

کتاب آموزشے



KERIO

Control & Connect



به نام خدایی که در تب و تاب دلوپسی‌هایم، دستان گرم و توانگرش، ره‌توشه‌ی نادانسته‌هایم است
و در این گریز، به معبود بی‌همتایم می‌بالم که انسان هستیم و می‌اندیشیم.

کتاب آموزشی کریو ۲۰۱۶

نویسنده: فرشید باباجانی

ویراستار: آزاده تیشه برسر



تهران-۱۳۹۵

۵مقدمه
۶نصب و راه‌اندازی کریو کنترلر
۲۱لایسنس کریو
۲۳تنظیم ساعت و تاریخ
۲۳غیرفعال کردن سرویس IPv6
۲۴غیرفعال کردن سرویس Update
۲۴وارد کردن اینترنت به کریو
۳۱اشتراک گذاری اینترنت با کاربران
۳۴بررسی Mac Filtering در کریو
۳۶بررسی Traffic Rule
۳۹قطع کردن اینترنت کاربران و شخصی سازی آن
۴۰راه‌اندازی VPN Clients
۴۹ارتباط Kerio با Active Directory
۵۲بررسی Log در Kerio
۵۷بررسی kerio control statistics
۵۹نمایش مقدار کارکرد کاربران توسط خودشان
۶۱دسترسی کامل کاربر به قسمت kerio control statistics
۶۴بررسی قسمت Content Filter
۶۵بستن سایت برای کاربران
۶۸انتقال کاربر از سایت مسدود شده به سایت دیگر
۷۰بررسی تب Forbidden Words در ContentFilter
۷۲بررسی تب Kerio Control Web Filter
۷۳بررسی تب HTTPS Filtering
۷۷بررسی Bandwidth Management QOS

۸۲محدودیت سرعت بر روی سرویس خاص
۸۴مدیریت و بستن تلگرام در کریو
۹۰Guest Interfaces بررسی
۹۳فعال سازی گش سرور در کریو
۹۴فعال سازی آنتی ویروس در کریو
۹۷Intrusion Prevention بررسی سرویس
۹۸Kerio Control در Restore و Backup
۱۰۵Kerio Connect کار با
۱۱۱Kerio Connect در Search استفاده از قابلیت
۱۱۲Kerio Connect تعریف کاربر در
۱۱۶Kerio Connect ایجاد گروه در
۱۱۸Aliases ایجاد نام برای ایمیل کاربران
۱۱۹Kerio Connect در Outlook ارتباط نرم افزار با
۱۲۲بررسی ایمیل تحت وب
۱۲۴Kerio Connect در instant Messaging راه اندازی سرویس چت
۱۳۰Kerio Connect در Backup و Archiving فعال کردن
۱۳۲پاک کردن ایمیل های کاربران به صورت اتوماتیک
۱۳۴kerio Connect در Antivirus فعال کردن
۱۳۶Kerio control در Spam یا هرزنامه
۱۳۷فیلتر کردن پیام ها از آدرس های خاص
۱۴۰محدود کردن فایل های پیوستی ایمیل

مقدمه:

کریو، یک شرکت در حوزه فناوری اطلاعات است که در سال ۱۹۹۷ در شهر سن خوزه آمریکا تأسیس شد و مدیران آن، Mirek KrenAlan, Hughes Scott, Schreiman هستند.

کریو که قبلاً با نام KERIO WINROUTE و پیشتر با نام WINROUTE شناخته می‌شد، توسط شرکت Kerio TECHNOLOGIES توسعه پیدا کرده است، این نرم‌افزار از مجموعه‌ی VPN، FireWall، Anti Virus، Web Filtering، Monitoring، Internet Management و... تشکیل شده است.

هسته‌ی مرکزی کریو، لینوکس است و برای سازمان‌های کوچک و متوسط طراحی شده است.

تولیدات شرکت کریو عبارت‌اند از:

- ۱- Samepage: یک سایت Cloud که برای اشتراک‌گذاری اطلاعات کاربران ایجاد شده است.
 - ۲- Kerio Connect: برای ایجاد ایمیل سرور در شبکه کاربرد دارد و در این کتاب بررسی خواهد شد.
 - ۳- Kerio Control: نرم‌افزار فایروال کریو که برای ویندوز، لینوکس و مک طراحی شده است.
 - ۴- Kerio Operator: نرم‌افزاری برای سیستم تلفنی است.
- در کتاب پیش‌رو، تمام نیازهای کاربر را به منظور راه‌اندازی سرور کریو، قدم به قدم به شکل کاملاً تصویری آموزش خواهیم داد، با یاری خدا، این آموزش مفید واقع گردد.
- این کتاب را تقدیم می‌دارم به همسر عزیزم که سایه‌ی مهربانی‌اش سایه‌سار زندگی‌ام می‌باشد و صبر و تحملش، کلید واژه‌ای از فداکاری و حضور است.

نصب و راه‌اندازی کریو کنترلر:

برای راه‌اندازی کریو می‌توانیم از یک سیستم واقعی استفاده کنیم و کریو را روی آن نصب و اجرا کنیم، چون کریو بر پایه‌ی لینوکس است، خیلی راحت می‌توانیم آن را نصب و از آن استفاده کنیم؛ روش دیگر استفاده این است که آن را بر روی یک ماشین مجازی نصب و استفاده کنیم؛ در ادامه بر روی این موضوعات بیشتر بحث خواهیم کرد.

برای شروع کار از آدرس زیر، آخرین ورژن نرم افزار Kerio Controller را دانلود کنید:

<http://technet24.ir/kerio-control-software-appliance-1498>

بعد از دانلود می‌توانید آن را بر روی DVD رایت کنید و مانند سیستم‌عامل‌های دیگر نصب کنید، روش دیگر آن است که آن را بر روی یک نرم‌افزار مجازی مانند: VMware یا Hyper-V نصب کنید.

در این کتاب برای راحتی کار شما عزیزان از نرم‌افزار مجازی‌سازی VMware استفاده می‌کنیم، برای این منظور، می‌توانید از لینک زیر نرم‌افزار VMware 12 را دانلود کنید:

<http://p30download.com/fa/entry/60296/>

اگر با این نرم‌افزار کار نکردید، می‌توانید از لینک زیر آموزش آن را دانلود کنید:

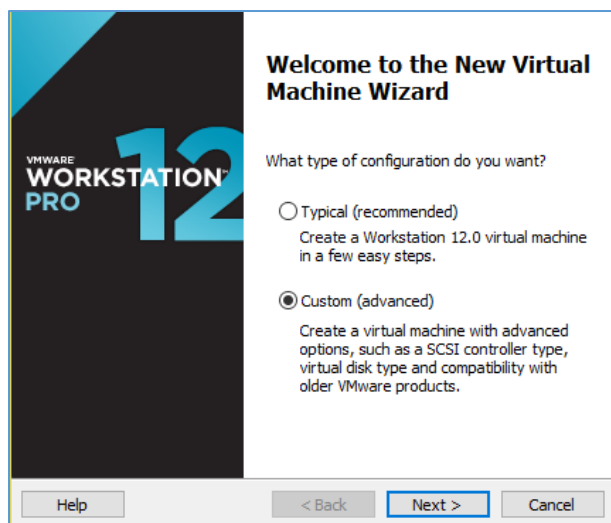
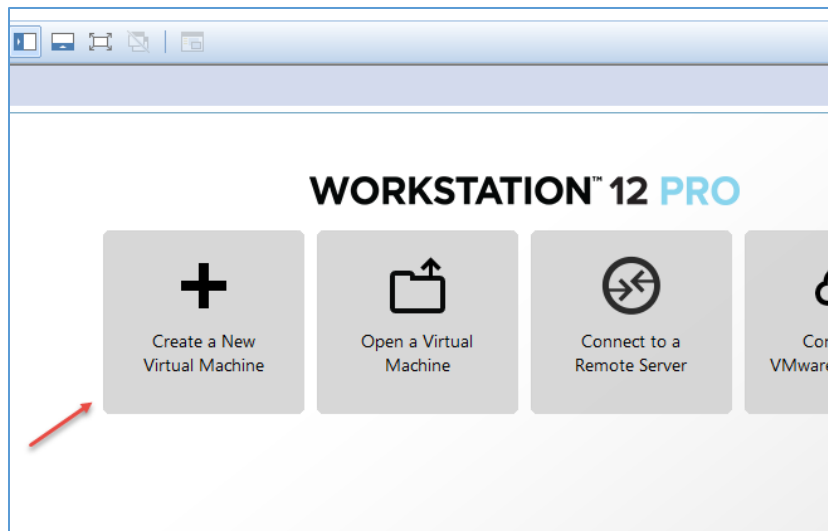
<http://p30download.com/fa/entry/49359/>

نصب نرم‌افزار VMware از طریق همین کتاب آموزشی که دانلود کردید، انجام دهید تا برای نصب کریو همه چیز آماده باشد.

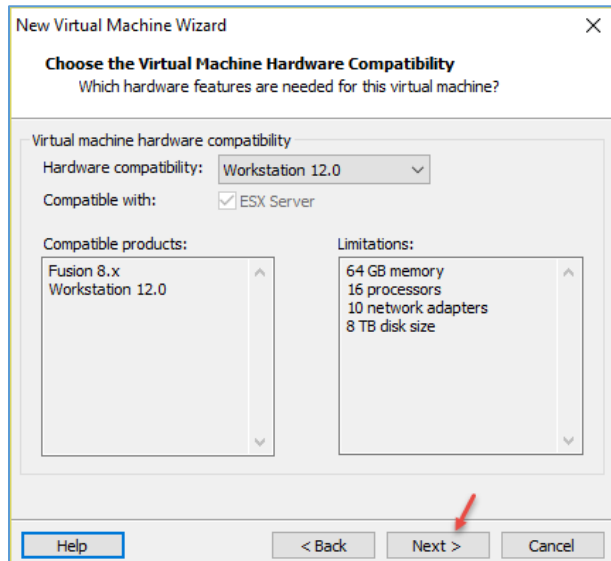
سعی کنید دقیقاً طبق کتاب، کارها را انجام دهید تا با مشکلی مواجه نشوید؛ اگر در هر قسمت از کتاب به مشکلی برخوردید، با من در تماس باشید.

شروع نصب:

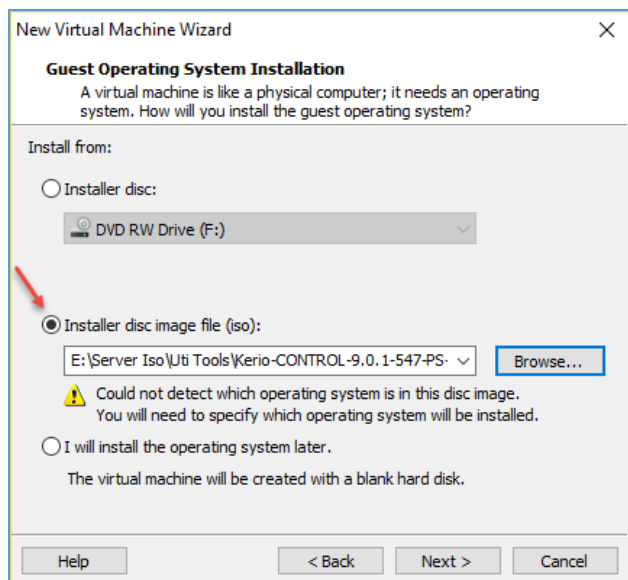
وارد نرم افزار VMware شوید و برای ایجاد ماشین مجازی بر روی Create a New Virtual Machine کلیک کنید تا شکل بعد ظاهر شود.



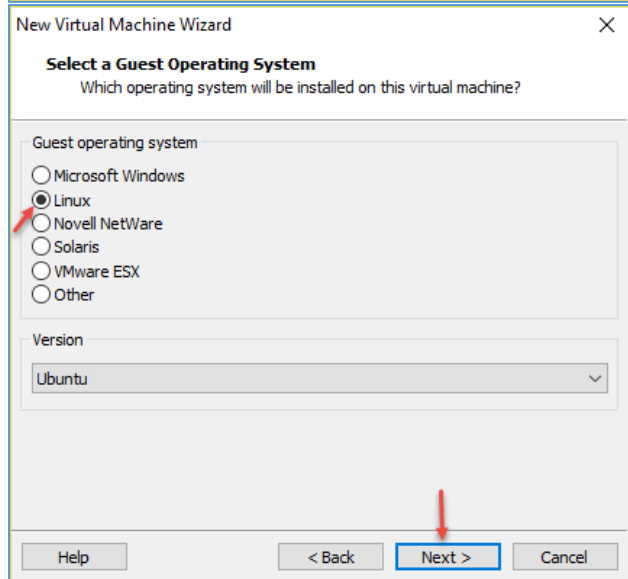
در این صفحه، گزینه‌ی Custom را انتخاب کنید و بر روی Next کلیک کنید.



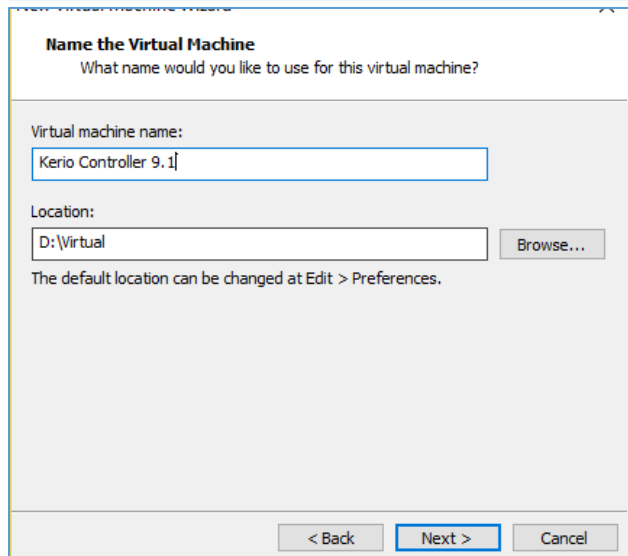
در این قسمت، Workstation 12.0 که آخرین ورژن آن است و جدیدترین سخت افزارها را پشتیبانی می کند را انتخاب و بر روی Next کلیک کنید.



در این شکل، گزینه‌ی دوم را انتخاب و بر روی **Browse** کلیک کنید و فایل ISO مربوط به Kerio Control 9.1 را که دانلود کردید، انتخاب و بر روی **Next** کلیک کنید.



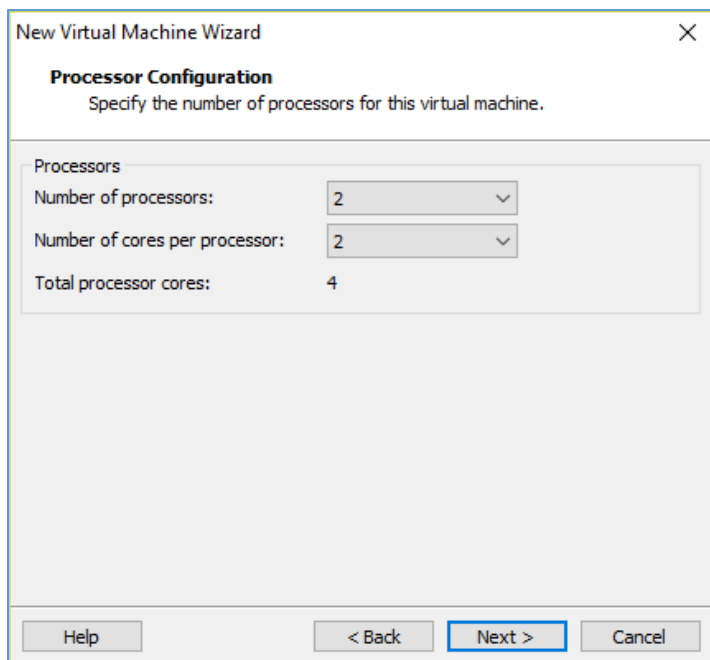
در این صفحه، گزینه‌ی **Linux** را انتخاب و بر روی **Next** کلیک کنید.



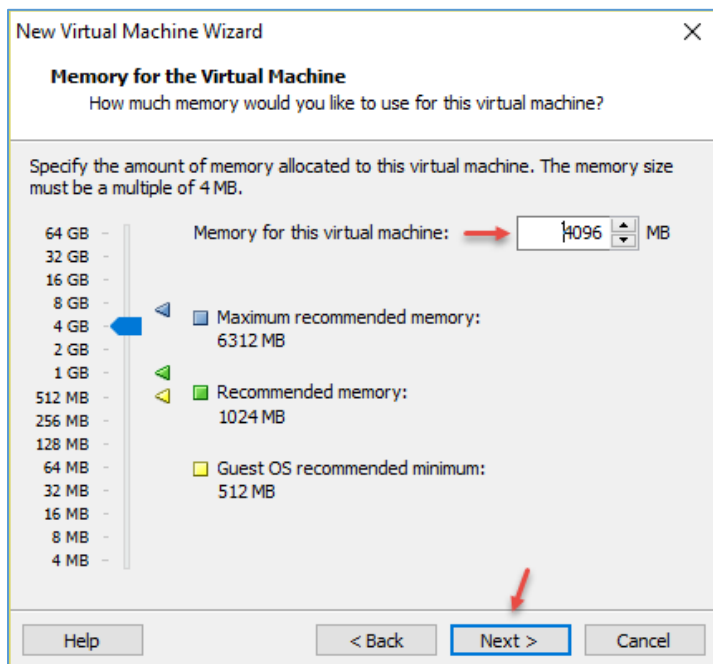
در این صفحه، نام سرور خود را وارد کنید و در قسمت **Location**، آدرس ذخیره‌سازی آن را مشخص و بر روی **Next** کلیک کنید.

برای دریافت اطلاعات در مورد سخت افزار و نرم افزار مورد نیاز برای نصب Kerio می توانید از لینک زیر استفاده کنید:

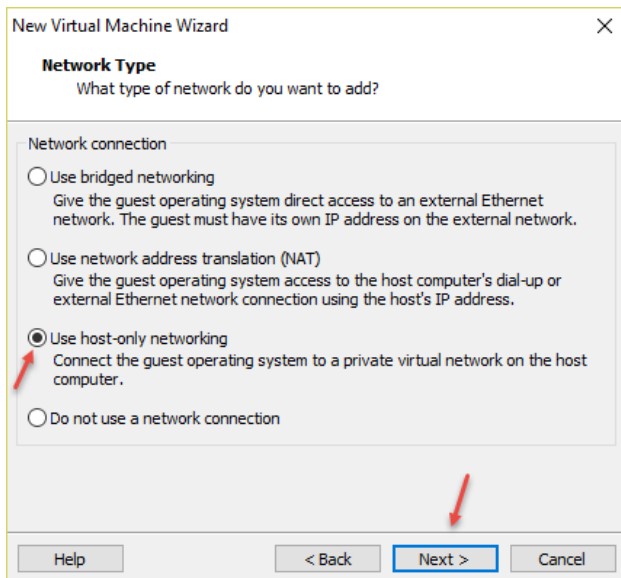
<https://www.kerio.com/content/control-system-requirements>



در این قسمت، حداکثر هسته‌ی CPU را انتخاب و بر روی **Next** کلیک کنید.

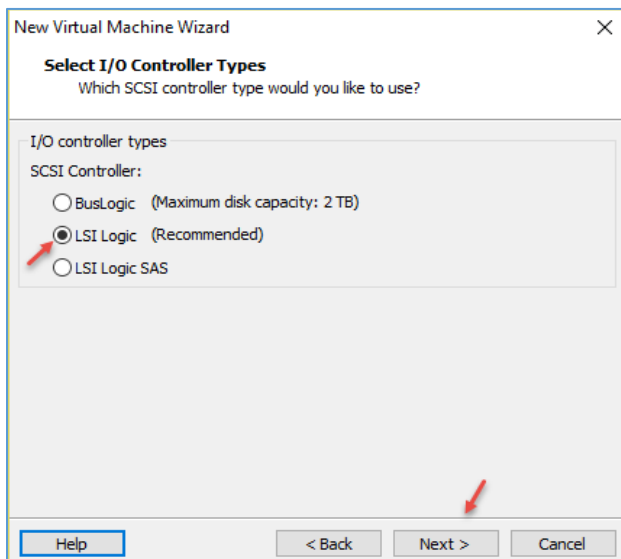


در این صفحه باید مقدار رم خود را انتخاب کنید، حداقل رم برای راه اندازی کریو، ۲ گیگابایت است که در این قسمت برای حداکثر کارایی، ۴ گیگابایت در نظر می گیریم و بر روی **Next** کلیک می کنیم.

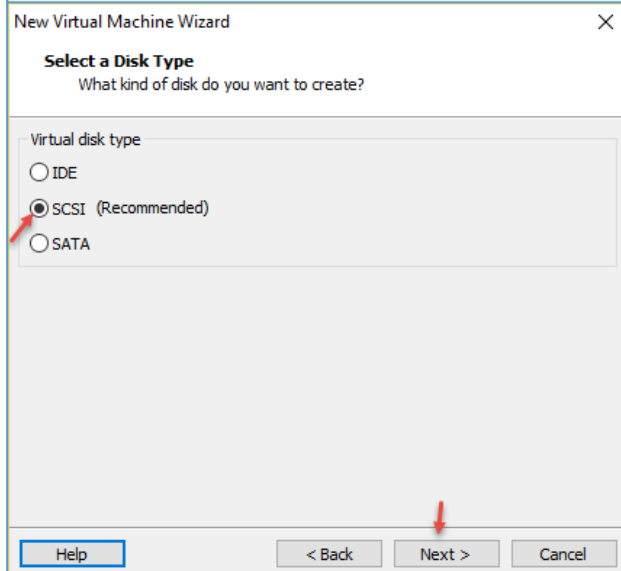


این قسمت برای ایجاد کارت شبکه‌ی مجازی برای کریو است تا بتوانیم از طریق آدرس ip به صفحه‌ی مدیریتی آن دست یابیم.

