض، IP آدرس 0.0.0.0 می‌باشد بنابراین SNMP منیجر در SNMP community می‌تواند مورد استفاده قرار بگیرد.
Interface	اینترفیسی که به شبکه متصل شده را انتخاب نمایید.
Delete	بر روی آیکون Delete کلیک کنید تا SNMP Manager وارد شده حذف گردد.
Add	انتخاب این گزینه جهت وارد کردن هاست جدید می‌باشد. تعداد هشت SNMP منیجر امکان اضافه شدن را دارند.
Queries	وارد کردن شماره پورت که به صورت پیش فرض ۱۶۱ می‌باشد. بوسیله این پورت ارسال کوئری‌ها انجام می‌شود.
Traps	شماره پورت ۱۶۲ به صورت پیش فرض وارد شده است. فورتی آنالایزر برای ارسال trapها از این شماره پورت استفاده می‌کند.

SNMP Event	**فعال کردن رخدادهایی که سبب می‌شود SNMP ترپ‌هایی را به community ارسال کند.** **Interface IP changed** **Log disk space low** **CPU Overuse** **Memory Low** **System Restart** **CPU usage exclude NICE threshold** **RAID Event (only available for devices that support RAID)** **Power Supply Failed (only available on supported hardware devices)** **High licensed device quota** **High licensed log GB/day** **Log Alert** **Log Rate** **Data Rate**

ویرایش SNMP community :

۱. به مسیر System Settings> Advanced> SNMP بروید.

۲. در قسمتSNMP v1/v2c ، بر روی community دابل کلیک کنید، بر روی community راست کلیک کرده سپس Edit را انتخاب نمایید. پنجره Edit SNMP Community برای شما باز می‌شود.

۳. تنظیمات مورد نیاز خود را ویرایش کنید. سپس جهت اعمال تغییرات بر روی OK کلیک نمایید.

حذف کردن SNMP community:

۱. به مسیر System Settings> Advanced> SNMP بروید.

۲. در قسمت SNMP v3 ، کاربرانی که درنظر دارید حذف نمایید را انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک نمایید.

٤. برای تایید تغییرات صورت گرفته و حذف کاربران انتخابی کافی است بر روی OK کلیک نمایید.

میل سرور

میل سرور به فورتی آنالایزر اجازه می‌دهد تا پیام‌هایی مانند: اعلان‌ها زمانی که گزارشی اجرا شده یا رخداد خاصی اتفاق افتاده ارسال نماید. میل سرورها می‌توانند اضافه شوند؛ ویرایش شوند، حذف شوند و یا مورد تست قرار بگیرند.

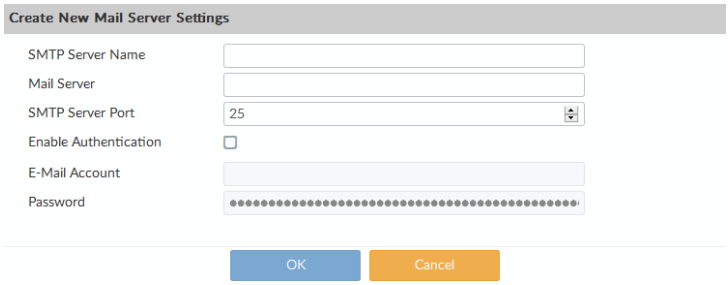
به مسیر System Settings> Advanced> Mail بروید تا بتوانید تنظیمات مربوط به میل سرور خود را انجام دهید.

اگر میل سرور در حال استفاده‌ای دارید، آیکون مربوط به حذف آن کار نخواهد کرد.

اضافه کردن میل سرور:

۱. به مسیر System Settings> Advanced> Mail Server بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید. پنجره Create New Mail Server Settings باز می‌شود.



۳. تنظیمات را بر اساس توضیحات زیر انجام داده و سپس جهت ساخت میل سرور OK نمایید.