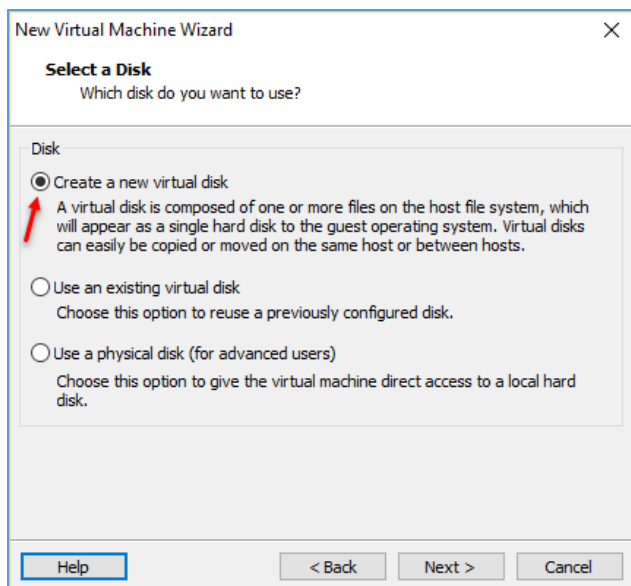
گزینه‌ی **use host-only networking** را انتخاب کنید، این گزینه، یک کارت شبکه‌ی مجازی در لیست کارت شبکه‌های ویندوز شما ایجاد می‌کند و شما از طریق آن می‌توانید به کریو متصل شوید، بر روی **Next** کلیک کنید.



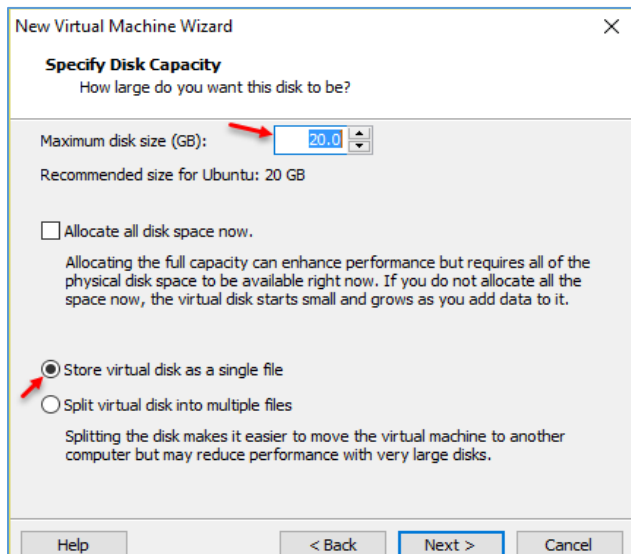
در این قسمت باید نوع کنترلر **SCSI** خود را انتخاب و بر روی **Next** کلیک کنید.



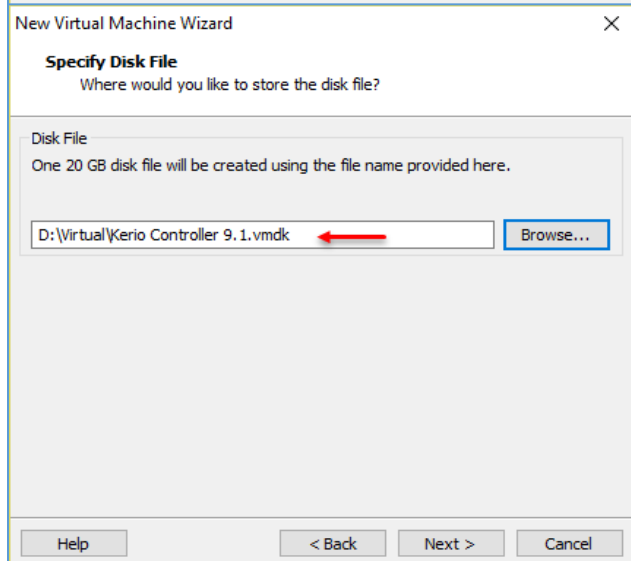
در این صفحه، نوع دیسک خود را **SCSI** انتخاب کنید و بر روی **Next** کلیک کنید.



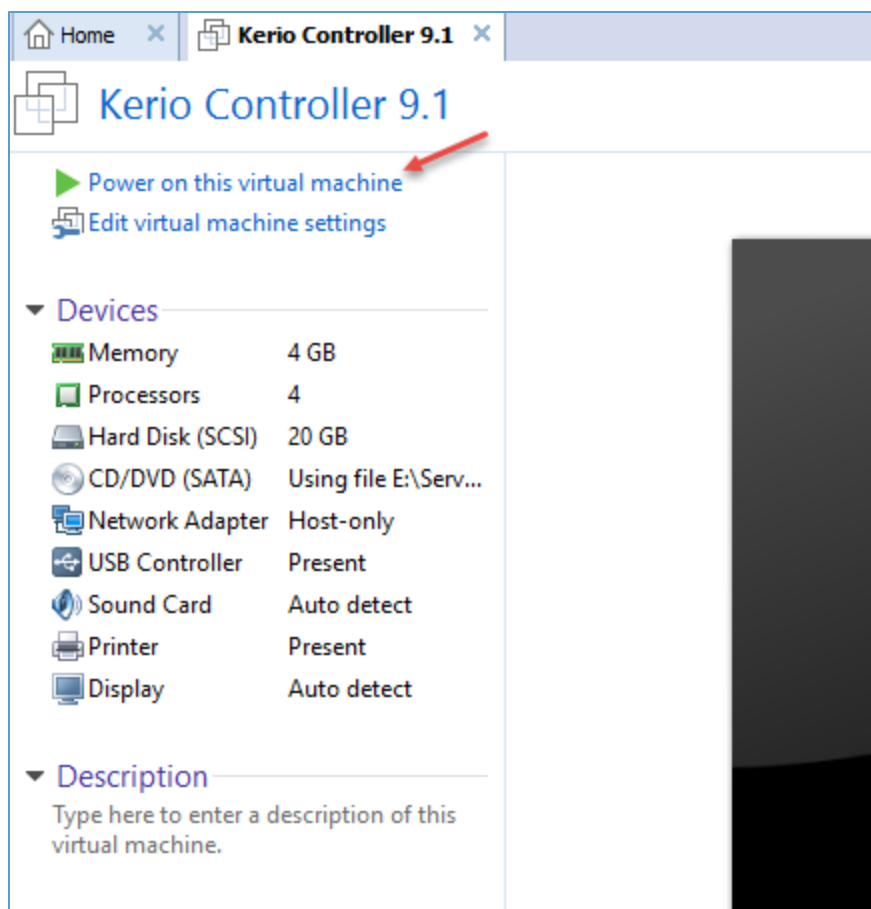
در این قسمت باید برای ایجاد هارد دیسک مجازی، گزینه **Create a new virtual disk** را انتخاب و بر روی **Next** کلیک کنید.



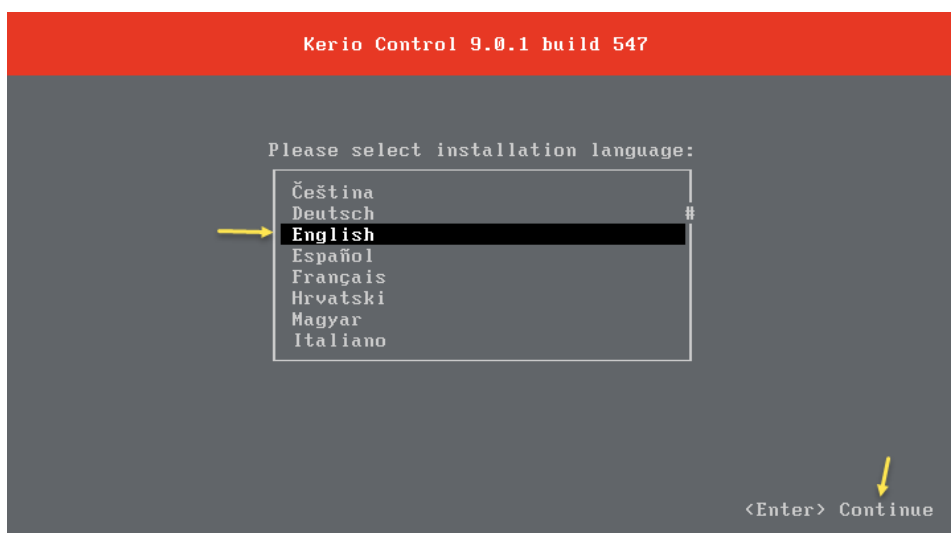
در این صفحه، مقدار فضای هارد دیسک خود را مشخص کنید، حداقل فضا برای استفاده از کریو، ۸ گیگابایت پیشنهاد شده است که شما می‌توانید آن را بیشتر کنید، اگر تیک گزینه **Allocate all disk...** را انتخاب کنید، کل فضای دیسک در هارد واقعی به کریو اختصاص داده خواهد شد؛ گزینه **Store virtual disk as a single file** را انتخاب کنید تا تمام اطلاعات در یک فایل ذخیره شود.



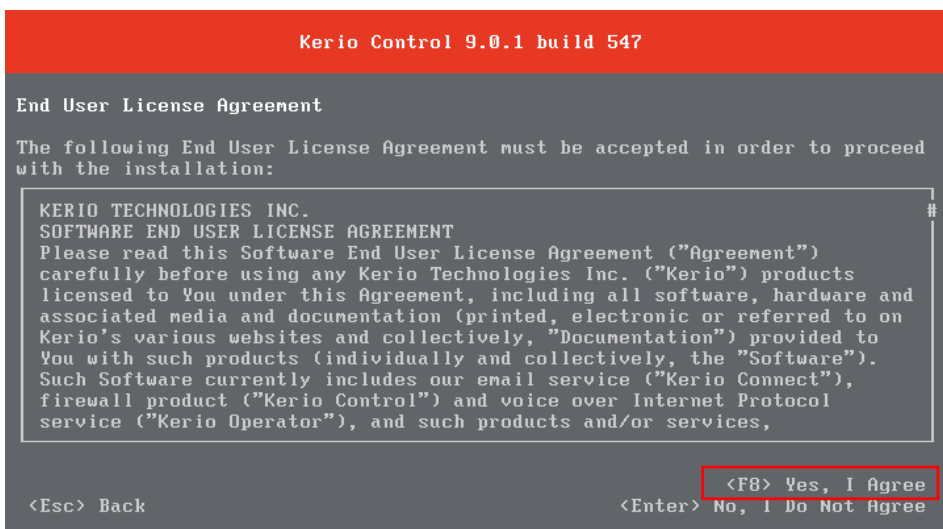
در این صفحه، محل ذخیره‌سازی فایل هارد دیسک خود را انتخاب و بر روی **Next** کلیک کنید.



بعد از ایجاد ماشین مجازی به مانند شکل، آن را روشن کنید تا کار نصب کریو را با هم انجام دهیم.



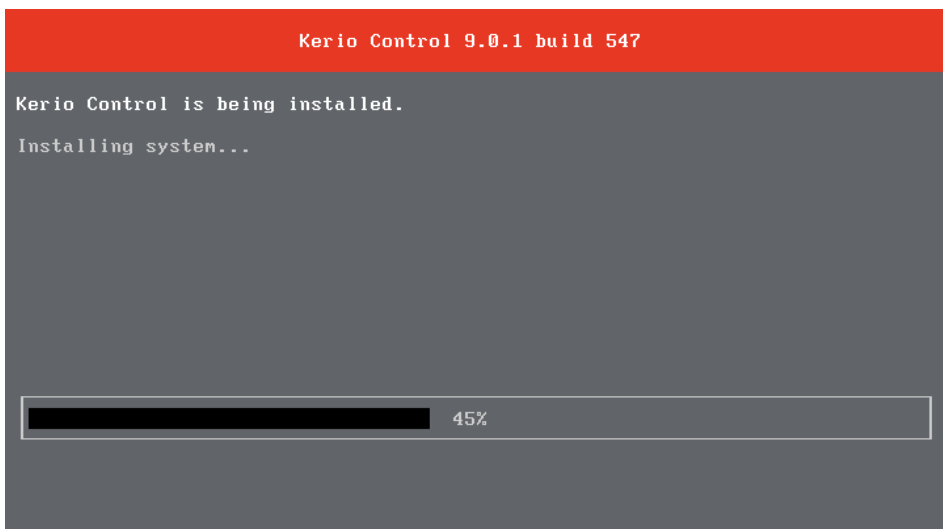
بعد از اجرای ماشین مجازی، صفحه‌ی ابتدایی نصب کریو را به مانند شکل روبرو مشاهده می‌کنید؛ زبان مورد نظر خود را انتخاب کنید و بر روی **Enter** فشار دهید.



در این صفحه، اگر قراردادنامه‌ی شرکت Kerio را قبول دارید، بر روی f8 کلیک کنید تا ادامه‌ی کار انجام شود.



در این صفحه به شما پیام اخطار داده می‌شود که اگر عدد ۱۳۵ را در قسمت مورد نظر وارد کنید و بر روی Enter فشار دهید، تمام اطلاعات هارد دیسک پاک خواهد شد، این کار را انجام دهید تا به صفحه‌ی بعد برویم.



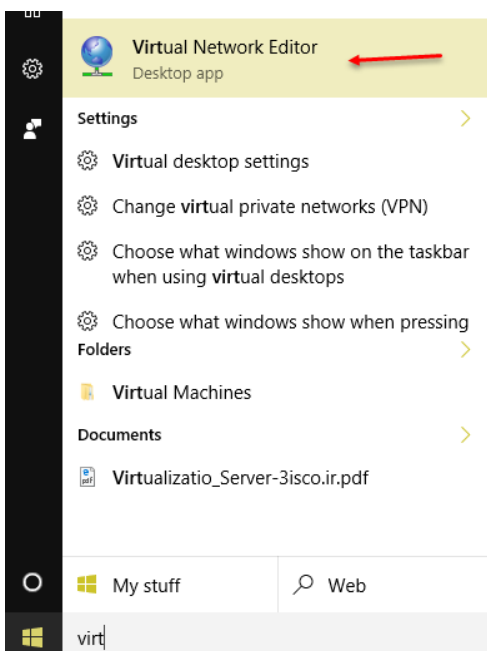
همانطور که مشاهده می‌کنید، کریو در حال نصب است.



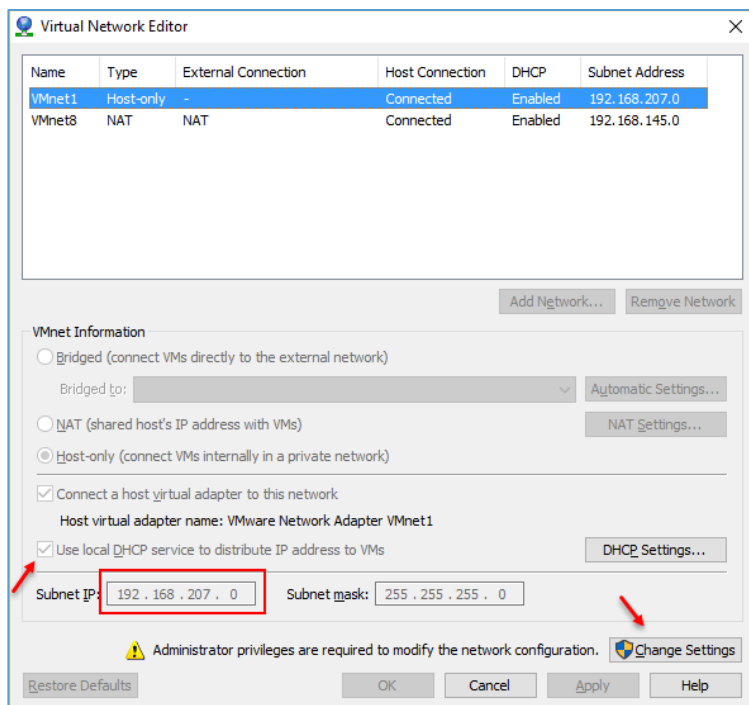
در این قسمت، نصب به اتمام رسیده است که برای تأیید نهایی باید بر روی **Enter** فشار دهید تا سیستم **Restart** شود.



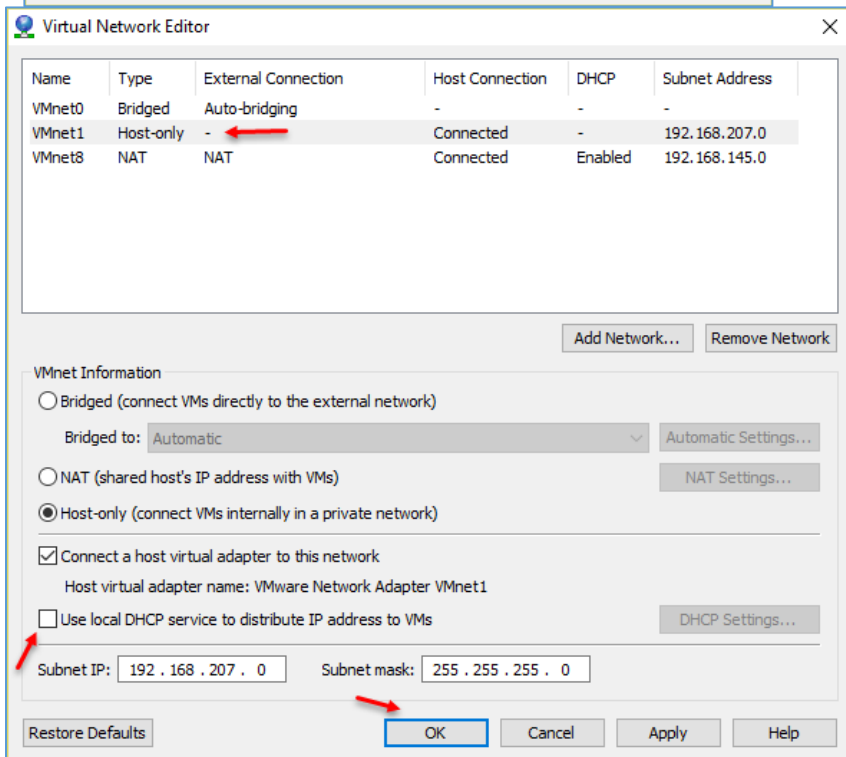
همانطور که مشاهده می‌کنید، کریو با موفقیت نصب شده است و یک آدرس تحت وب نمایش داده شده است، این آدرس همان آدرس صفحه‌ی مدیریتی کریو است؛ حال این سؤال برای شما پیش می‌آید که چگونه این آدرس را به ما نشان داده است.



زمانی که نرم‌افزار **VMware** را نصب می‌کنید، به صورت پیش‌فرض، دو کارت شبکه‌ی مجازی را به لیست کارت شبکه‌های شما اضافه می‌کند که از طریق سرویس **DHCP** به کلاینت‌ها و سرورها **IP** می‌دهد، برای مدیریت آن باید وارد **Search** شوید و **Virtual** را وارد کنید و به مانند شکل، **Virtual Network Editor** را انتخاب کنید.



همانطورکه در این صفحه مشاهده می‌کنید، دو کارت شبکه در لیست موجود است که کارت شبکه‌ی اول، همان کارت شبکه‌ای است که قبلاً به کریو متصل کردیم، اگر به پایین صفحه توجه کنید، تیک گزینه‌ی **use local DHCP...** انتخاب شده است و رنج IP آن نیز، همان رنجی است که در کریو مشاهده می‌کنید، برای اینکه این تنظیمات را تغییر دهید باید بر روی **Change Settings** کلیک کنید.



همانطورکه مشاهده می‌کنید، یک کارت شبکه‌ی دیگر با عنوان **VMnet0** به لیست اضافه شده است که بر روی **Bridged** قرار دارد و به صورت مستقیم به کارت شبکه‌ی اصلی سیستم، متصل است؛ برای اینکه به کریو یک آدرس استاتیک (دستی) و مشخص دهیم، بهتر است **DHCP** را در این قسمت، غیرفعال کنیم که برای این کار باید تیک گزینه‌ی **Use local DHCP...** را برداریم و بر روی **ok** کلیک کنیم.



برای انجام تنظیمات در کریو وارد سرور شوید و بر روی **Enter** فشار دهید تا شکل بعد ظاهر شود.



وارد تنظیمات Kerio شده‌اید، برای تنظیم آدرس IP، گزینه‌ی اول را انتخاب کنید و بر روی **Enter** فشار دهید.



در این صفحه و در قسمت Ethernet، مشخص شده است که IP Address بر روی DHCP قرار دارد، چون از قبل سرویس را غیرفعال کرده‌ایم، در حال حاضر هیچ IP را دریافت نکرده است؛ برای دادن IP به صورت دستی بر روی **Enter** فشار دهید.

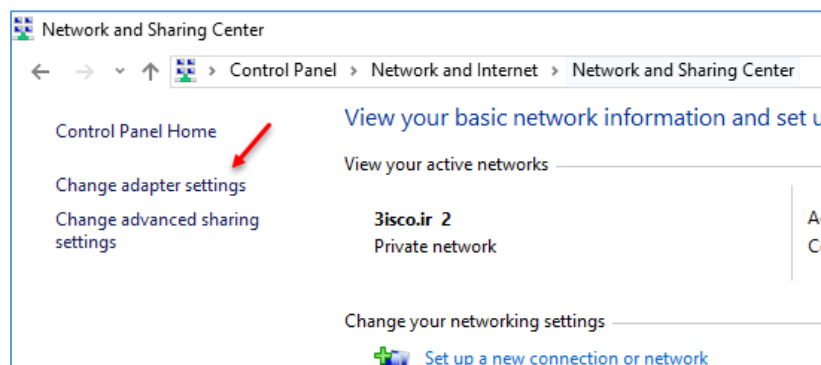


در این صفحه برای وارد کردن IP به صورت دستی یا همان Static باید گزینه‌ی دوم را با فشار دکمه‌ی Space انتخاب کنید و با کلید IP Address جهت‌نما به قسمت رجوع و اطلاعات مورد نظر را به مانند شکل وارد کنید و در آخر برای ذخیره‌کردن آن باید بر روی F8 کلیک کنید.

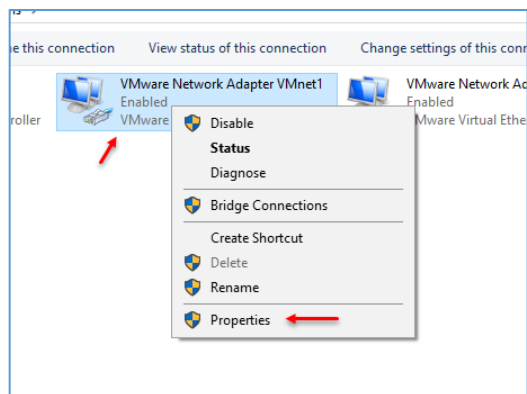
همانطورکه مشاهده می‌کنید، آدرس مورد نظر تغییر کرده است، پس باید بتوانید به آن متصل شوید.