Name	یک نام برای SMTP سرور خود انتخاب نمایید
Mail Server	**اطلاعات میل سرور را وارد نمایید.**
SMTP Server Port	**شماره پورت SMTP سرور را وارد نمایید. به صورت پیش فرض ۲۵ می‌باشد.**
Enable Authentication	**فعال سازی احراز هویت را انجام دهید.**

Email Account	**ایمیل اکانت را وارد نمایید. این گزینه فقط در شرایطی در دسترس است که احراز هویت فعال باشد.**
Password	**کلمه عبور اکانت ایمیل را وارد کنید. این گزینه در شرایطی کار می‌کند که احراز هویت فعال شده باشد.**

ویرایش میل سرور:

۱. به مسیر System Settings> Advanced> Mail Server بروید.

۲. بر روی سرور دابل کلیک کنید، از منو بر روی Edit راست کلیک نمایید. پنجره Edit Mail Server Settings باز می‌شود.

۳. بر اساس درخواست تغییرات را اعمال کنید و سپس جهت اعمال بر روی OK کلیک نمایید.

آزمودن میل سرور:

۱. به مسیر System Settings> Advanced> Mail Server بروید.

۲. سروری مورد بررسی را انتخاب نمایید.

۳. از نوار ابزار بر روی Test کلیک نمایید.

٤. آدرس ایمیلی که قرار است پیام تست را ارسال نمایید وارد کرده و سپس OK را بزنید. پیغام تائیدیه یا خطا نمایش داده خواهد شد.

۵. با کلیک بر روی OK کادر محاوره‌ای تایید بسته خواهد شد.

حذف کردن میل سرور:

۱. به مسیر System Settings> Advanced> Mail Server بروید.

۲. میل سروری که می‌خواهید حذف نمایید را انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک کنید.

٤. جهت تایید حذف سرور بر روی OK کلیک نمایید.

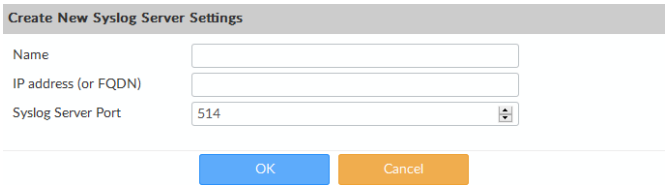
Syslog Server

به مسیر System Settings> Advanced> Syslog Server بروید تا تنظیمات سرور syslog خود را انجام دهید. امکان ویرایش، حذف و اضافه کردن Syslog سرورها وجود دارد.

اضافه کردن یک Syslog سرور:

۱. به مسیر System Settings> Advanced> Syslog Server بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید. پنجره Create New Syslog Server Settings نمایش داده می‌شود.



۳. تنظیمات زیر را بر اساس توضیحات انجام داده و بر روی OK جهت تایید کلیک نمایید.

Name	یک نام برای syslog سرور خود انتخاب نمایید
IP address or FQDN	**IP آدرس یا FQDN مربوط به syslog server را وارد نمایید.**
Syslog Server Port	**شماره پورت syslog سرور را وارد نمایید. پورت پیش فرض 514 می‌باشد.**

ویرایش یک syslog سرور:

۱. به مسیر System Settings> Advanced> Syslog server بروید.

۲. بر روی سرور دابل کلیک نمایید و سپس از منو گزینه Edit را انتخاب کنید. پنجره Edit Syslog Server Settings برای شما باز می‌شود.

۳. تنظیمات را بر اساس نیاز ویرایش کرده و جهت اعمال تغییرات بر روی OK کلیک نمایید.

جهت بررسی syslog سرور:

۱. به مسیر System Settings> Advanced> Syslog Server بروید.

۲. سروری که نیاز به بررسی دارد را انتخاب نمایید.

۳. از نوار ابزار بر روی Test کلیک نمایید. تایید یا خطای وضعیت برای شما نمایش داده خواهد شد.

حذف کردن Syslog سرور/سرورها

۱. به مسیر System Settings> Advanced> Syslog Server بروید.

۲. سرور/سرورها که درنظر دارید حذف نمایید را انتخاب کنید.

۳. از نوار ابزار بر روی Delete کلیک کنید.

٤. با کلیک بر روی OK سرورهای انتخاب حذف می‌شوند.

متا فلیدها

متافیلدها به ادمین این امکان را می‌دهد که در هنگام پیکربندی اطلاعات ویژه‌ای را اضافه نماید. امکان ایجاد فلیدهای اجباری یا اختیاری وجود داشته و همچنین تنظیم اندازه فیلدها وجود دارد.