در حال حاضر، اگر بخواهید به این آدرس متصل شوید با خطا مواجه خواهید شد، چون سرویس DHCP را قطع کردید باید در ویندوز نیز به کارت شبکه مورد نظر یک آدرس در همان رنج بدهیم، برای همین وارد آدرس زیر شوید:

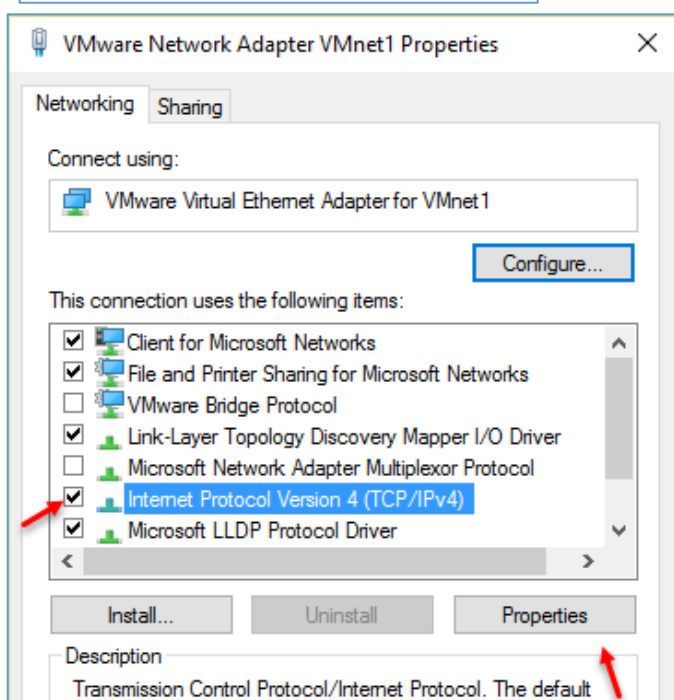
Control Panel\Network and Internet\Network and Sharing Center



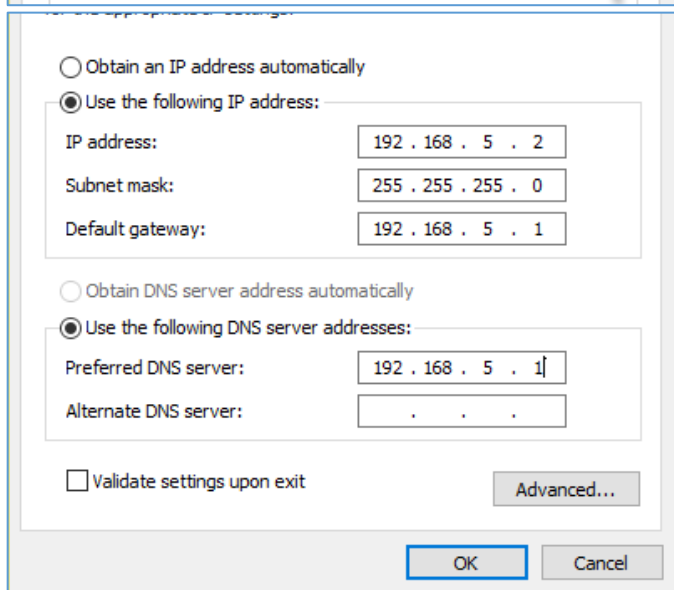
در این صفحه بر روی Change Adaptor Settings کلیک کنید تا کارت شبکه‌ی این سیستم را مشاهده کنید.



در صفحه‌ی مورد نظر باید روی کارت شبکه‌ای که قبلاً روی آن سرویس DHCP را غیرفعال کردیم، انتخاب کنید که در این قسمت باید کارت شبکه‌ی VMnet1 را انتخاب و بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



در این صفحه و از لیست مورد نظر گزینه‌ی Internet Protocol Version 4 را انتخاب و بر روی Properties کلیک کنید.



در این صفحه، یک آدرس ۱۹۲،۱۶۸،۵،۲ که در رنج ۵ قرار دارد را به مانند شکل وارد کنید و بر روی ok کلیک کنید؛ چنانچه در قسمت IP مشکل دارید، می‌توانید کتاب ++ CCNA بنده را مطالعه نمایید، برای دریافت آن از لینک زیر استفاده کنید:

<http://p30download.com/fa/entry/60695>

```

C:\> Command Prompt - ping 192.168.5.1 -t

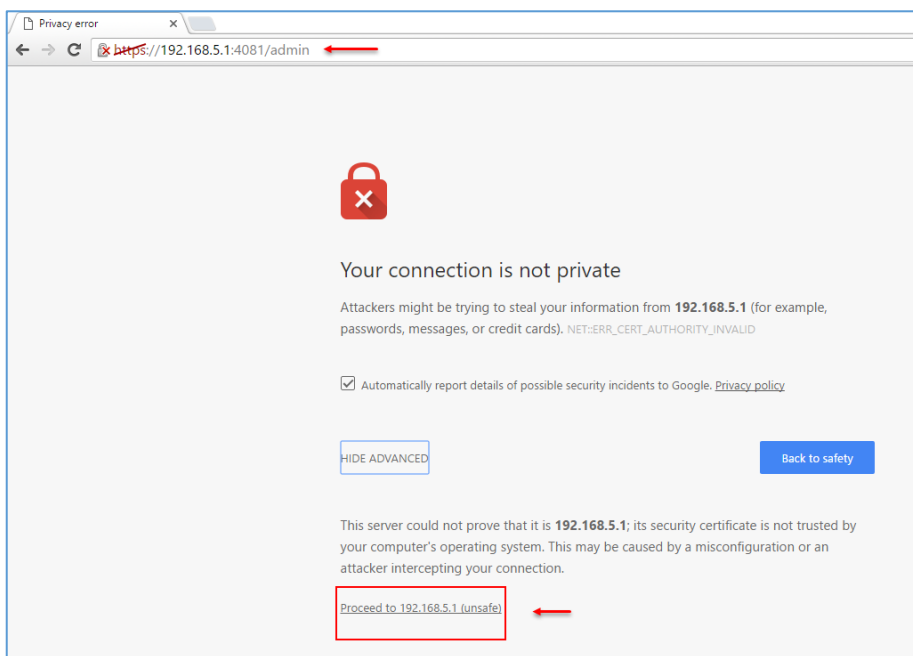
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\A-F> ping 192.168.5.1 -t

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64
Reply from 192.168.5.1: bytes=32 time<1ms TTL=64

```

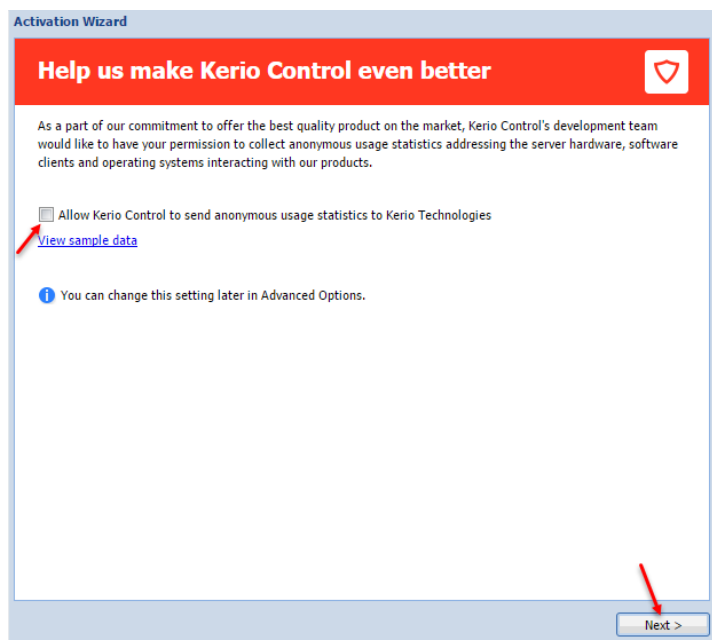
بعد از وارد کردن IP Address مورد نظر، اگر سرور کریو را به مانند شکل روبرو، Ping بگیرید، مشاهده خواهید کرد که به خوبی ارتباط بین ویندوز و کریو برقرار است.



بعد از اینکه آدرس IP آماده شد، وارد یکی از مرورگرهای خود شوید و آدرس زیر را وارد کنید:

`/https://192.168.5.1:4081/admin`

شما باید به جای ۱۹۲،۱۶۸،۵،۱ آدرس سرور خود را وارد کنید که بعد از اجرا با خطای Certificate مواجه خواهید شد که باید بر روی Proceed کلیک کنید.

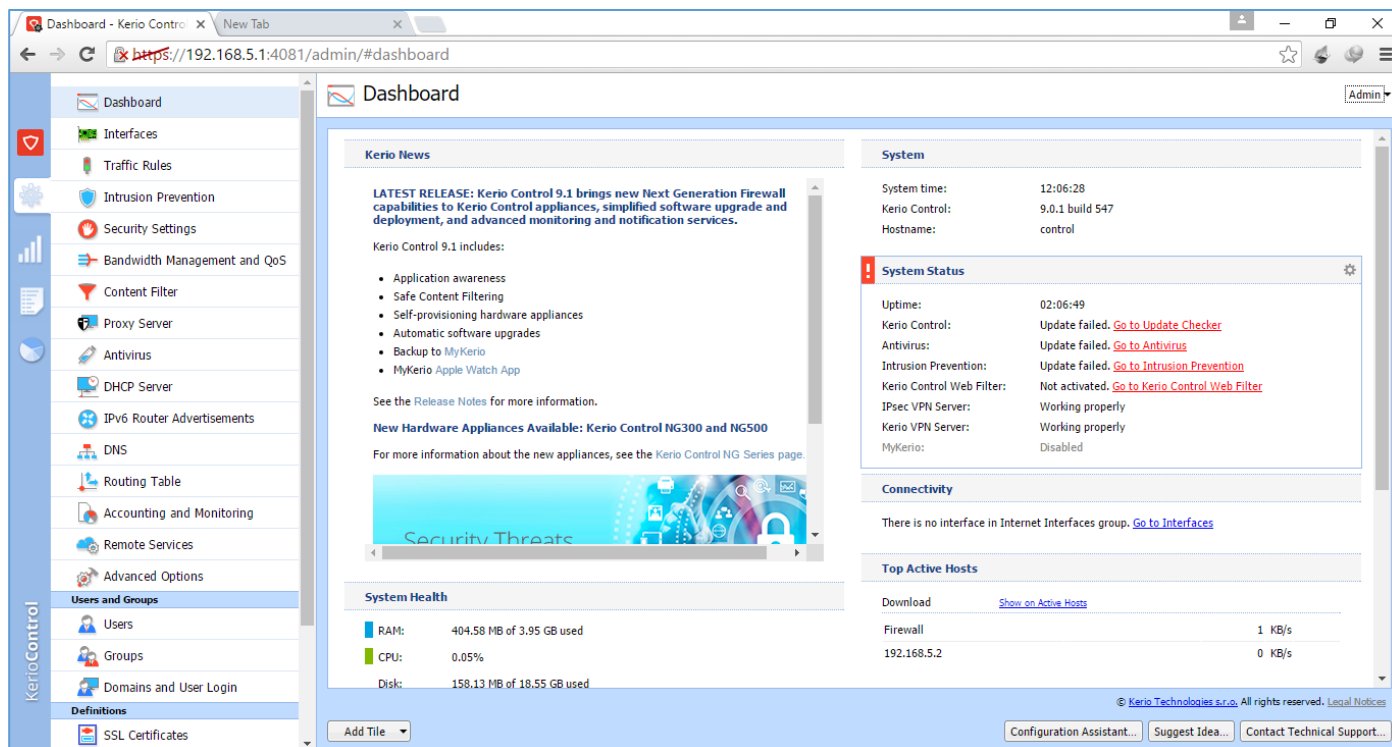


بعد از اجرای آدرس کریو، اولین صفحه‌ای که به شما نمایش داده می‌شود، شکل روبرو است. در این صفحه، اگر تیک گزینه‌ی **Allow kerio...** را انتخاب کنید، یک سری اطلاعات از سیستم شما برای سایت کریو ارسال خواهد شد، این در صورتی خوب است که سیستم شما کرک شده نباشد، اگر کریو شما کرک شده است، بهتر است تیک گزینه‌ی مورد نظر را بردارید و بر روی **Next** کلیک کنید.

در این قسمت باید یک رمز عبور خوب برای صفحه‌ی مدیریتی خود وارد کنید، بعد از آن می‌توانید برای اینکه پیام‌های کریو را در ایمیل خود داشته باشید، تیک گزینه‌ی **Do you...** را انتخاب و آدرس ایمیل خود را وارد کنید و در قسمت آخر نیز، تیک گزینه‌ی **Allow remote...** را بردارید تا کریوی شما به سایت کریو متصل نشود.

بر روی **Finish** کلیک کنید.

بعد از اینکه بر روی **Finish** کلیک کردید، صفحه‌ی ورود به شما نمایش داده می‌شود که برای ورود باید نام کاربری **Admin** را به همراه رمز عبوری که در قسمت قبل وارد کردید را در این قسمت وارد و بر روی **Login** کلیک کنید.



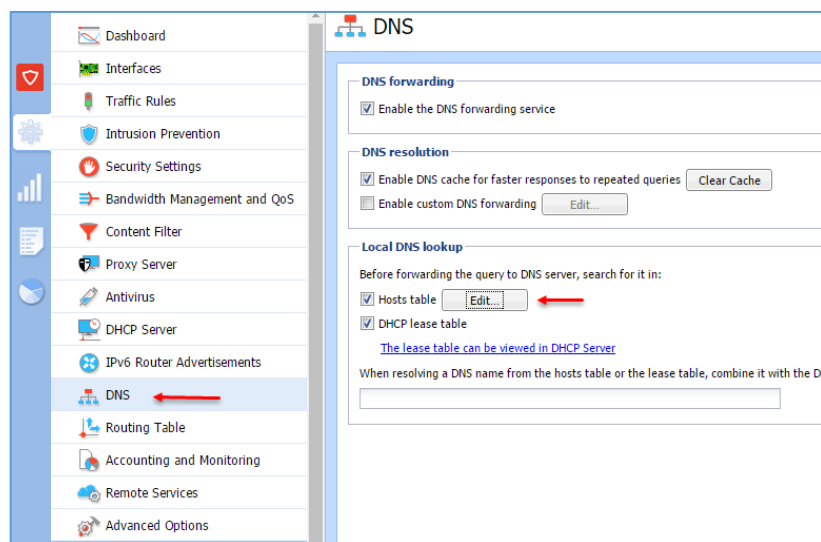
بعد از ورود، اولین صفحه‌ای که مشاهده می‌کنید، صفحه‌ای شبیه به شکل بالا است که نشان‌دهنده‌ی آماده‌بودن کریو برای شروع کار است.

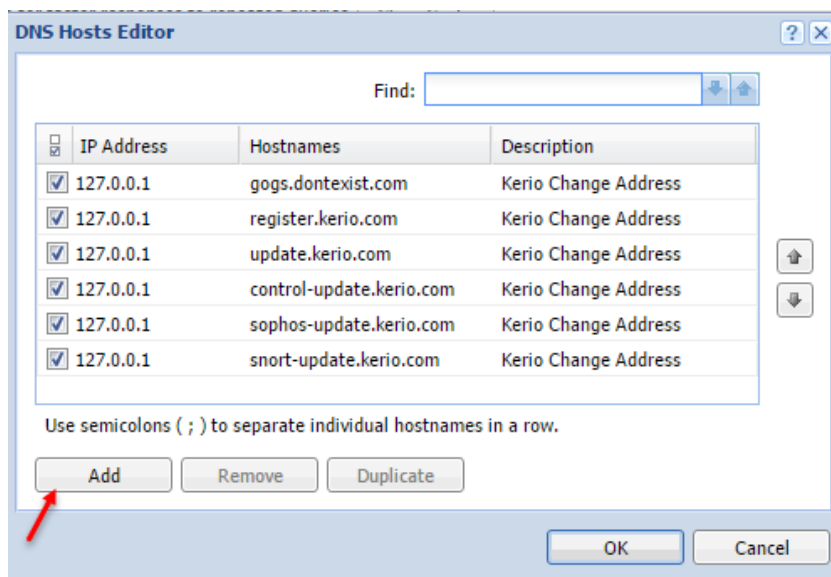
لایسنس کریو:

قبل از اینکه سرور کریو را به اینترنت متصل کنید، اگر چنانچه سرور شما کرک شده باشد باید یک‌سری رول در

قسمت DNS آن وارد کنید تا کریو نتواند خود را آپدیت کند و لایسنس خود را از دست دهد، برای این کار به صورت زیر عمل کنید.

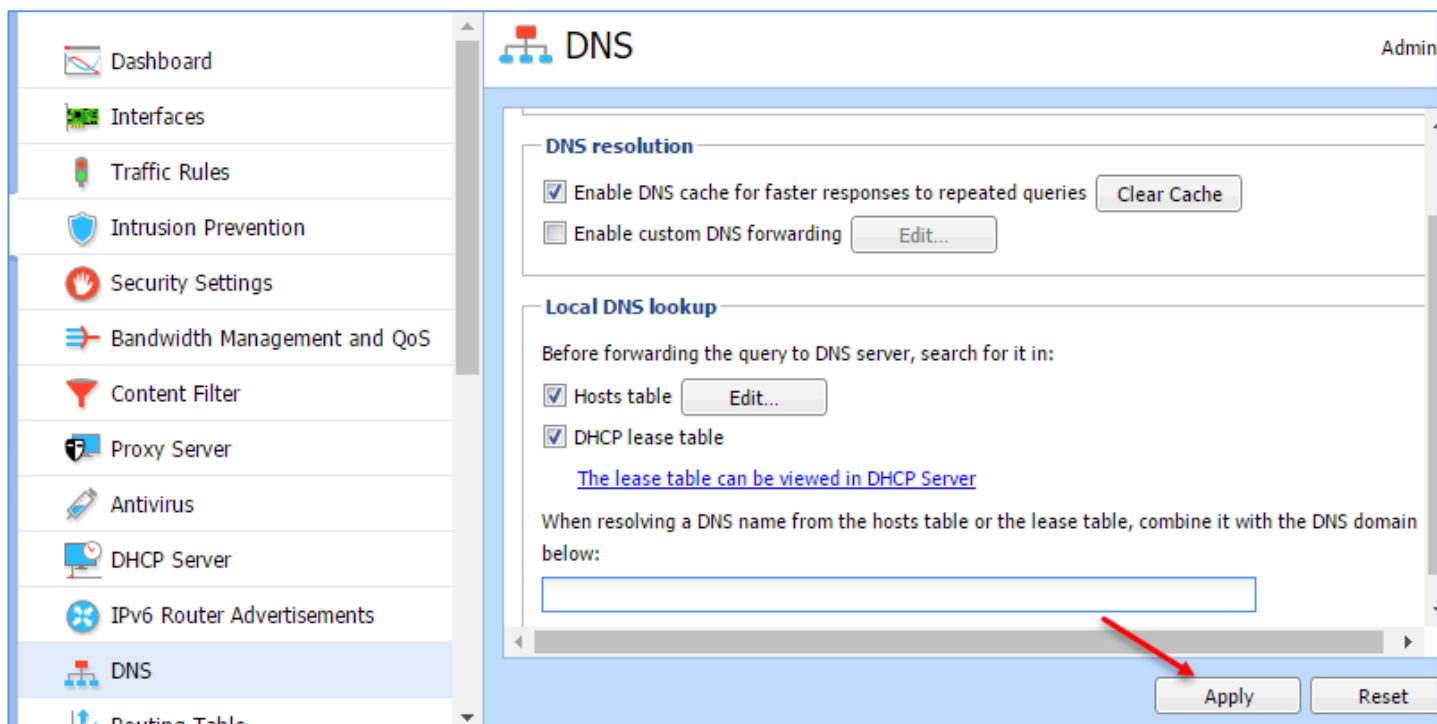
در قسمت مدیریتی از سمت چپ بر روی DNS کلیک کنید و در صفحه‌ی باز شده و در قسمت Local DNS Lookup بر روی Edit کلیک کنید تا شکل بعد ظاهر شود.





در این صفحه با کلیک بر روی **Add** باید به مانند شکل، آدرس‌های زیر را وارد و بر روی **ok** کلیک کنید:

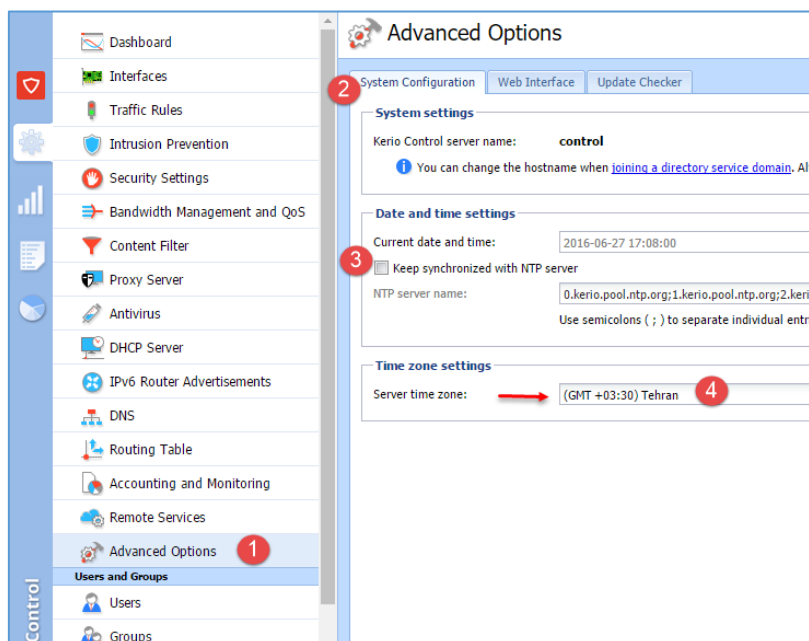
127.0.0.1 gogs.dontexist.com
 127.0.0.1 register.kerio.com
 127.0.0.1 update.kerio.com
 127.0.0.1 control-update.kerio.com
 127.0.0.1 sophos-update.kerio.com
 127.0.0.1 snort-update.kerio.com



بعد از اعمال آدرس‌ها بر روی **Apply** کلیک کنید تا اطلاعات ذخیره شود.

تنظیم ساعت و تاریخ:

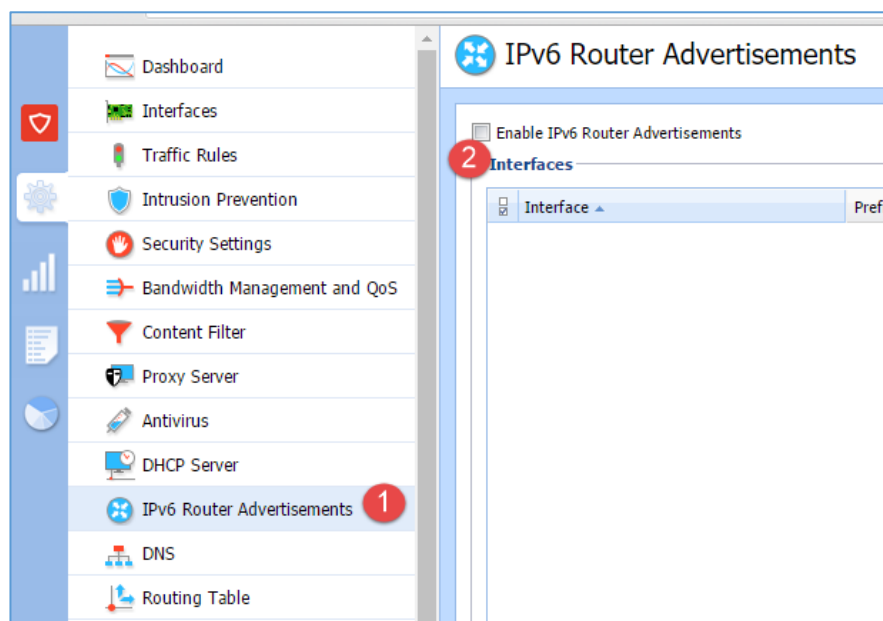
بعد از انجام کارهای قبلی، برای شروع کار با کریو باید ابتدا، ساعت و تاریخ آن را تنظیم کنید، برای این کار به مانند زیر عمل کنید.



در صفحه‌ی روبرو بر روی گزینه‌ی **Advanced Options** کلیک کنید و بعد وارد تب **System Configuration** شوید؛ در این قسمت اگر شما در شبکه‌ی خود از سرور **NTP** استفاده می‌کنید، می‌توانید در قسمت شماره‌ی ۳، تیک گزینه‌ی مورد نظر را انتخاب و آدرس سرور را برای دریافت اطلاعات تاریخ و زمان وارد کنید، البته به صورت پیش‌فرض چند آدرس وارد شده

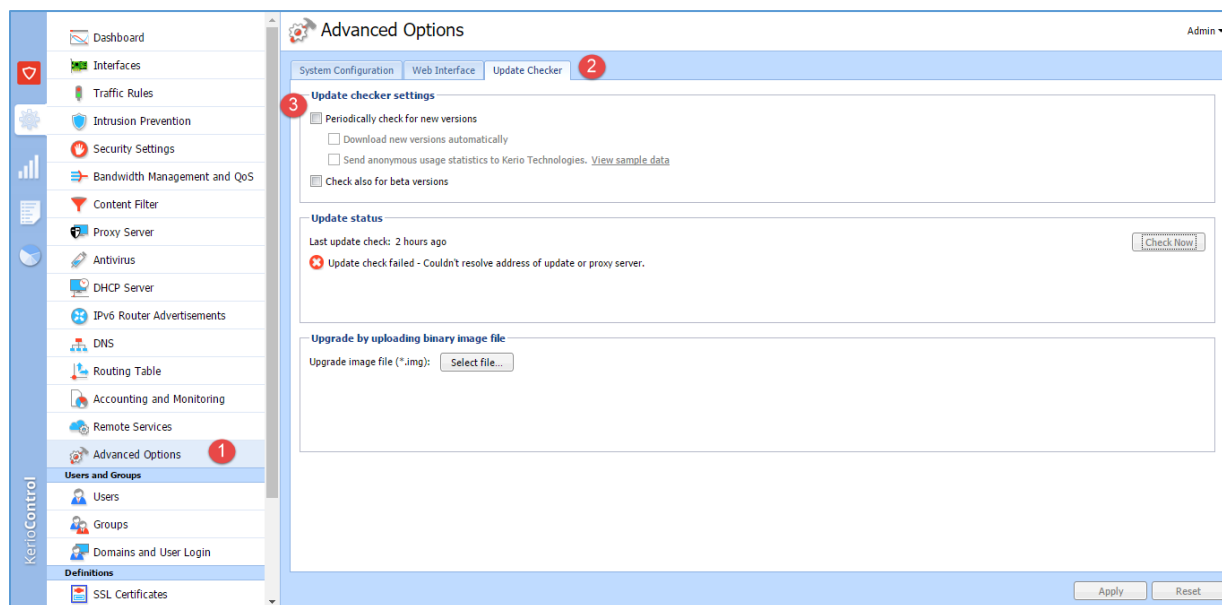
است. در قسمت شماره‌ی ۴ باید منطقه‌ی زمانی خود را بر روی تهران قرار دهید تا ساعت به درستی تنظیم شود، بعد از این کار بر روی **Apply** کلیک کنید تا تنظیمات اعمال شود.

غیرفعال کردن سرویس IPv6:



اگر در شبکه‌ی خود از آدرس **IP**، ورژن ۶ استفاده نمی‌کنید، بهتر است که سرویس آن را غیرفعال کنید تا بار کاری کمتری روی سرور اعمال شود، برای این کار باید از سمت چپ بر روی گزینه‌ی ۱ کلیک کنید و تیک گزینه‌ی ۲ را بردارید تا سرویس **IPv6** غیرفعال شود و در پایان نیز بر روی **Apply** کلیک کنید.

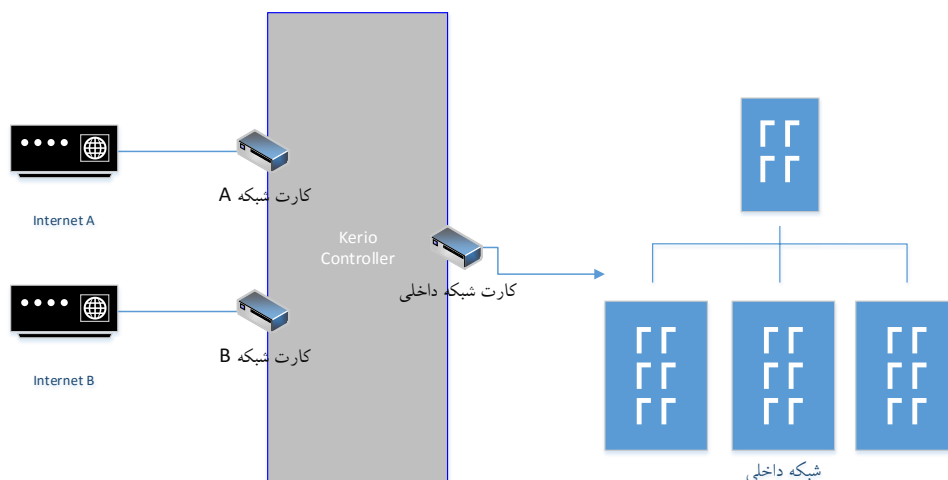
غیرفعال کردن سرویس Update:



برای جلوگیری از **update** نشدن کریو، بر روی گزینه‌ی یک، یعنی **Advanced options** کلیک کنید و در صفحه‌ی باز شده، وارد تب **Update Checker** شوید و تیک گزینه‌ی ۳ را بردارید و بر روی **Apply** کلیک کنید.

وارد کردن اینترنت به کریو:

برای ورود اینترنت باید یک کارت شبکه‌ی دیگر را به ماشین مجازی خود اضافه کنید؛ در سیستم واقعی هم باید به تعداد خط اینترنت، کارت شبکه به سیستم اضافه کنید، برای درک بهتر این موضوع به شکل زیر توجه کنید:

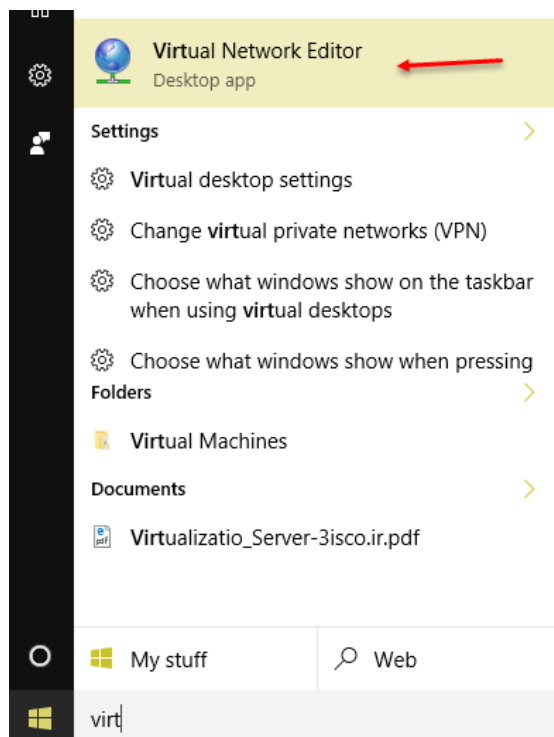


در شکل صفحه‌ی قبل، دو خط اینترنت داریم که برای ورود آن به کریو باید دو کارت شبکه به آن اضافه کنیم و دو خط اینترنت را به آن‌ها متصل کنیم و بعد، تنظیماتی در کریو انجام دهیم و اینترنت را از طریق کارت شبکه‌ی داخلی به کاربران خود تخصیص دهیم.

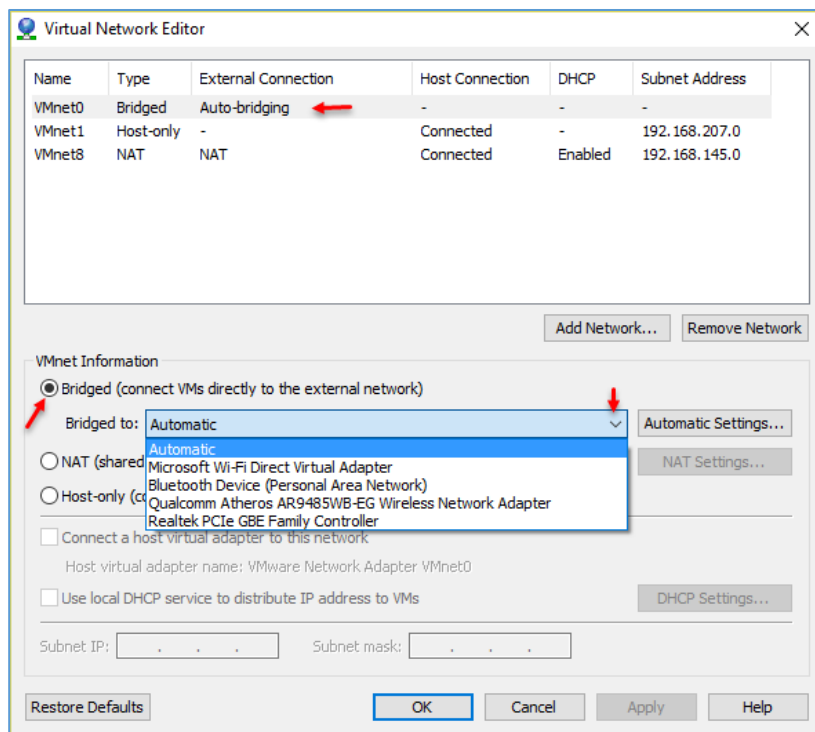
برای شروع کار از یک خط اینترنت استفاده می‌کنیم و آن را به کریو متصل می‌کنیم؛ برای اضافه‌کردن کارت شبکه به ماشین مجازی به صورت زیر عمل کنید:



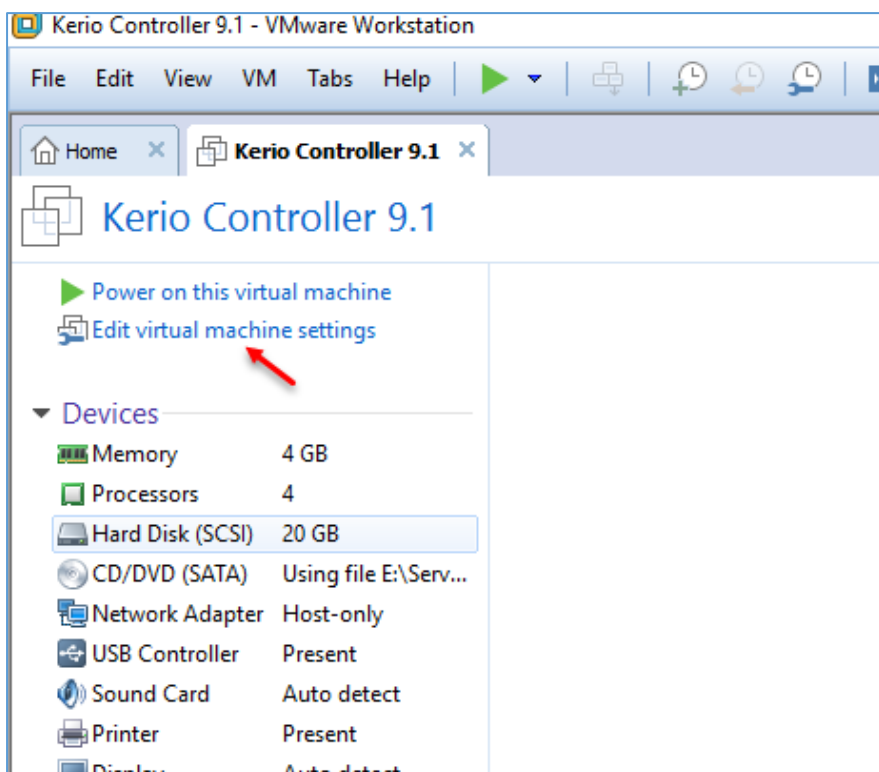
ابتدا سرور کریو را خاموش کنید، برای اینکه به صورت نرم‌افزاری سرور را خاموش کنید باید وارد سرور شوید و در قسمت تنظیمات، گزینه‌ی Shutdown را انتخاب و بر روی کلید F8 فشار دهید تا سرور کریو خاموش شود.



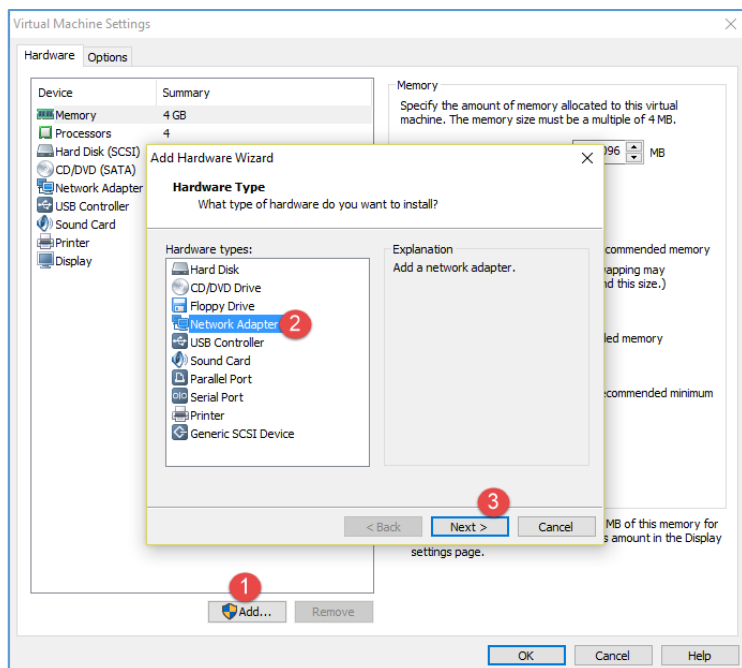
برای تنظیم کارت شبکه‌ی مجازی برای ارتباط با کارت شبکه‌ی واقعی باید دوباره وارد Virtual Network Editor شوید و تنظیمات مورد نظر را انجام دهید.



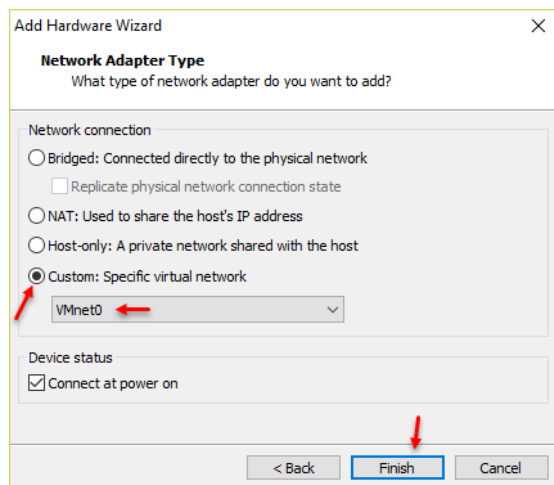
طبق شکل، کارت شبکه‌ی VMnet0 از نوع **Bridged** است که این نوع کارت شبکه به‌عنوان پلی بین کارت شبکه‌ی اصلی و ماشین مجازی شما است؛ بعد از انتخاب در قسمت پایین صفحه و از قسمت **Bridged to** بر روی لیست کشویی کلیک کنید، همان‌طور که مشاهده می‌کنید، تعدادی کارت شبکه مشخص شده است، شما باید همان کارت شبکه‌ای را انتخاب کنید که به اینترنت متصل است و بعد از این کار بر روی **ok** کلیک کنید.



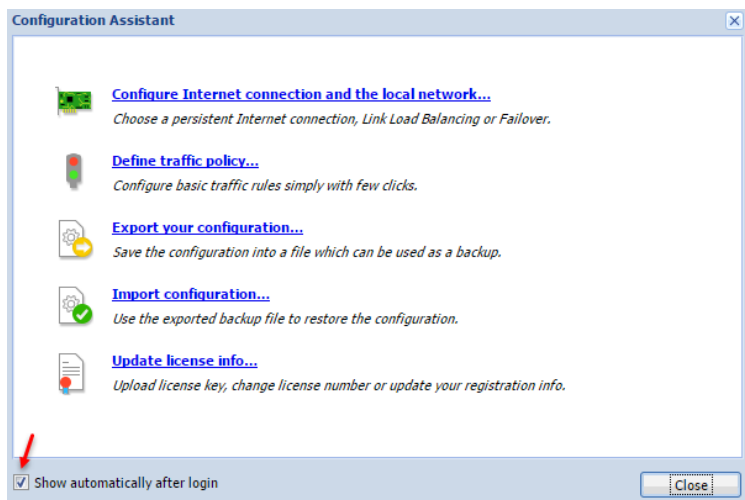
در این صفحه در نرم‌افزار VMware بر روی گزینه‌ی **Edit virtual machine settings** کلیک کنید تا بتوانید کارت شبکه جدید را به سرور کریو اضافه کنید.



در این صفحه برای اضافه کردن کارت شبکه بر روی Add کلیک کنید و از لیست مورد نظر، گزینهی Network Adapter را انتخاب و بر روی Next کلیک کنید.



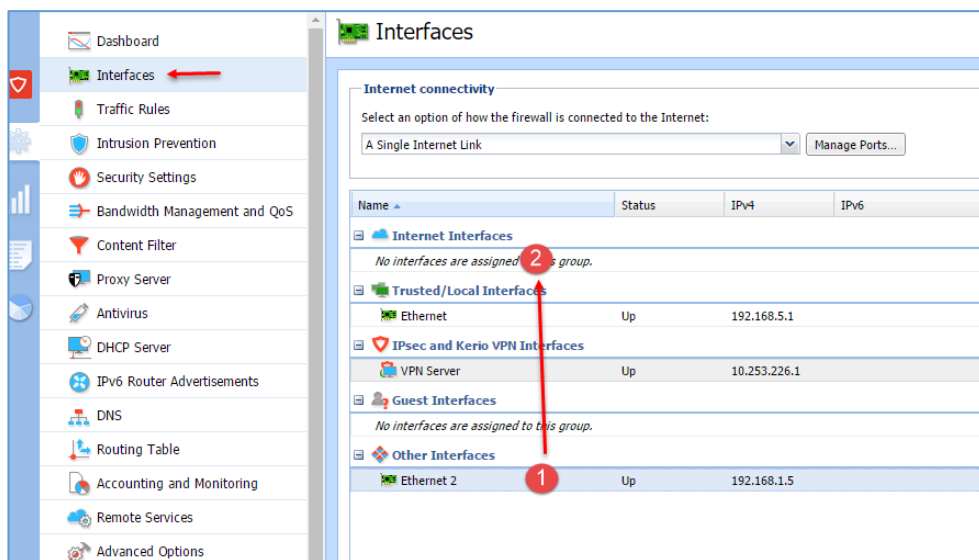
در این شکل، گزینهی Custom را انتخاب و از لیست مورد نظر نیز گزینهی VMnet0 را انتخاب کنید.



بعد از اینکه کارت شبکه را تنظیم کردید، کریو را روشن کنید تا تنظیمات مربوط به کارت شبکهی جدید را انجام دهیم.