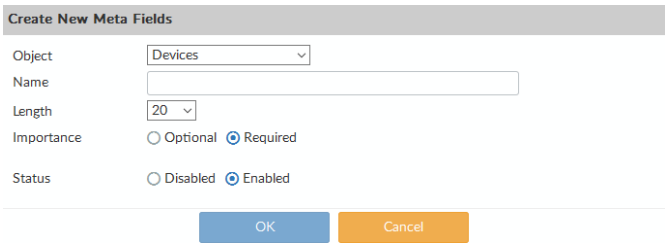
فیلدی که به صورت الزامی مقدار گرفته است حتما باید توسط ادمین‌ها در آن اطلاعات اضافی داده شود مثلا وقتی که این فیلد ایجاد می‌شود یک آبجکت جدید در فورتی‌گیت مواردی مثل یک اکانت ادمین یا فایروال پالیسی باید مقادیر اضافه وارد گردد. فیلدها برای اطلاعات جدید اضافه می‌شوند همانند یک کادر محاوره‌ای در جایی که آبجکت‌ها را اضافه می‌کنید. امکان درست کردن فیلدها برای اضافه کردن اطلاعات دلخواه وجود دارد.

به مسیر System Settings> Advanced> Meta Fields بروید تا پیکربندی متافلیدها را انجام دهید. متافیلدها می‌توانند اضافه شوند، ویرایش شوند و حذف گردند.

ایجاد کردن یک متافیلد جدید:

۱. به مسیر System Settings> Advanced> Meta Fields بروید.

۲. از نوار ابزار بر روی Create New کلیک کنید. پنجره Create New Field باز می‌شود.



۳. تنظیمات را بر اساس توضیحات زیر انجام داده و در انتها بر روی دکمه OK کلیک نمایید.

Object	مواردی که متادیتا به آنها اعمال می‌شود: دستگاه‌ها، گروه‌های دستگاه و دامین‌های ادمین
Name	**برای استفاده از فیلد یک نام وارد نمایید.**
Length	**بیشترین مقدار کاراکترهایی که اجازه دارید برای فیلد وارد نمایید را از لیست انتخاب نمایید.**
Importance	**انتخاب گزینه Required باعث می‌شود فیلد اجباری شود در غیر اینصورت در حالت اختیاری قرار می‌گیرد.**
Status	**انتخاب گزینه Disable باعث می‌شود این فیلد غیرفعال شود. انتخاب پیش فرض Enable است.**

ویرایش یک متافیلد:

۱. به مسیر System Settings> Advanced> Meta Fields بروید.

۲. بر روی یک فیلد دابل کلیک کنید، از منو گزینه Edit را کلیک نمایید. پنجره Edit Meta Fields باز می‌شود.

۳. تنظیمات را بر اساس نیاز ویرایش کنید و سپس جهت اعمال بر روی OK کلیک نمایید.

حذف کردن متافیلد:

۱. به مسیر System Settings> Advanced> Meta Fields بروید.

۲. فیلد یا فیلدهایی که می‌خواهید پاک کنید را انتخاب نمایید.

۳. از نوار ابزار بر روی Delete کلیک نمایید.

٤. جهت تایید بر روی OK کلیک نمایید تا فیلد/فیلدهای انتخابی حذف گردد.

متافیلدهای پیش فرض نمی‌توانند پاک شوند.

لاگ‌های دستگاه

فورتی آنالایزر این امکان را در اختیار شما می‌گذارد تا لاگ‌های سیستمی و رخدادها را بر روی دیسک نگهداری کنید. سایز لاگ فایل‌ها قابل تنظیم می‌باشد. تنظیم وضعیت لاگ و زمانبندی بارگذاری بر روی سرور کاملا قابل کنترل می‌باشد.

زمانی که فورتی آنالایزر لاگ آیتم‌های جدید را دریافت می‌کند، کارهای زیر انجام می‌شود:

- تایید اینکه آیا لاگ فایل از سایز مجاز خود بالاتر رفته است.
- چک شود که آیا زمان آن رسیده که پرونده ورودی در صورتی که حجم پرونده به حد مجاز نرسیده بررسی شود.

وقتی لاگ به بالاترین مقدار خود می‌رسد یا به زمان برنامه‌ریزی شده رسیده است. دستگاه بر اساس قوانین تعریف شده لاگ فعال را تغییر نام می‌دهد. نام فایل در فرم به شکل xlog.N.log. خواهد بود. X نامی است که نشان دهنده تایپ لاگ و N یک عدد همتا است که متناظر با زمان دریافت اولین لاگ ورودی می‌باشد. تغییر زمان فایل، زمانی است که مطابقت خواهد داشت با آخرین لاگ دریافت شده در لاگ فایل‌ها.

لاگ‌های جدید در شماتیک tlog.log. ذخیره می‌شوند. اگر آپلود لاگ فعال باشد یکبار logها آپلود شده و در سرور خارجی از طریق GUI دانلود می شوند و فرمتی شبیه به زیر دارند:

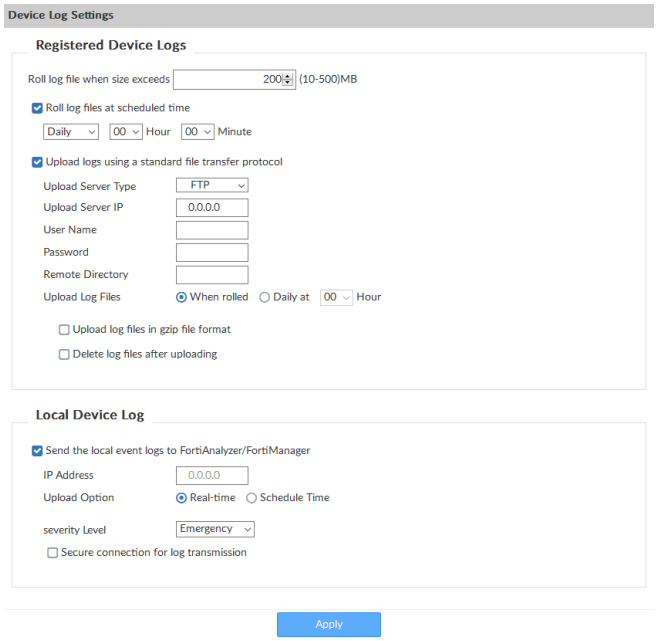
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.gz

اگر آپلود کردن log را فعال کرده باشید میتوان به صورت خودکار وضعیت را انتخاب کرد. بدین صورت که بعد از آپلود لاگ، کاملا حذف گردد و در نتیجه آزاد کردن مقداری از فضای دیسک مورد استفاده قرار می‌گیرد. اگر آپلود لاگ با خطا همراه باشد مانند زمانی که FTP سرور غیرفعال است لاگ‌ها در زمانبندی‌های مشخص آپلود می‌شوند.

قوانین لاگ‌ها و آپلود کردن آنها با استفاده از GUI و CLI می‌توانند پیکربندی و فعال شوند.

پیکربندی و آپلود لاگ‌های مورد استفاده در GUI:

به مسیر System Settings> Advanced> Device Log Settings رفته و تنظیمات مربوط به لاگ دستگاه را انجام دهید.



تنظیمات را بر اساس توضیحات جدول زیر انجام داده و سپس Apply کنید.

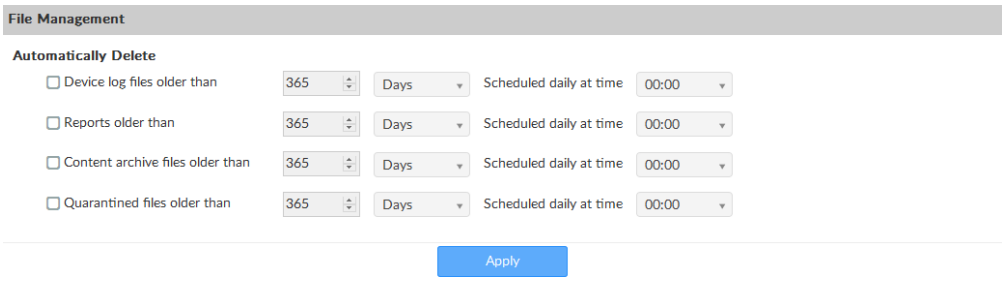
Registered Device Logs	
Roll log file when size exceeds	**سایز لاگ فایل را وارد نمایید. به صورت پیش فرض 200MB می‌باشد.**
Roll log files at scheduled time	• **Daily**: از لیست مقدار ساعت و دقیقه را مشخص نمایید. • **Weekly**: از لیست روز، ساعت و دقیقه را مشخص نمایید.
Upload logs using a standard file transfer protocol	**بارگذاری لاگ‌ها را انتخاب کرده و تنظیمات زیر را انجام دهید.**