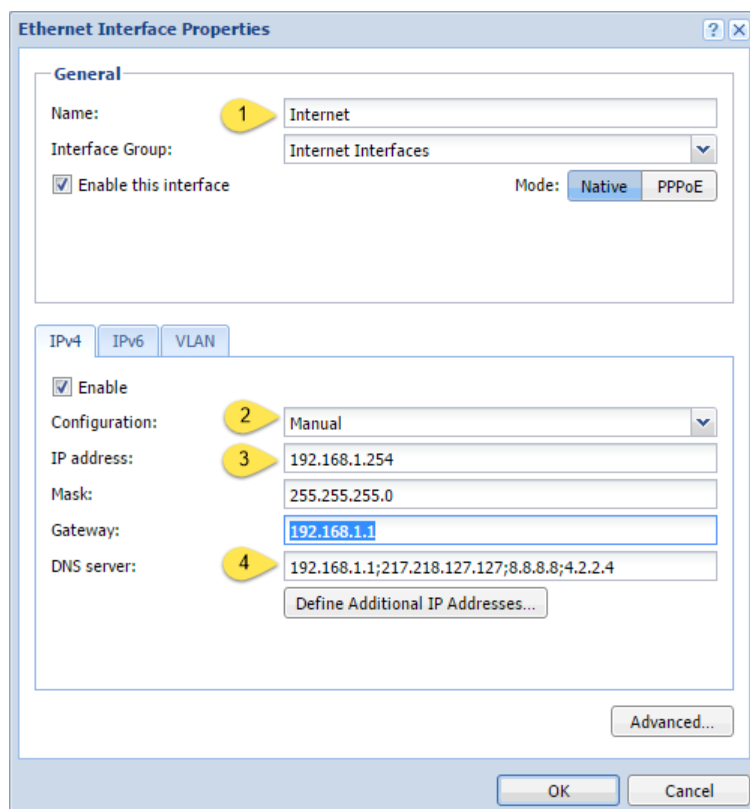
بعد از اجرای صفحهی مدیریتی کریو، صفحهی جدیدی به صورت اتومات اجرا می شود که یک سری گزینهها را برای مدیریت اینترنت به شما ارائه می دهد.

توجه داشته باشید در این کتاب از یک مودم که به صورت PPPoE به اینترنت متصل است، استفاده شده است که به این علت، اینترنت به صورت مستقیم وارد کریو می شود.

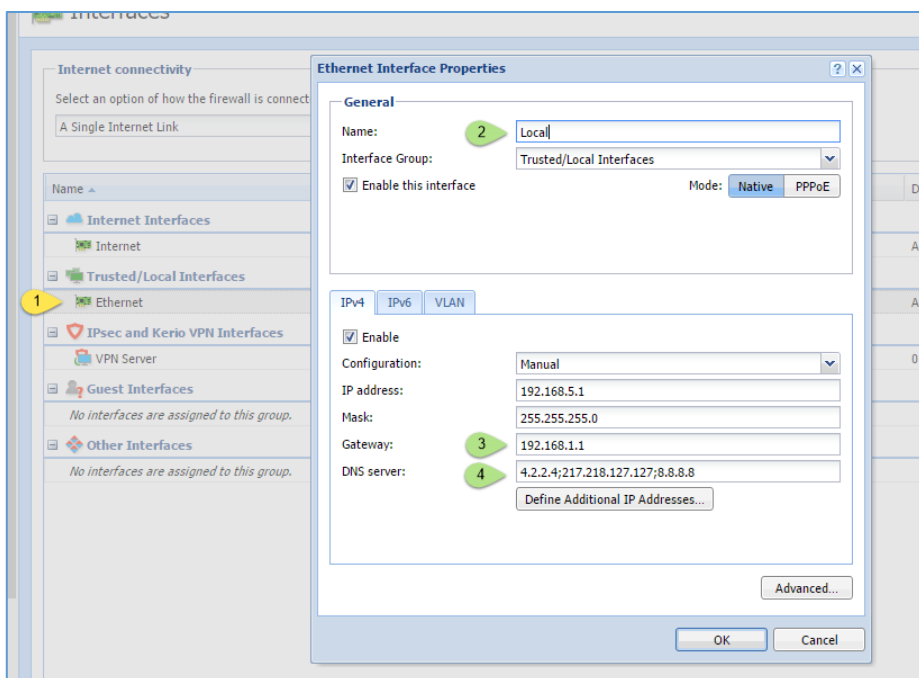


به مانند شکل روبرو از سمت چپ بر روی Interface کلیک کنید، اگر به خوبی دقت کنید، یک کارت شبکه‌ی جدید در قسمت شماره‌ی یک اضافه شده است که در قسمت Other Interfaces مشاهده می‌کنید، چون این کارت شبکه مربوط به اینترنت

است آن را کشیده و در قسمت شماره‌ی ۲، یعنی Internet Interface رها کنید، بعد از این کار بر روی کارت شبکه‌ی مورد نظر دوبار کلیک کنید.

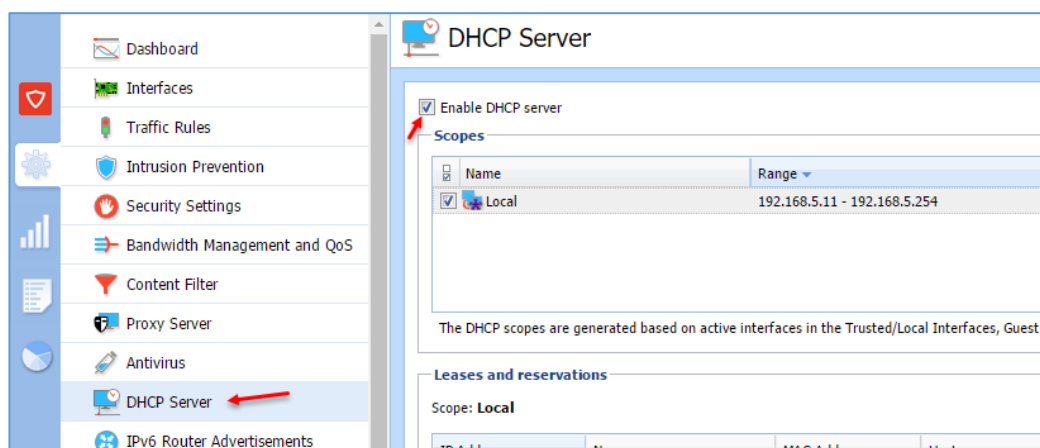


در این صفحه و در قسمت شماره‌ی یک، نام کارت شبکه‌ی خود را به Internet تغییر دهید تا مدیریت آن آسان‌تر باشد؛ در قسمت شماره‌ی دو باید آدرس IP را به صورت دستی وارد کنید، برای همین باید گزینه‌ی Manual را انتخاب کنید و در قسمت شماره‌ی سه، آدرس IP ارتباطی بین کارت شبکه و مودم اینترنت را وارد کنید که در اینجا کارت شبکه‌ی اینترنت IP آدرس ۱۹۲،۱۶۸،۱،۲۵۴ و مودم اینترنت، آدرس ۱۹۲،۱۶۸،۱،۱ داده شده است، در قسمت شماره‌ی چهار، آدرس DNS را وارد کنید و بر روی OK کلیک کنید.



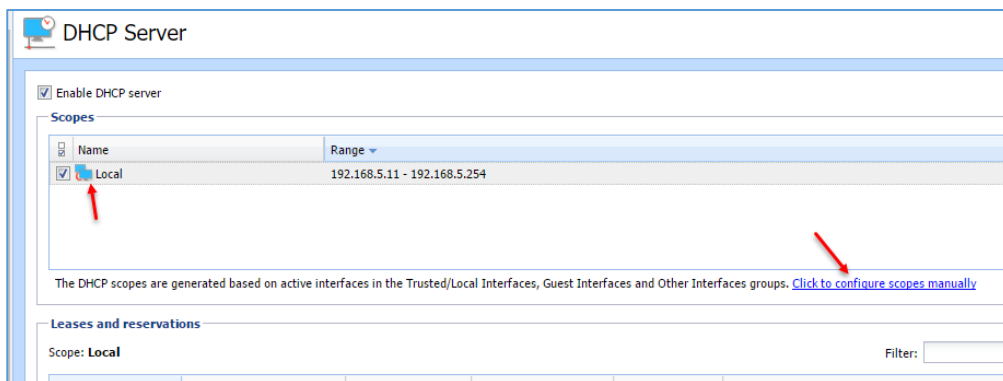
بعد از تنظیم کارت شبکه‌ی اینترنت، در قسمت Trusted/Local Interfaces که مربوط به کارت شبکه‌ی داخلی است بر روی کارت شبکه‌ی قسمت شماره‌ی یک، دو بار کلیک کنید؛ در صفحه‌ی باز شده و در قسمت شماره‌ی دو، نام کارت شبکه‌ی خود را به دلخواه تغییر دهید و در قسمت شماره‌ی ۳ باید آدرس کارت شبکه‌ی اینترنت را که به‌عنوان gateway عمل می‌کند در قسمت

Gateway وارد کنید و در قسمت DNS هم آدرس‌های موردنظر خود را وارد و بر روی OK کلیک کنید، بعد از انجام کارهای بالا، همه چیز آماده است تا کلاینت‌ها بتوانند از طریق کریو دارای اینترنت شوند، اما چگونه یک کلاینت از طریق شبکه، آدرس IP دریافت می‌کند و به اینترنت دسترسی پیدا می‌کند؟، این عمل توسط سرویس DHCP انجام می‌شود که به صورت پیش‌فرض روی Kerio فعال شده است، برای دستیابی به تنظیمات آن باید به آدرس زیر مراجعه کنید:

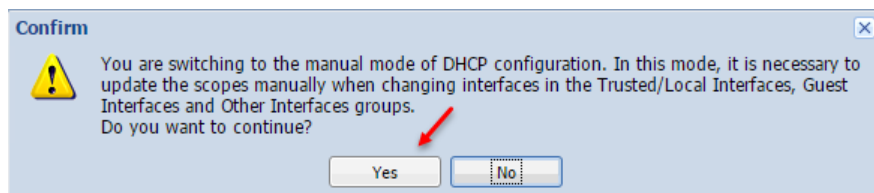


همانطورکه در شکل روبرو مشاهده می‌کنید از سمت چپ، DHCP Server را انتخاب کردیم که به صورت پیش‌فرض، این سرویس روی کارت شبکه‌ی Local فعال شده

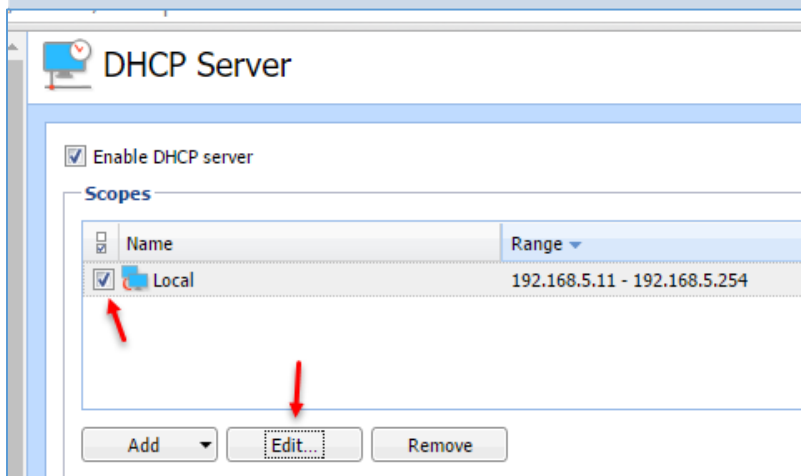
است و رنج IP آن از 192.168.5.11 تا 192.168.5.254 در نظر گرفته شده است، هر کلاینتی که به شبکه متصل شود، یک آدرس IP در همین رنج دریافت خواهد کرد.



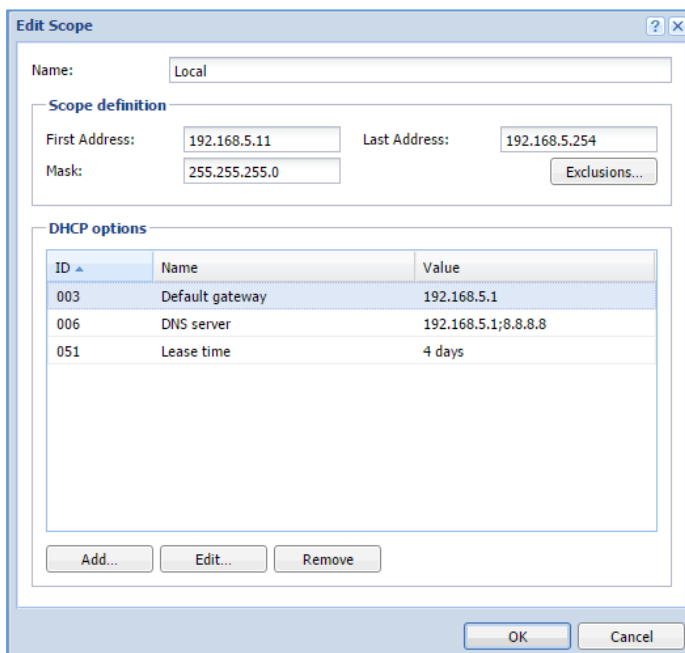
برای اینکه بتوانیم DHCP را به دلخواه خود تنظیم کنیم باید به مانند شکل روبرو در قسمت DHCP بر روی **Click to configure scopes manually** کلیک کنیم



کنیم؛ در این پیغام از ما پرسیده می شود که آیا تمایل دارید به حالت **Manual** بروید یا خیر؟، که باید بر روی **Yes** کلیک کنید.



کارت شبکه‌ی مورد نظر خود را انتخاب و بر روی **Edit** کلیک کنید تا صفحه‌ی بعد ظاهر شود.

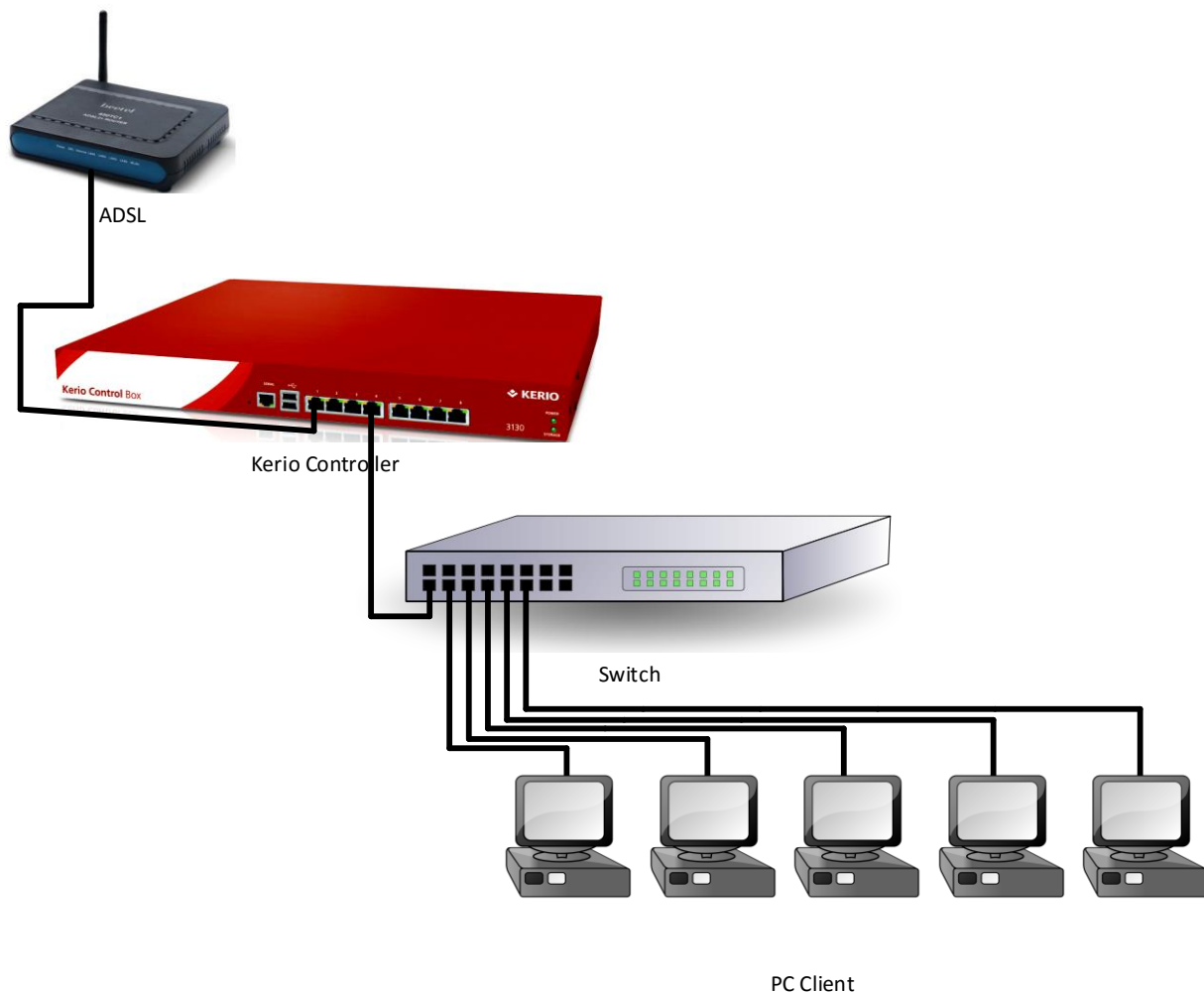


در این صفحه می توانید رنج IP خود را محدودتر کنید، مثلاً از ۱۹۲,۱۶۸,۵,۲۵ تا ۱۹۲,۱۶۸,۵,۵۰ که این کار به شبکه‌ی شما بستگی دارد که چه رنج IP را انتخاب می کنید.

در قسمت **DHCP Options** می توانید تنظیمات مورد نظر خود را تغییر دهید، اگر بخواهید زمان تخصیص یک آدرس به کلاینت را که در این تصویر، **4days** است را تغییر دهید بر روی **Lease time** دوبار کلیک کنید و آن را به ۳۰ روز تغییر دهید، بعد از این کار بر روی **OK** کلیک کنید.

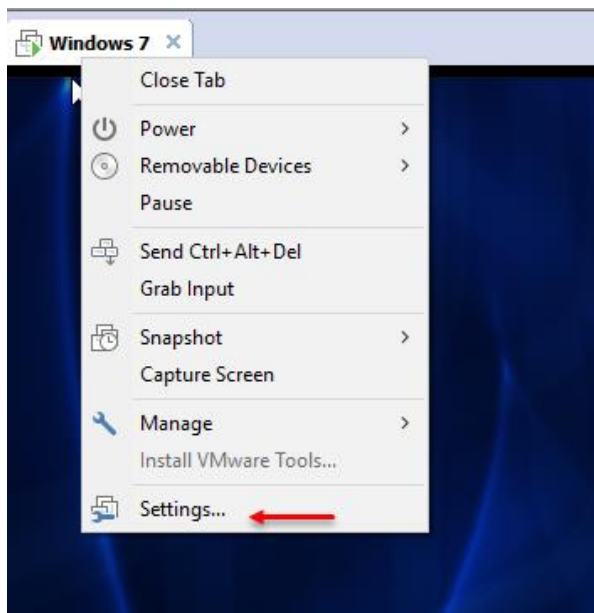
اشتراک گذاری اینترنت با کاربران:

بعد از اینکه کارهای بالا را به خوبی انجام دادید، می‌توانید اینترنت را برای کاربران به اشتراک بگذارید؛ در این کتاب بر روی برنامه‌ی VMware، یک ماشین مجازی راه می‌اندازیم و اینترنت را با این کلاینت به اشتراک می‌گذاریم؛ در شبکه‌ی واقعی نیز دقیقاً به این صورت است؛ برای درک بهتر این موضوع به شکل زیر توجه کنید:

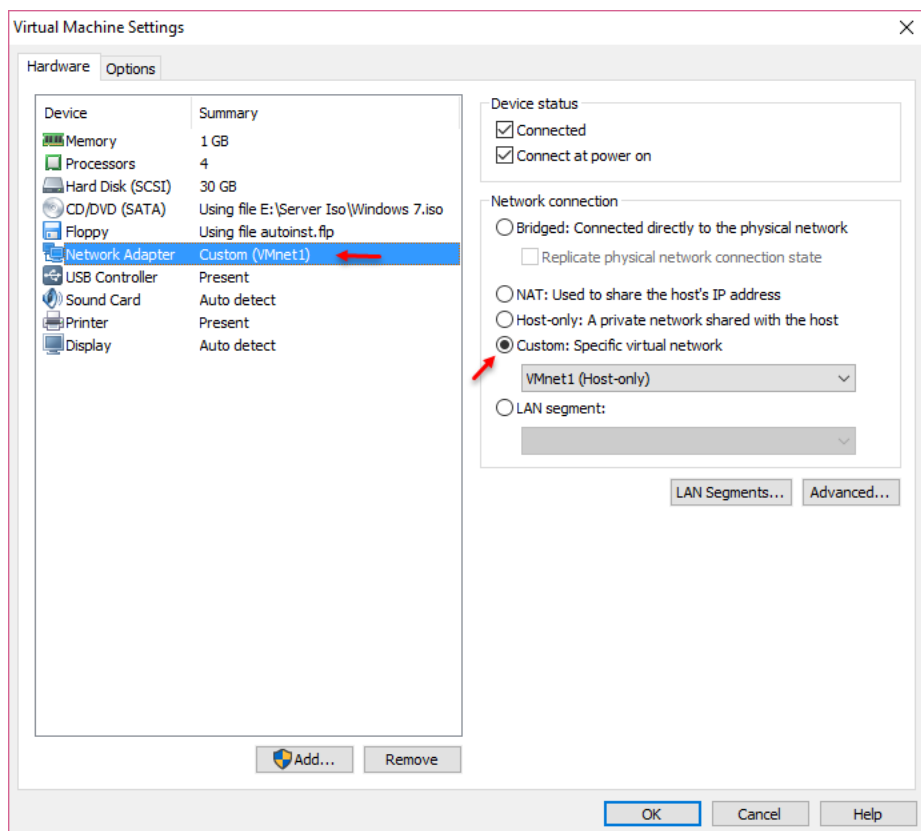


در شکل بالا، طرحی از شبکه را مشاهده می‌کنید، یک مودم ADSL که خط اینترنت را برای ما فراهم می‌کند به یکی از پورت‌های شبکه‌ی سرور کریو متصل شده است که این عمل را در قسمت‌های قبل آموزش دادیم و بعد از آن، از یکی دیگر از پورت‌های شبکه‌ی کریو که اسم آن را در قسمت قبل، به Local تغییر دادیم، یک کابل به سوئیچ متصل کردیم و اگر هر کلاینتی به این سوئیچ متصل شود از سرویس DHCP که در کریو فعال کردیم اطلاعات IP را دریافت خواهد کرد و به اینترنت متصل خواهد شد.