Upload Server Type	یکی از حالت‌های **FTP**،**SFTP** ، **SCP** را انتخاب نمایید.
Upload Server IP	**IP** آدرس سرور آپلود را وارد نمایید.
User Name	نام کاربری جهت اتصال به سرور آپلود را وارد نمایید.
Password	کلمه عبور مورد استفاده جهت اتصال به سرور آپلود را وارد نمایید.
Remote Directory	ریموت دایرکتوری را وارد نمایید هنگامی که قرار است لاگ‌ها بارگذاری شوند.
Upload Log Files	لاگ فایل‌هایی که درنظر دارید آپلود شوند را انتخاب نمایید.
Upload rolled files in gzip file format	قبل از آپلود لاگ‌ها گزینه **gzip** را انتخاب کنید این کار سبب می‌شود لاگ‌ها کوچکتر شده و سریعتر آپلود شود.
Delete files after uploading	با انتخاب این گزینه لاگ فایل‌ها بعد از آپلود شدن پاک می‌شوند.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	ارسال لاگ‌های داخلی به فورتی آنالایزر یا فورتی‌منیجر
IP Address	**IP** آدرس فورتی آنالایزر یا فورتی منیجر را وارد نمایید.
Upload Option	انتخاب کنید آپلود لاگ‌ها به صورت بلادرنگ یا در زمانبدی‌های مشخص صورت گیرد. وقتی حالت زمانبندی را مشخص می‌کنید می‌توانید ساعت و دقیقه را مشخص نمایید.
Severity Level	از لیست کمترین **severity** لاگ را مشخص نمایید.
Secure connection for log transmission	برای استفاده از یک کانکشن مطمئن برای انتقال لاگ این قسمت را انتخاب نمایید.

مدیریت فایل

فورتی آنالایزر این امکان را به شما می‌دهد تا محتوای آرشیو فایل‌ها را در زمانبندی خودکار پاک، قرنطینه کرده و یا از آنها گزارش بگیرید.

به مسیر System Settings> Advanced> File Management بروید تا تنظیمات مدیریت فایل را پیکربندی نمایید.



تنظیمات زیر را انجام داده و سپس Apply کنید.

Device log files older than	قابلیت خودکار پاک کردن لاگ‌های فشرده شده را انتخاب نمایید. مقداری وارد نموده و دوره زمانی را انتخاب کنید.(روز، ماه، هفته)
Reports older than	**با انتخاب این گزینه امکان پاک کردن خودکار گزارش‌ها از لاگ فشرده شده وجود دارد.**
Content archive files older than	**امکان پاک کردن آرشیوهای IPS و DP از لاگ‌های آرشیوی را انتخاب کنید. دوره زمانی را مشخص و زمانی را انتخاب نمایید.**
Quarantined files older than	**قابلیت پاک کردن فایل‌های لاگ قرنطینه شده را فعال نمایید. یک مقدار مشخص و دوره زمانی را تعیین کنید.**

تنظیمات پیشرفته

به مسیر System Settings> Advanced> Advanced Settings رفته تا تنظیمات پیشرفته سیستم را انجام داده و فایل‌های WSDL را دانلود کنید.

پیکربندی را بر اساس جدول زیر انجام داده و Apply کنید.

ADOM Mode	ADOM را انتخاب و یکی از حالت‌های Normal یا Advanced را برگزینید. حالت Advanced به شما اجازه می‌دهد تا یک ADOM از یک دستگاه را به ADOM متفاوتی تخصیص دهید اما نتیجه بسیار پیچیده خواهد شد. این حالت فقط برای کاربران حرفه‌ای توصیه می‌شود.
Download WSDL file	WSDL مورد تقاضا را انتخاب کرده سپس بر روی دکمه Download کلیک کرده تا فایل WSDL را بر روی کامپیوتر دانلود نمایید. وقتی Legacy Operations را انتخاب می‌کنید، گزینه دیگری قابل انتخاب نیست. وب سرویس‌ها، پلتفرم‌های مستقل، روش دسترسی برای سایر سخت افزار و نرم افزار API استاندارد می‌باشند. استفاده از WSDL فایل، سبب ایجاد ارتباط برنامه‌های جانبی یا برنامه‌های دلخواه با دستگاه فورتی آنالایزر می‌شود و اطلاعات را بدست می‌آورد.
Task List Size	محدودیتی بر روی اندازه لیست وظایف تنظیم می‌کنید. به صورت پیش فرض ۲۰۰۰ است.