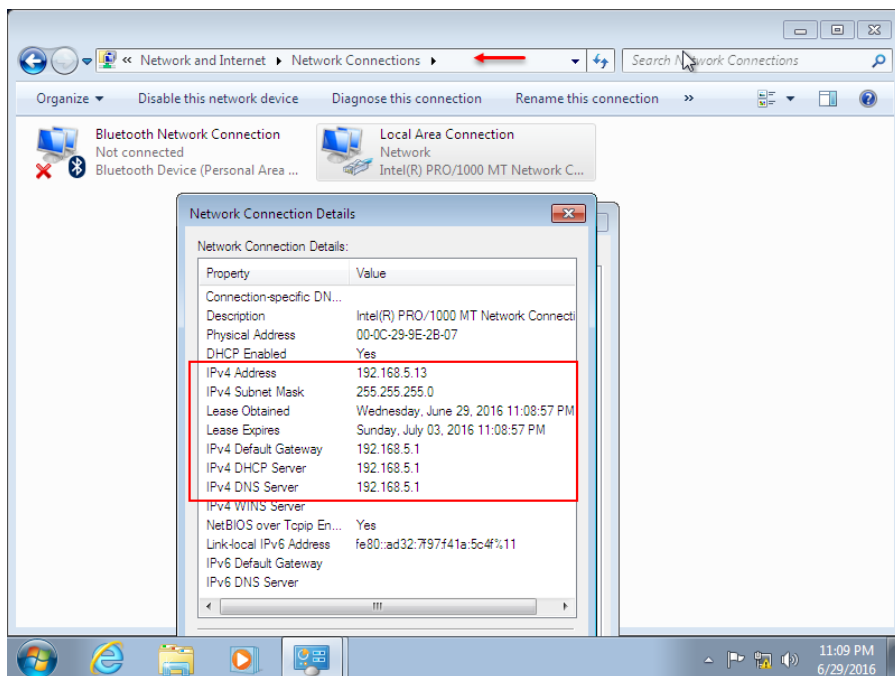
در حال حاضر، یک ماشین مجازی با ویندوز 7 راه می‌اندازیم و آن را به شبکه‌ی Local کریو متصل می‌کنیم تا ببینیم چه اتفاقی رخ می‌دهد. چون قبلاً نحوه‌ی ایجاد ماشین مجازی را توضیح دادیم، دیگر نیازی به توضیح دوباره‌ی آن نیست، تنها نحوه‌ی ارتباط با کارت شبکه‌ی سرور کریو را با هم بررسی می‌کنیم.



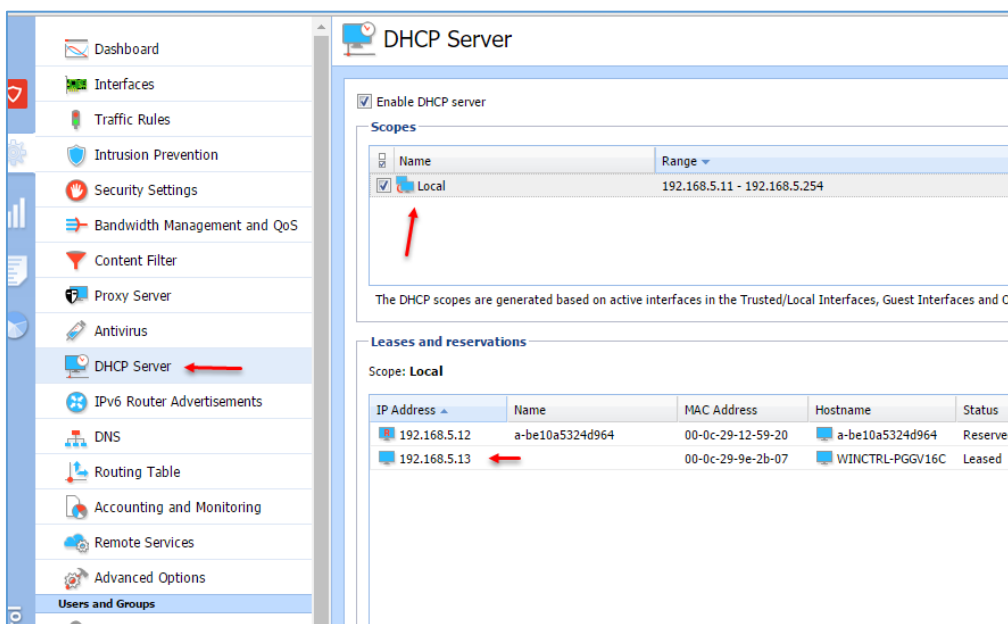
بر روی ماشینی که ایجاد کردید، کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



در این قسمت، کارت شبکه را از سمت چپ انتخاب کنید و از سمت راست باید در قسمت Custom، همان کارت شبکه‌ای را انتخاب کنید که در کریو به‌عنوان Local انتخاب کردید که در اینجا کارت شبکه‌ی VMnet1 که از نوع Host-only است را انتخاب می‌کنیم و بر روی ok کلیک می‌کنیم.



اگر وارد ماشین مجازی خود شوید و وارد قسمت **Network Connection** شوید و اطلاعات کارت شبکه‌ی خود را مشاهده کنید، همانطورکه در شکل روبرو مشاهده می‌کنید، یک آدرس ۱۹۲،۱۶۸،۱،۱۳ به صورت اتوماتیک توسط سرویس **DHCP** کریو به این ماشین داده شده است و این ماشین دارای اینترنت شده است.



برای مشاهده‌ی اطلاعات این کلاینت در سرویس **DHCP** وارد **DHCP** شوید و بر روی کارت شبکه‌ی **Local** به مانند شکل روبرو کلیک کنید، همانطورکه مشاهده می‌کنید، سیستم کلاینت ما به لیست اضافه شده است و IP آن هم ۱۹۲،۱۶۸،۵،۱۳ ست شده

است و نام و مک آدرس کلاینت مورد نظر هم مشخص شده است.

تا به این قسمت کریو را راه‌اندازی کردیم و اینترنت را به کلاینت دادیم و توضیحاتی در مورد سرویس **DHCP** ارائه کردیم.

بررسی Mac Filtering در کریو:

با استفاده از این گزینه، شما می‌توانید سیستم‌هایی که به کریو متصل می‌شوند و از سرویس‌های آن استفاده می‌کنند را مشخص کنید، این گزینه به شما در امنیت شبکه کمک کننده است، در ادامه با نحوه‌ی کارکرد آن آشنا خواهید شد.

```

C:\Users\test>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WINCTRL-PGGU16C
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 24-0A-64-74-35-38
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Local Area Connection:

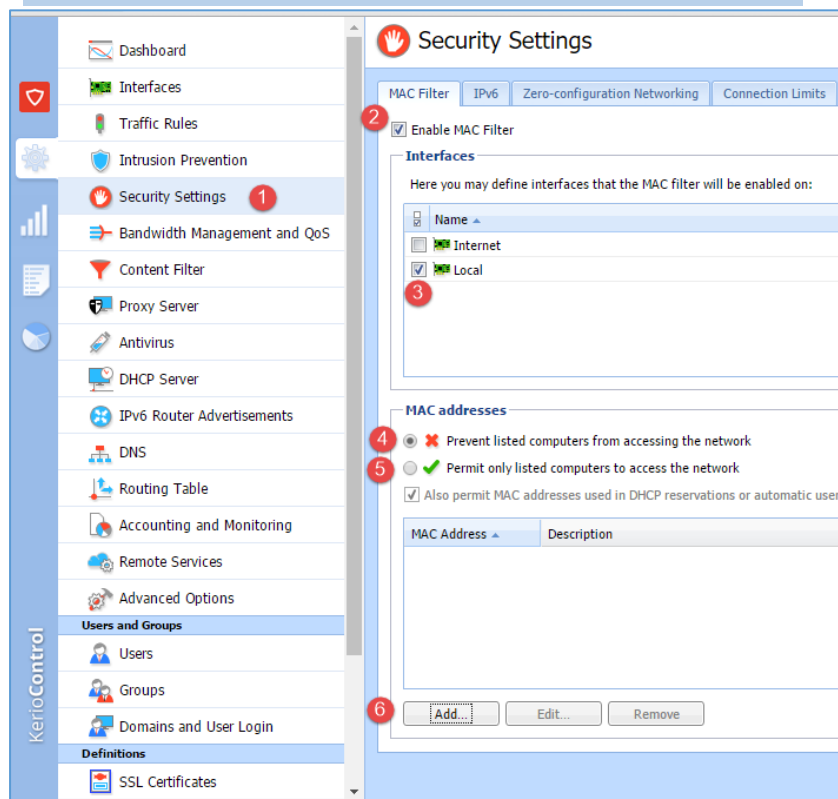
Connection-specific DNS Suffix . . . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-9E-2B-07
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ad32:7f97:f41a:5c4f%11(Preferred)
IPv4 Address. . . . . : 192.168.5.13(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 29, 2016 11:08:58 PM
Lease Expires . . . . . : Monday, July 04, 2016 10:17:33 PM
Default Gateway . . . . . : 192.168.5.1
DHCP Server . . . . . : 192.168.5.1
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-06-63-C2-00-0C-29-9E-2B-07

DNS Servers . . . . . : 192.168.5.1
NetBIOS over Tcpi. . . . . : Enabled

Tunnel adapter isatap.{6518B09F-8061-4754-93AC-B31F03B5DF41}:

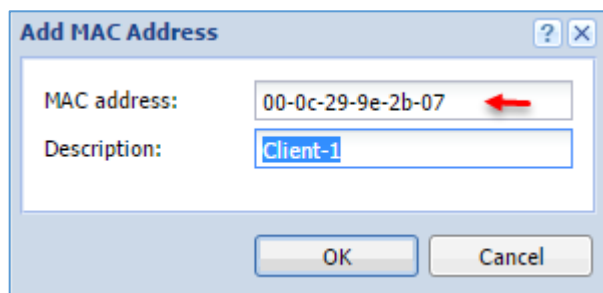
Media State . . . . . : Media disconnected
  
```

برای بدست آوردن مک آدرس کلاینت‌ها به مانند شکل روبرو در ویندوز، CMD را اجرا کنید و دستور IPConfig /all را اجرا کنید، باید نام کارت شبکه‌ی خود را بدانید که نام پیش‌فرض Local Area Connation است، اگر به شکل توجه کنید، جلوی Physical Address، آدرس مک مشخص شده است؛ این آدرس را کپی کنید تا در ادامه از آن استفاده کنیم.

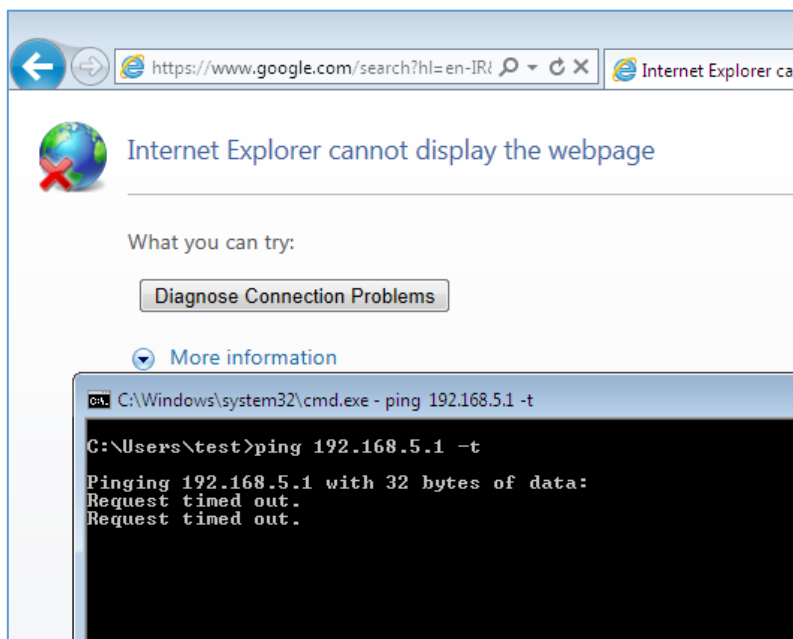


بعد از پیدا کردن Mac Address وارد کریو شوید و بعد وارد قسمت Security Settings شوید، سپس وارد تب MAC Filtering شوید، در این تب برای فعال کردن این قابلیت باید تیک گزینه‌ی ۲ را انتخاب کنید و در مهمترین بخش، یعنی شماره‌ی ۳ باید کارت شبکه‌ای را انتخاب کنید که به شبکه‌ی داخلی متصل است و کاربران از این طریق، IP دریافت می‌کنند و به اینترنت متصل می‌شوند که در این کتاب، کارت شبکه Local است در قسمت شماره‌ی ۴، اگر گزینه‌ی Prevent... را انتخاب کنید، تمام

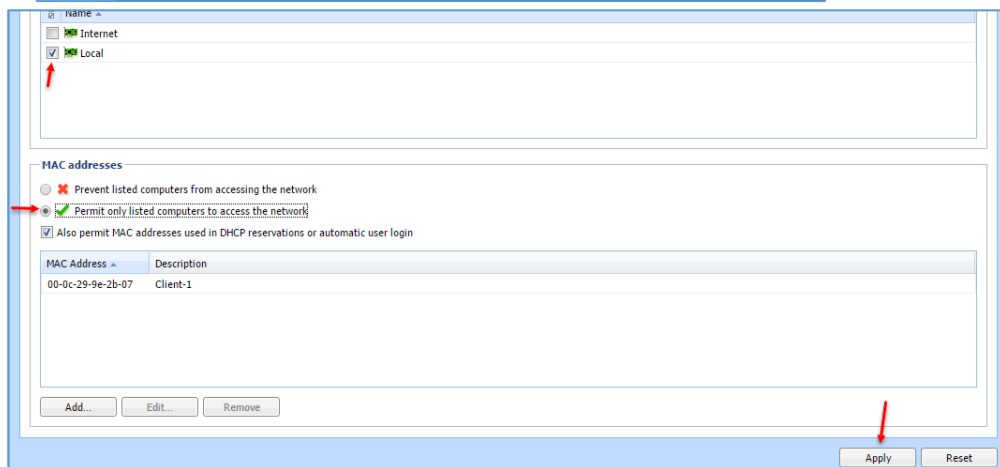
سیستم‌هایی را که در لیست زیری **ADD** می‌کنید، توانایی دسترسی به شبکه را نخواهند داشت و گزینه‌ی ۵، برعکس گزینه‌ی ۴ است و با فعال کردن آن، سیستم‌هایی را که در لیست وارد می‌کنید، توانایی دستیابی به شبکه را دارا هستند؛ برای تست مک آدرسی که در قسمت قبل بدست آوردیم، با کلیک بر روی **Add** در قسمت شماره‌ی ۶ تست می‌گیریم.



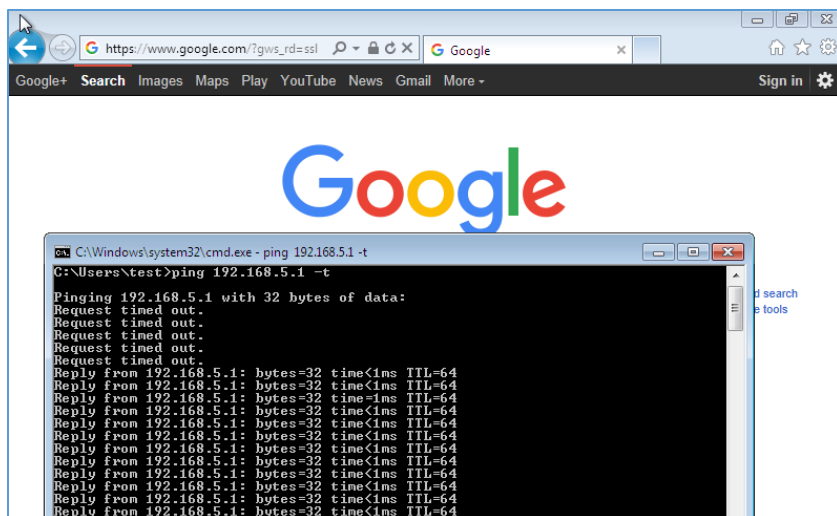
به مانند شکل روبرو، **Mac Address** را وارد کنید و توضیحاتی را در مورد کلاینت خود وارد و بر روی **ok** کلیک کنید؛ بعد از این کار بر روی **Apply** در سمت راست و پایین صفحه کلیک کنید تا تغییرات ذخیره شود.



با این کار کلاینتی که آدرس **MAC** آن را وارد کردید، دیگر به شبکه دسترسی نخواهد داشت که این موضوع را در شکل روبرو مشاهده می‌کنید؛ با دستور **Ping** ارتباط روتر کریو را بررسی کردیم که با پیام **Reauest Timed out** مواجه شدیم، اگر در همین حالت **MAC** آدرس مورد نظر را در لیست **Permit** قرار دهیم، دوباره کلاینت می‌تواند به سرور متصل شود.



به مانند شکل، گزینه‌ی **Permit** را انتخاب و بر روی **Apply** کلیک کنید تا اطلاعات ذخیره شود.



همانطور که مشاهده می‌کنید، دوباره ارتباط کلاینت با روتر کریو برقرار شده است، پس با این کار نتیجه می‌گیریم برای حفظ امنیت شبکه‌ی خود و جلوگیری از دسترسی کلاینت‌های غیر مجاز به شبکه این کار می‌تواند به شما کمک کند.

بررسی Traffic Rule

Name	Source	Destination	Service	IP version	Action	Translation
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow	
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow	
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host
Local traffic	Firewall	Firewall	Any	Any	Allow	
Firewall traffic	Trusted/Local Interfaces VPN clients All VPN tunnels	Trusted/Local Interfac...	Any	Any	Allow	
Guests traffic	Firewall	Firewall	Any	Any	Allow	
Block other traffic	Guest Interfaces	Firewall	Guest services	Any	Allow	
	Any	Any	Any	Any	Drop	

بخش Traffic Rules، یکی از بخش‌های مهم در کنترل ترافیک شبکه‌ی یک سازمان است که اگر خوب کانفیگ نشود، می‌تواند امنیت شبکه را زیر سؤال ببرد. در شکل بالا، قسمت Traffic Rules را مشاهده می‌کنید که به صورت پیش‌فرض، Rule‌هایی توسط خود شرکت کریو ایجاد شده است که هر کدام برای کار خاصی ایجاد شده است که در ادامه آنها را بررسی خواهیم کرد.

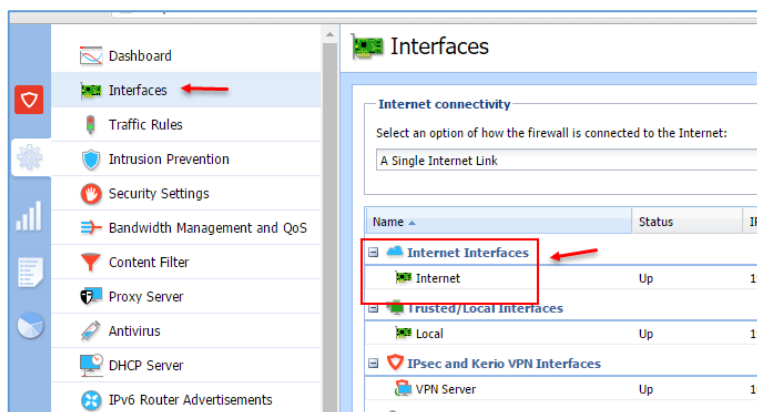
Name	Source	Destination	Service	IP version	Action
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow
Firewall traffic	Firewall	Any	Any	Any	Allow
Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow
Block other traffic	Any	Any	Any	Any	Drop

در این قسمت، تمامی گزینه‌ها را در Traffic Rules مشاهده می‌کنید؛ در قسمت شماره ۱، گزینه‌ی VPN Services را مشاهده می‌کنید که به

صورت پیش‌فرض غیرفعال است که اگر بخواهید در شبکه‌ی خود VPN ایجاد کنید باید این گزینه را فعال کنید و در قسمت Action باید گزینه‌ی Allow را انتخاب کنید، برای انتخاب گزینه‌ها در هر قسمت باید بر روی گزینه‌ی مورد نظر، دو بار کلیک کنید تا صفحه‌ی دیگری باز شود و در آن صفحه باید گزینه‌ها را انتخاب کنید.

گزینه‌ی دوم، Web Services برای کنترل سایت‌هایی با پروتکل HTTP و HTTPS است که در ادامه، بیشتر با آن کار خواهیم کرد.

گزینه‌ی سوم، Internet Access است که تمام پورت‌ها و کلاینت‌هایی که در قسمت Source تعریف می‌شوند، می‌توانند به اینترنت که در قسمت Destination تعریف شده است، دسترسی داشته باشند، اگر دقت

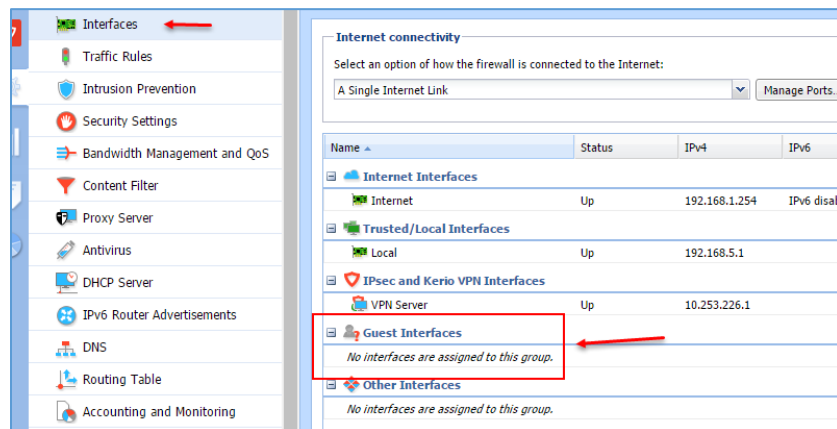


کنید در قسمت Destination، گزینه‌ی internet interface وارد شده است که این گزینه، مربوط به قسمت Interfaces است که در شکل روبرو مشاهده می‌کنید، در این قسمت کارت شبکه اینترنت وجود دارد، یعنی اینکه هر چیزی که در قسمت Source وارد کنیم، دسترسی مستقیم به اینترنت دارند و به خاطر

همین موضوع بود که کلاینتی که به کریو متصل شد به صورت مستقیم به اینترنت متصل شده است.

برمی‌گردیم به شکل اول صفحه و گزینه‌ی چهارم که **Local Traffic** است را بررسی می‌کنیم، این گزینه همانطور که از نام آن پیداست به شبکه‌ی داخلی مربوط می‌شود دسترسی گزینه‌های مشخص شده را به هم باز کرده است.

در قسمت شماره‌ی پنج هم دسترسی **Rule** هایی که در ادامه در **Firewall** تعریف می‌کنیم به تمام سرویس‌های شبکه باز شده است.



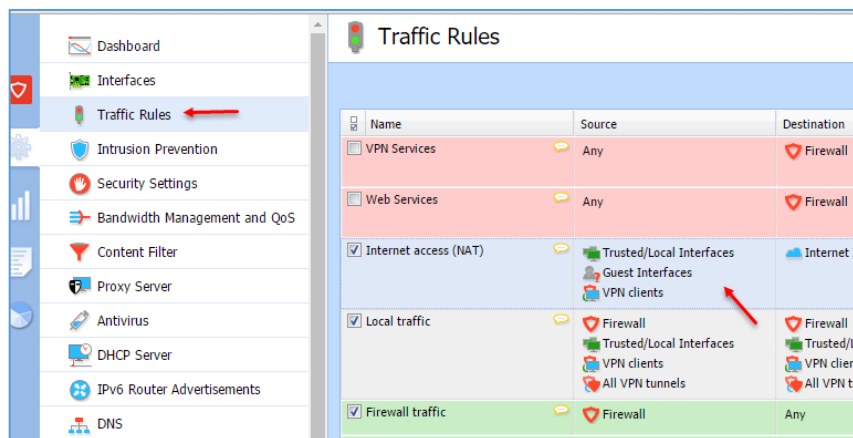
در قسمت شماره‌ی شش، **Guests** در قسمت **Traffic** را مشاهده می‌کنید که این گزینه به اینترنت‌فیس **Guest** در قسمت **interface** اشاره دارد که در شکل روبرو مشاهده می‌کنید، اصولاً برای کاربران مهمان این **Interface** را در نظر گرفتند، زمانی که کارت شبکه‌ای را

در این قسمت قرار دهید و کاربران به آن متصل شوند، برای ورود به اینترنت، ابتدا، یک صفحه‌ی دسترسی با نام کریو برای آن‌ها باز می‌شود که بعد از تأیید کاربر می‌توانند به اینترنت دسترسی داشته باشند؛ این گزینه را می‌توان چیزی شبیه به سرویس **Hotspot** در نظر گرفت.

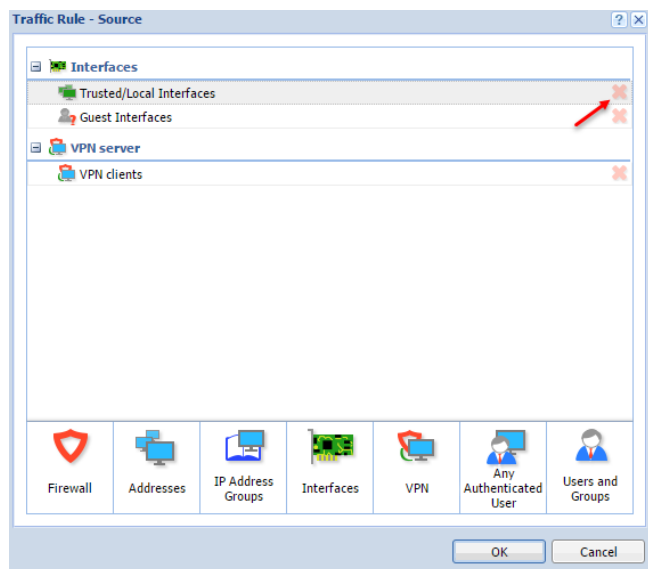
در قسمت آخر، شماره‌ی هفت نیز تمام ترافیک‌هایی که در شبکه وجود دارد، به جز آن‌هایی که در بالای آن تعریف شده‌اند، قطع خواهند شد.

برای تست، گزینه‌های **Traffic Rule** یکی از آن‌ها را با هم بررسی می‌کنیم.

قطع اینترنت کاربران و شخصی سازی آن:

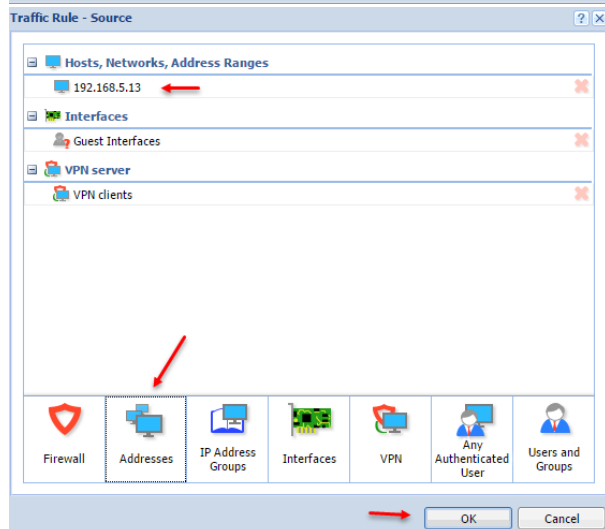


برای اینکه تمام اینترنت کاربران در شبکه را قطع کنیم، کافی است به مانند شکل وارد قسمت Traffic Rule شویم و در Source مربوط به Internet Access دوبار کلیک کنیم.



در این صفحه بر روی آیکون ضربدر جلوی Trusted/Local Interface و بر روی OK کلیک کنید و سپس بر روی Apply کلیک کنید، با این کار تمام کاربران شبکه اینترنت نخواهد داشت.

حالا برای اینکه کلاینت خاصی را اینترنت دار کنیم باید در همین صفحه بر روی Addresses کلیک کنیم و IP Address آن را در این قسمت وارد کنیم، البته گزینه‌های دیگری هم وجود دارد که در ادامه روی آن‌ها بحث خواهیم کرد.



همانطور که مشاهده می‌کنید با کلیک بر روی Addresses آدرس مورد نظر را به لیست اضافه کردیم و بعد از کلیک بر روی ok و apply، کلاینت مورد نظر به اینترنت دسترسی خواهد داشت.

از این نکات می‌توانید برای حفظ امنیت سیستم خود استفاده کنید و اجازه ندهید، هیچ سیستمی به غیر از سیستم‌های سازمان شما به اینترنت دسترسی داشته باشند.

Name	Source	Destination	Service	IP version	Action	Translation
VPN Services	Any	Firewall	Ipssec services Kerio VPN	Any	Allow	
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow	
Internet access (NAT)	192.168.5.13 Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing p
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow	
Firewall traffic	Firewall	Any	Any	Any	Allow	
Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow	
Block other traffic	Any	Any	Any	Any	Drop	

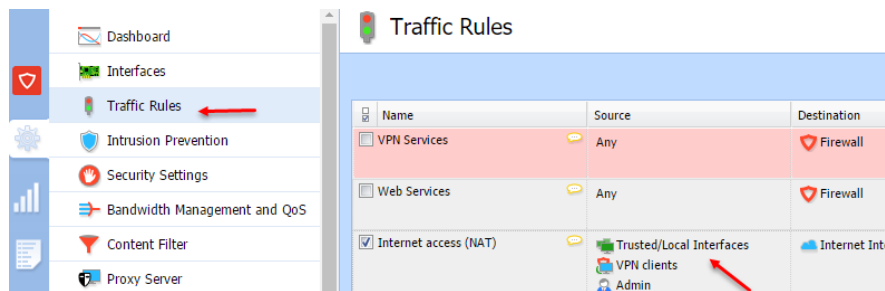
در این صفحه هم به خوبی این تنظیمات را مشاهده می‌کنید.

راه‌اندازی VPN Clients:

این روش یک از پرکاربردترین روش‌ها برای اشتراک گذاری اینترنت و کنترل کاربران در یک شبکه است، با این روش به این موارد دست پیدا می‌کنید:

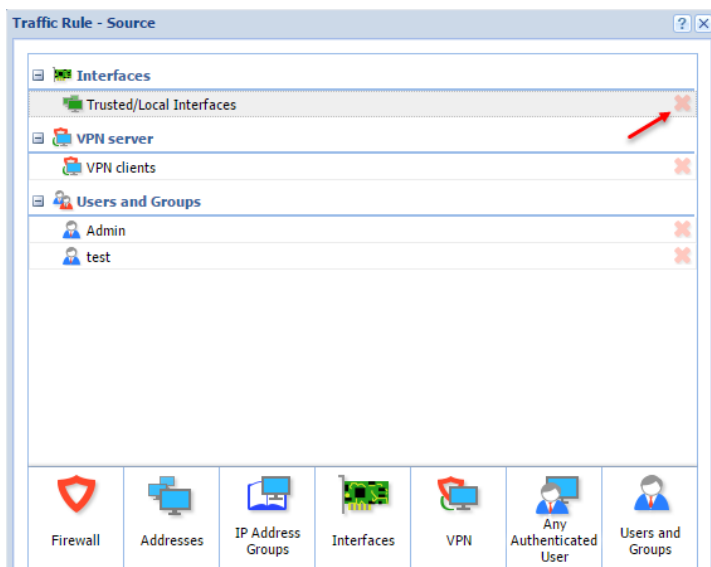
- ۱- اینترنت فقط مختص کاربران واقعی شبکه خواهد بود و بقیه‌ی افراد که از بیرون وارد شرکت می‌شوند، نمی‌توانند به اینترنت دسترسی پیدا کنند.
- ۲- تمام کارهایی که کاربران در اینترنت انجام می‌دهند، در قسمت مانیتورینگ ثبت خواهد شد که در مورد مانیتورینگ در ادامه، به‌طور مفصل بحث خواهیم کرد.
- ۳- برای هر کاربر می‌توانید، حجم مشخص تعیین کنید تا بیشتر از آن حد از اینترنت استفاده نکند.
- ۴- و.....

برای اینکه VPN را برای دسترسی به اینترنت به کاربران دهیم باید یک سری تنظیمات در کریو انجام دهیم.

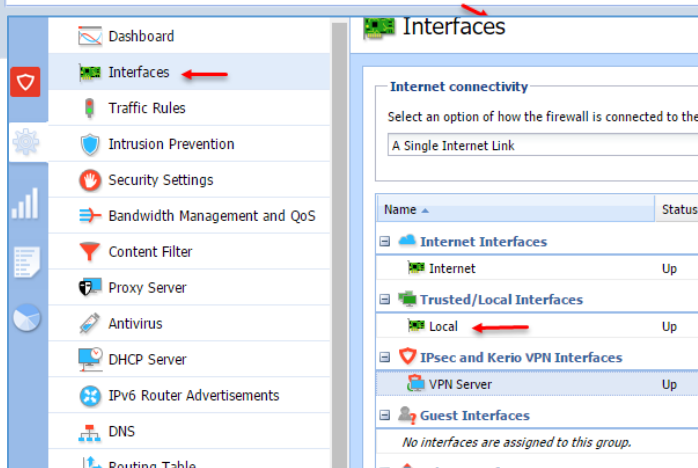


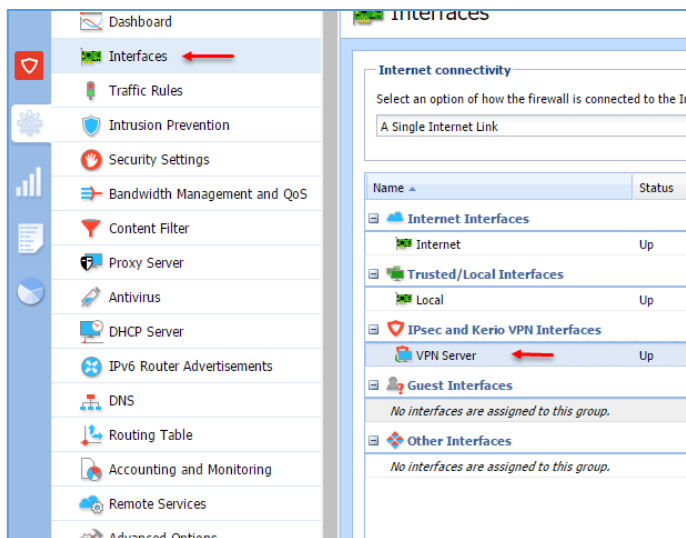
برای شروع باید دسترسی خودکار کاربران را به اینترنت قطع کنیم، برای این کار به مانند شکل روبرو از سمت چپ بر روی Traffic Rules کلیک کنید و در قسمت Source مربوط به internet Access، دو بار کلیک کنید.

در این صفحه، گزینه‌ی Trusted/Local Interface را حذف کنید و بر روی OK کلیک کنید؛ با این کار دسترسی اتومات کاربران به اینترنت قطع خواهد شد.

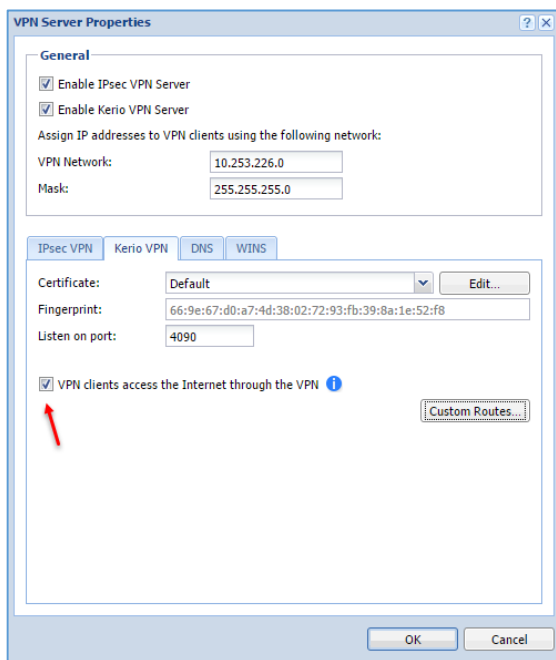


در مورد Trusted/Local Interface، قبلاً با هم صحبت کردیم که شکل آن را هم مشاهده می‌کنید، اگر خوب به شکل توجه کنید، کارت شبکه‌ی داخلی، یعنی Local در زیر مجموعه‌ی Trusted/Local Interface قرار دارد که با حذف آن در مرحله‌ی قبل، دسترسی کلیه کاربران به اینترنت غیرممکن خواهد بود.





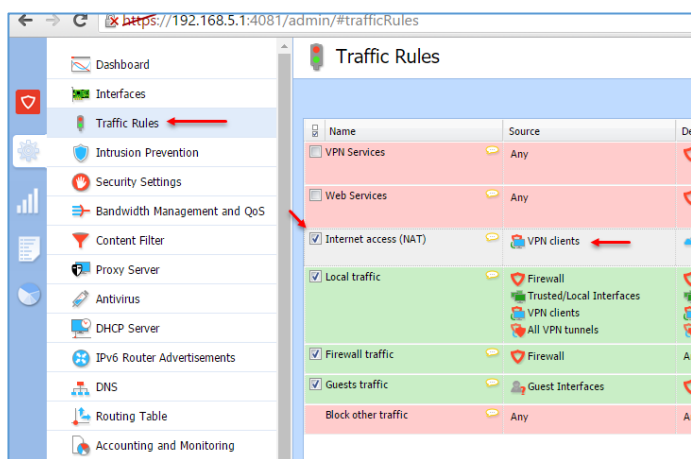
بعد از انجام مراحل بالا باید VPN را برای دسترسی کاربران به اینترنت فعال‌سازی کنید، برای این کار وارد Interface شوید و بر روی VPN Server دو بار کلیک کنید.



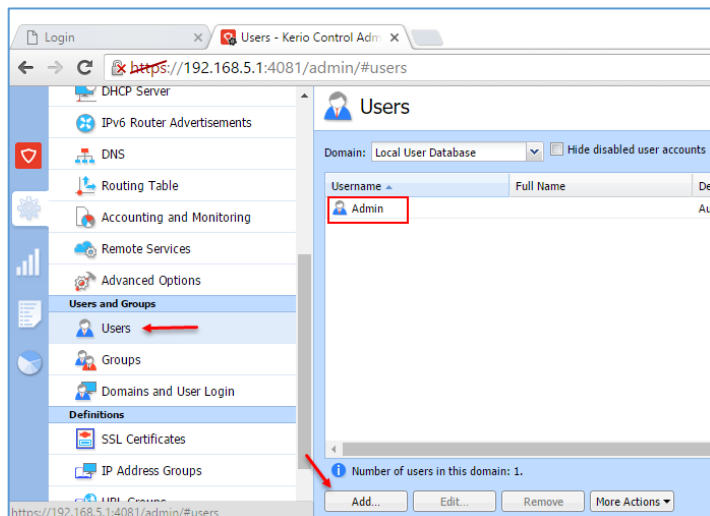
در این صفحه وارد تب Kerio VPN شوید و تیک گزینه‌ی VPN Clients Access the internet through the VPN را انتخاب کنید و بر روی ok کلیک کنید؛ با این کار، کاربرانی که از طریق VPN به کریو متصل می‌شوند، دارای اینترنت می‌شوند، در این قسمت دو نکته وجود دارد که:

- ۱- رنج IP سرور VPN بر روی 10.253.226.0 قرار دارد که آن را می‌توانید به دلخواه خود تغییر دهید.
- ۲- برای اینکه کاربرانی که با VPN به کریو متصل می‌شوند به

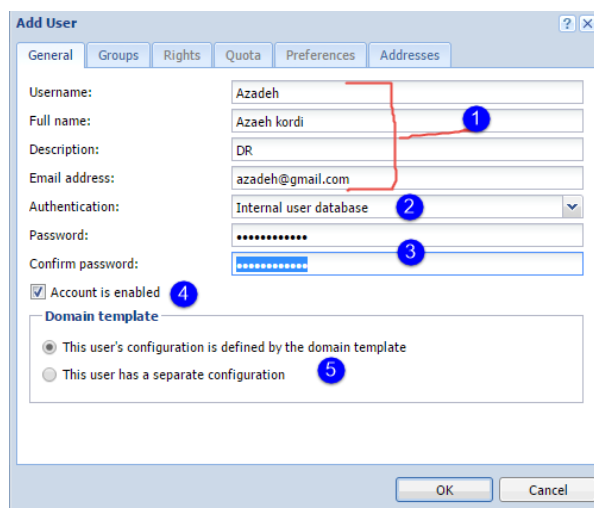
اینترنت دسترسی داشته باشند باید در شکل مقابل و در قسمت Traffic Rule در Rule مربوط به Internet Access و در قسمت Source آن اضافه شده باشند؛ با این کار، کاربران بعد از متصل شدن به کریو به اینترنت هم متصل خواهند شد.



در مرحله‌ی بعد باید برای کاربران خود یک نام کاربری تعریف کنیم که این نام می‌تواند به صورت دستی یا به صورت متصل شدن به سرور **Active Directory** باشد؛ در این مرحله، ایجاد کاربر به صورت دستی را بررسی خواهیم کرد و در ادامه، کریو را به سرور **Active** متصل خواهیم کرد.

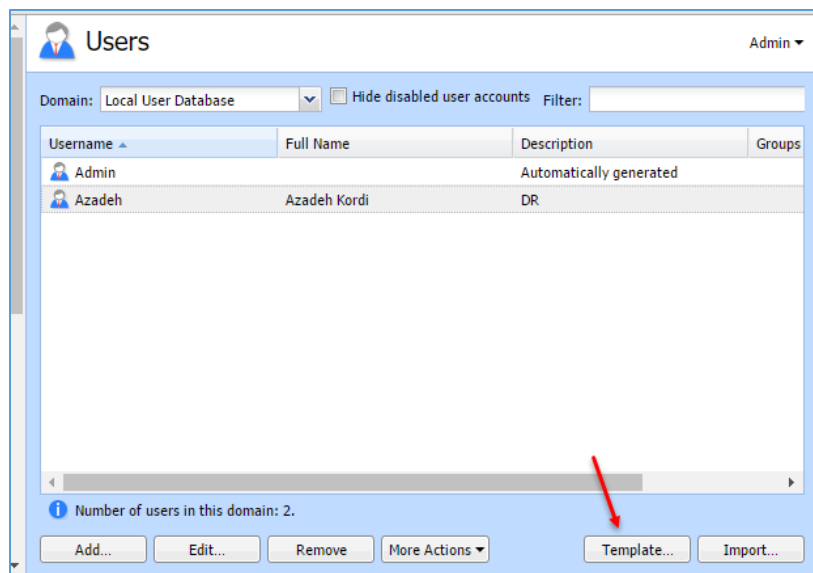


در شکل روبرو وارد قسمت **Users** شدیم، همانطور که مشاهده می‌کنید، یک کاربر **Admin** به صورت پیش-فرض در لیست قرار دارد و این همان کاربری است که با آن وارد کریو می‌شویم؛ برای شروع و ایجاد کاربر جدید بر روی **Add** کلیک کنید.

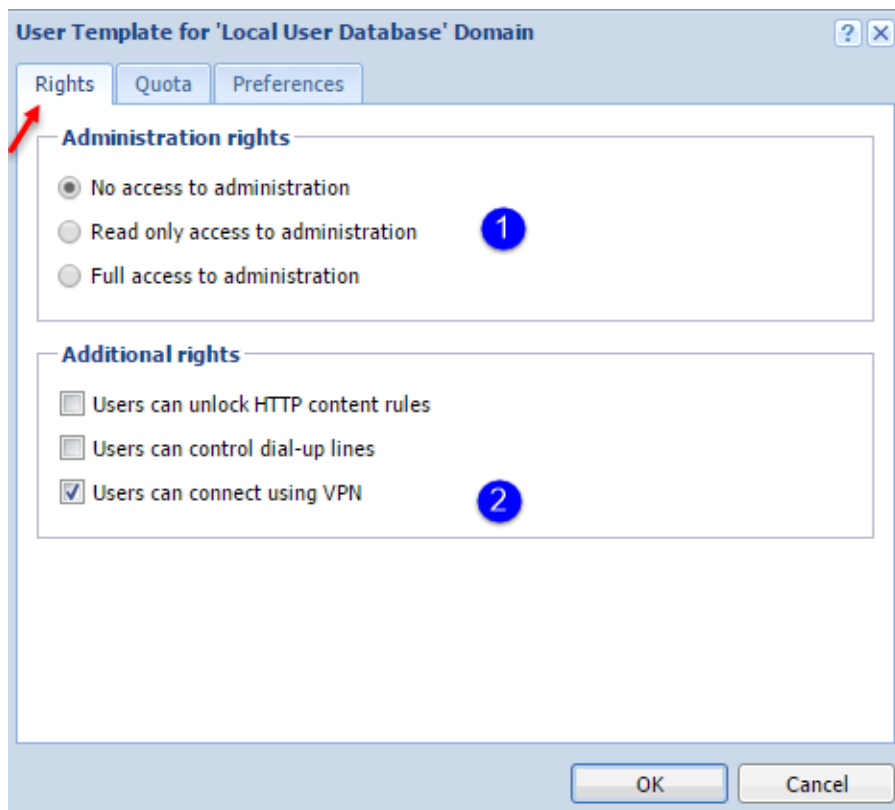


در تب **General** و در قسمت شماره‌ی یک، **Username** کاربر مورد نظر خود را به همراه نام کامل، توضیحات و آدرس ایمیل آن وارد کنید، در قسمت شماره‌ی دو اگر گزینه‌ی **Internal...** را انتخاب کنید، یعنی اینکه کاربر شما از نوع داخلی است، اما اگر گزینه‌ی **Active Directory** را انتخاب کنید، می‌توانید کاربر خود را از **Active Directory** صدا بزنید؛ در قسمت رمز عبور هم یک رمز پیچیده برای کاربر خود وارد کنید و در قسمت شماره‌ی چهار، تیک گزینه‌ی **Account Enable** را انتخاب کنید

تا کاربر مورد نظر فعال شود. در قسمت شماره‌ی پنج نیز، اگر گزینه‌ی اول را انتخاب کنید، یک سری تنظیمات را به صورت پیش‌فرض به شما می‌دهد که باید آن را تنظیم کنید، اما اگر بخواهید دسترسی‌های کاربر و حجم استفاده‌ی کاربر را به صورت دستی کنترل کنید باید گزینه‌ی پایینی آن را انتخاب و بر روی **ok** کلیک کنید.