FortiManager

Device Manager (for FortiManager)	برای اضافه، تنظیم و مدیریت دستگاه‌های فورتی‌گیت ایجاد می‌گردد.
Policy and Object	مدیریت مرکزی دستگاه‌های فورتی‌گیت بوسیله ایجاد پالیسی‌ها و آبجکت‌ها و نصب آنها می‌باشد.

AP Manager	**مدیریت مرکزی FortiAP اکسس پوینت‌هایی که بوسیله مجوز دادن و مانیتور کردن دستگاه‌های FortiAP می‌باشد. امکان مانیتور و ویرایش دستگاه‌های مجاز وجود دارد.**
FortiClient Manager	**پروفایل‌های فورتی کلاینت به صورت مرکزی مدیریت می‌شوند تا دستگاه‌های فورتی‌گیت بهتر بتوانند فورتی کلاینت‌ها را مانیتور کنند.**
VPN Manager	**مدیریت مرکزی IPsec VPN برای ارتباطات و تنظیمات SSL-VPN است.**
FortiSwitch Manager	**مدیریت مرکزی فورتی سوئیچ و VLANها و مانیتور فورتی سوئیچ‌هایی که متصل به دستگاه‌های فورتی‌گیت هستند.**

در پنجره System Settings، قسمت HA وجود دارد تا تنظیمات مربوط به دسترس پذیری بالا را انجام دهید.

قابلیت‌های فورتی منیجر را فعال یا غیرفعال نمایید

قابلیت‌های فورتی منیجر را از طریق فورتی آنالایزر می‌توانید فعال نمایید بنابراین امکان مدیریت تعدادی از دستگاه‌های فورتی‌گیت وجود دارد. به استثنای قابلیت فورتی گارد تمام قابلیت‌های فورتی منیجر بر روی فورتی آنالایزر فعال می‌گردد.

لایسنس رایگانی که همراه با دستگاه فورتی آنالایزر وجود دارد قابلیت مدیریت دو فورتی‌گیت را می‌دهد. خرید یک لایسنس مدیریتی این امکان را به فورتی آنالایزر شما می‌دهد تا ۲۰ دستگاه فورتی‌گیت را مدیریت نمایید.

امکان فعال کردن یا غیرفعال کردن فورتی منیجر با استفاده از GUI یا CLI وجود دارد.

۱. به مسیر System Settings> Dashboard بروید.

۲. در ویجت System Information، سوئیچ FortiManager را به حالت On تغییر وضعیت بدهید.

۳. بعد از ریبوت سیستم از طریق محیط گرافیکی لاگین کنید.

صفحه اصلی فورتی آنالایزر قابلیت‌های فورتی منیجر را برای شما نمایش می‌دهد.

فعال کردن امکانات فورتی منیجر بر روی فورتی آنالایزر با استفاده از CLI:

۱. از CLI دستورات زیر را وارد نمایید:

```
config system global
set fmg-status enable
end
```

اعلان زیر نمایش داده می‌شود:

```
Changing fmg status will affect FAZ feature. If you continue, system will reboot.
Do you want to continue? (y/n)
```

۲. Y را تایپ نمایید.

۳. بعد از ریبوت سیستم، از طریق محیط GUI لاگین نمایید. قابلیت‌های فورتی منیجر فعال می‌گردد.

بروزرسانی لایسنس مدیریت:

۱. از طریق CLI دستورات زیر را وارد کنید:

```
config system global
set fmg-status disable
end
```

اعلان زیر نمایش داده می‌شود:

```
hanging fmg status will affect FAZ feature. If you continue, system will reboot.
Do you want to continue? (y/n)
```

۲. Y را تایپ کنید.

پایان