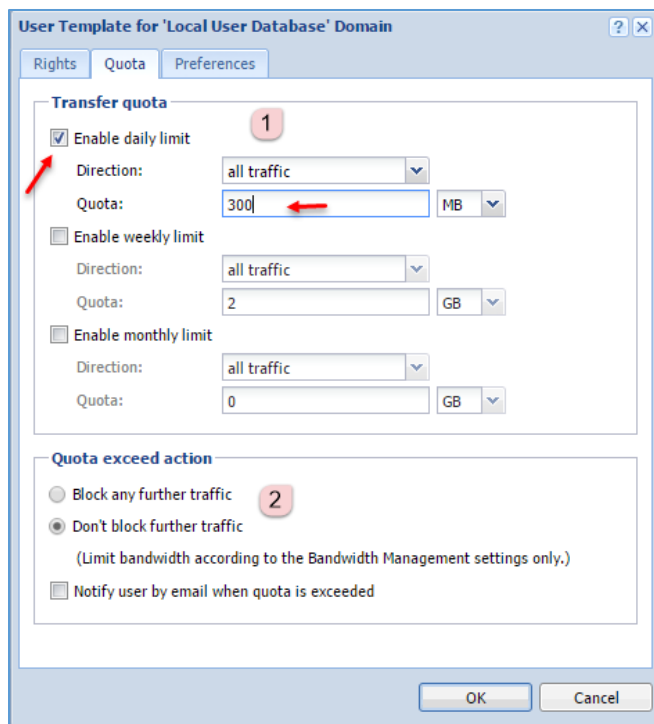


همانطور که مشاهده می‌کنید، کاربر مورد نظر ایجاد شده است؛ در قسمت قبل و شماره‌ی پنج، دو گزینه وجود داشت که گزینه‌ی اول، تنظیمات پیش‌فرضی است که برای مشاهده آن باید بر روی **Template** کلیک کنید.



در این صفحه و در تب **Right**، یک - سری تنظیمات پیش‌فرض وجود دارد که اگر آن را تغییر ندهیم، کاربران نمی‌توانند به کریو متصل شوند، قسمت شماره‌ی یک برای دسترسی **Read** و **Write** کاربر به صفحه‌ی مدیریتی کریو است که به صورت پیش‌فرض، هیچ کاربری به جز کاربر **Admin** به سرور دسترسی ندارد، اگر در قسمت شماره‌ی دو، تیک گزینه‌ی **Users can connect using VPN** را انتخاب نکنید، کاربران نمی‌توانند از طریق

VPN به کریو متصل شوند، بعد از انتخاب گزینه‌ها وارد تب **Quota** شوید.



در تب Quota می‌توانید حجم مصرفی کاربران را مشخص کنید؛ در قسمت شماره‌ی یک، سه گزینه‌ی روزانه، هفتگی و ماهانه وجود دارد که مقدار آن را باید مشخص کنید. در شکل روبرو، تیک گزینه‌ی **Enable daily limit** فعال شده است و عدد ۳۰۰ مگابایت مشخص شده است که این مقدار حجم برای استفاده کاربر در یک روز است، اما اگر این مقدار مصرف شود، اینترنت کاربر قطع نخواهد شد!، به دلیل اینکه در قسمت شماره‌ی دو، گزینه‌ی **Don't block further traffic** انتخاب شده است و زمانی که کاربری، حجم مورد نظر خود را مصرف کند، اینترنت وی قطع نخواهد شد، تنها با فعال کردن **Notify user...** یک ایمیل برای وی ارسال

خواهد شد، برای اینکه اینترنت کاربران قطع شود باید گزینه‌ی **Block any Further traffic** را انتخاب و بر روی **ok** کلیک کنید. در تب **Preference**، گزینه‌هایی برای فیلتر کدهای **HTML** وجود دارد که در صورت نیاز آن را بررسی خواهیم کرد.

بعد از بررسی کاربر و ایجاد آن باید وارد کلاینت‌ها شویم و **VPN Client** را بر روی آنها نصب کنیم، برای نصب **VPN Client** باید از آدرس زیر استفاده کنیم:

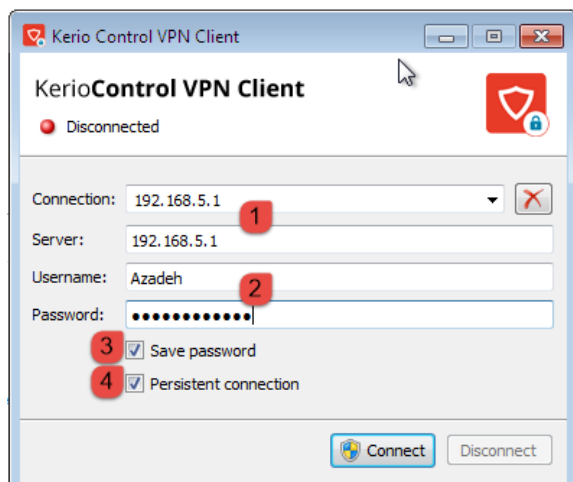
ورژن ۳۲ بیتی:

<http://www.mapnaturbine.com/en/Download/kerio-control-vpnclient-8.0.1-609-win32.zip>

ورژن ۶۴ بیتی:

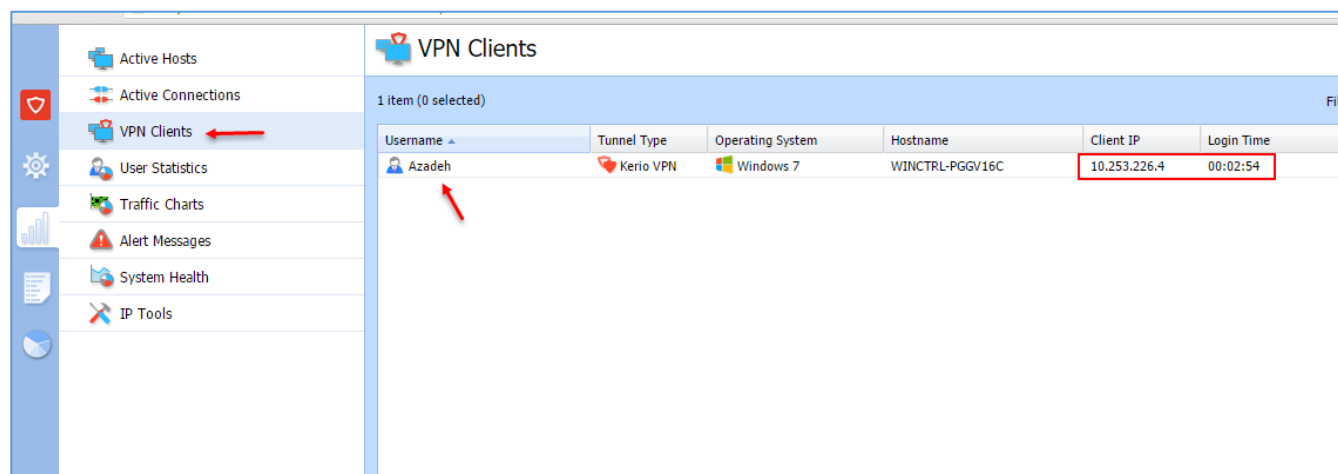
<http://www.mapnaturbine.com/en/Download/kerio-control-vpnclient-8.0.1-609-win64.zip>

بعد از دانلود آن را به راحتی نصب و اجرا کنید.



زمانی که **VPN Client** را نصب کردید، شکل روبرو را مشاهده خواهید کرد که باید در قسمت شماره‌ی یک و در قسمت **Connection**، آدرس سرور کریو را وارد کنید و در قسمت **server** هم اگر آدرس‌های مختلف برای ارتباط با کریو دارید، می‌توانید با وارد کردن آنها را وارد کنید، در قسمت شماره‌ی دو، نام کاربری که با هم ایجاد کردیم را وارد کنید و در قسمت شماره‌ی سه، اگر تیک گزینه‌ی **Save Password** را انتخاب کنید، رمز عبور شما ذخیره خواهد شد و اگر تیک گزینه‌ی ۴

را انتخاب کنید، زمانی که کریو کانکشن به هر علتی قطع شود، دوباره اقدام به اتصال با سرور کریو می‌کند. بر روی **Connect** کلیک کنید تا ارتباط برقرار شود.



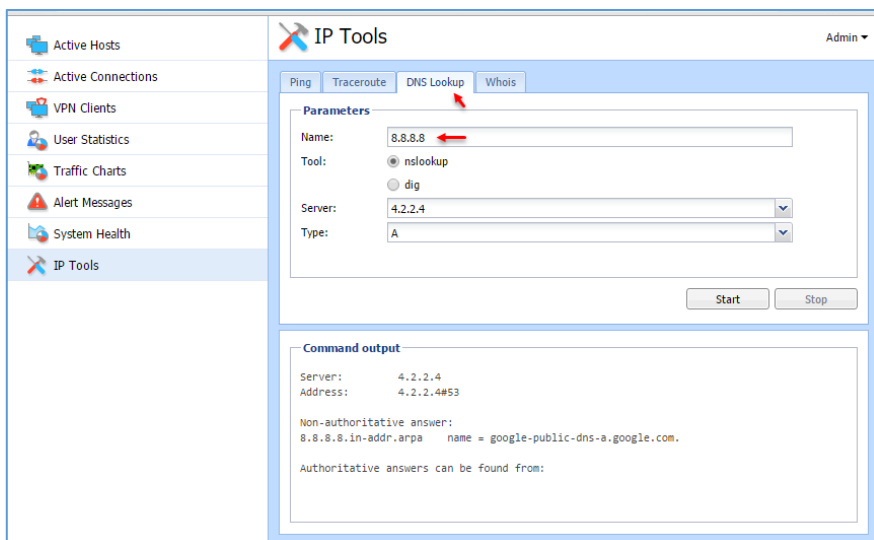
برای اینکه دریابید به صورت آنلاین چه کسانی از طریق **VPN** به کریو متصل هستند، به مانند شکل بالا از سمت چپ بر روی آیکون کلیک کنید و در گزینه‌های مورد نظر، وارد قسمت **VPN Clients** شوید که کاربر مورد نظر خود را مشاهده خواهید کرد؛ در صفحه‌ی بالا، نوع سیستم‌عامل، نام سیستم، آدرس IP، به همراه زمان اتصال مشخص شده است که برای قطع اتصال هم می‌توانید روی آن کلیک‌راست کنید و گزینه‌ی **Disconnect** را کلیک کنید.

User Statistics		7 items (1 selected)					Filter:
Username	Full Name	Quota	Today [MB]	Week [MB]	Month [MB]	Total [MB]	
guest users	guest users		0	0	11	11	
not logged in	not logged in		1	1	3	90	
Azadeh	Azadeh Kordi	2%	8	8	8	8	
test	test1	1%	3	3	3	3	
Admin		0%	0	0	0	0	
babajani		0%	0	0	0	0	
all users	all users		12	12	25	112	

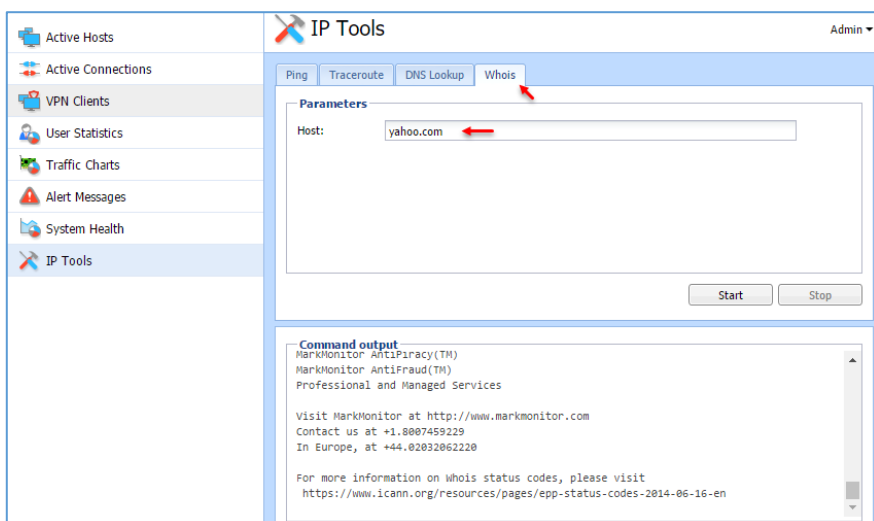
اگر بر روی **User Statistics** کلیک کنید، می‌توانید تمامی کاربرانی که از اینترنت استفاده کردند را مشاهده کنید، گزینه‌ی **Guest User** به کاربران مهمانی اشاره دارد که برای مدت محدودی از اینترنت استفاده می‌کنند که برای این قسمت در ادامه، صحبت خواهیم کرد. قسمت **Not Logged In** به کلاینت‌هایی گفته می‌شود که بدون واسطه به اینترنت، متصل می‌شوند، مثلاً اگر شما در شبکه‌ی خود از **Access Point** استفاده کنید، تمام حجم مصرفی آن در این قسمت ثبت خواهد شد، اگر حجم کاربر در لیست به ۱۰۰ درصد رسید می‌توانید بر روی کاربر مورد نظر کلیک راست کنید و آن را ریست کنید تا دوباره حجم جدید به آن تخصیص داده شود.

در قسمت **IP Tools** هم می‌توانید چهار عملیات **Ping** , **Traceroute** , **DNS Lookup** , **Whos** را به مانند شکل روبرو انجام دهید؛ در قسمت‌های دیگر مانند **System Health** می‌توانید مقدار مصرف **CPU** و **RAM** را بررسی کنید.

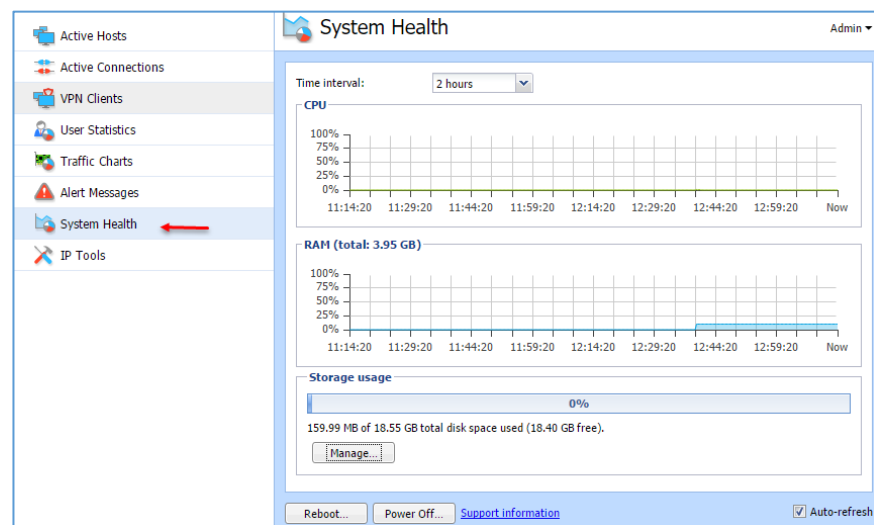
در قسمت **Traceroute** می‌توانید با وارد کردن آدرس یک سایت، مسیرهایی که برای رسیدن به این سایت بر سر راه شما قرار دارد را مشاهده کنید که در شکل روبرو، روترهایی بر سر راه برای رسیدن به سایت **3isco.ir** را مشاهده می‌کنید.



در تب DNS Lookup می‌توانید با وارد کردن یک IP، نام آن را در شبکه‌ی داخلی و یا خارجی مشاهده کنید؛ در شکل روبرو، IP به شماره ۸,۸,۸,۸ وارد شده است که نام آن برابر با google-public-dns-a.google.com است که مربوط به شرکت گوگل است.



در تب Whois، شما می‌توانید با وارد کردن نام یک دومین خاص، مانند یاهو اطلاعاتی از صاحب سایت، شماره‌ی تماس، تاریخ دریافت دومین و... دست پیدا کنید که در بعضی موارد به آن نیاز پیدا خواهید کرد. به کارتان خواهد آمد.



در قسمت System Health می‌توانید به صورت آنلاین مقدار کارکرد CPU, Hard Disk, Ram را مشاهده کنید و در پایین صفحه هم دو گزینه‌ی Reboot و Power off وجود دارد که می‌توانید سیستم را ریست و یا خاموش کنید.

ارتباط Kerio با Active Directory:

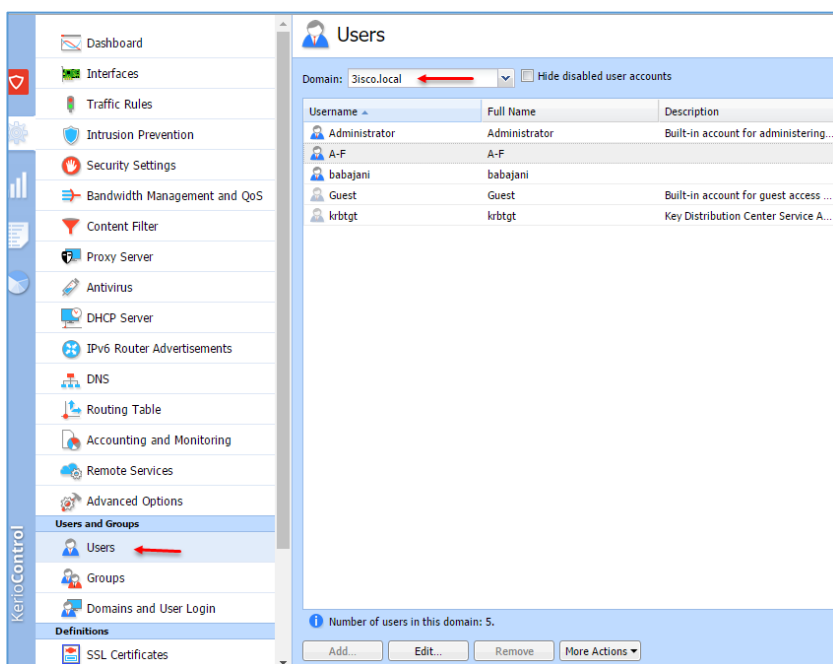
برای کنترل بهتر کاربران و تمرکز کاری، بهترین راه حل این است که کریو را به Active Directory شبکه‌ی خود متصل کنید تا از این طریق، کاربرانی که با نام کاربری و رمز عبور خود وارد سیستم می‌شوند، بتوانند با همان حساب از VPN هم استفاده کنند؛ با این کار مدیریت کاربران آسان‌تر خواهد شد و خود کاربران با تغییر رمز عبور حساب خود، رمز عبور کریو آن‌ها هم تغییر خواهد کرد.

نصب و راه‌اندازی سرویس Active Directory را در ویندوز سرور ۲۰۱۲ از قبل انجام دادیم و دومین آن را 3isco.local در نظر گرفتیم، شما هم برای نصب و راه‌اندازی Active Directory و سرویس‌های دیگر می‌توانید کتاب MCSE 2012 را از سایت 3isco.ir دریافت کنید.

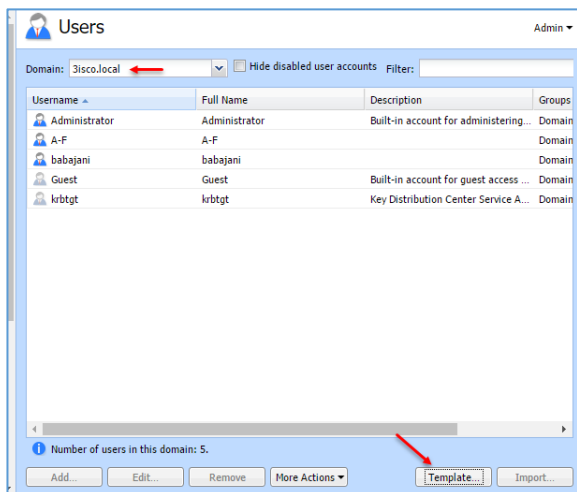
برای متصل شدن به دومین باید وارد قسمت مدیریتی Kerio شوید و از سمت چپ بر روی Domain and User Login کلیک کنید و بعد بر روی شماره‌ی ۲، یعنی Directory Services کلیک کنید؛ در این صفحه، تیک گزینه‌ی شماره‌ی ۳ را انتخاب کنید تا بتوانید اطلاعات کاربران و گروه‌ها را از Active Directory بخوانید.

در قسمت **Directory Service Type**، دو نوع **Directory** وجود دارد که یکی برای مایکروسافت و دیگری برای اپل است. در قسمت شماره‌ی ۴ باید نام دومین خود را وارد کنید که در این کتاب، نام دومین را **3isco.local** در نظر گرفتیم که در قسمت مورد نظر وارد کردیم.

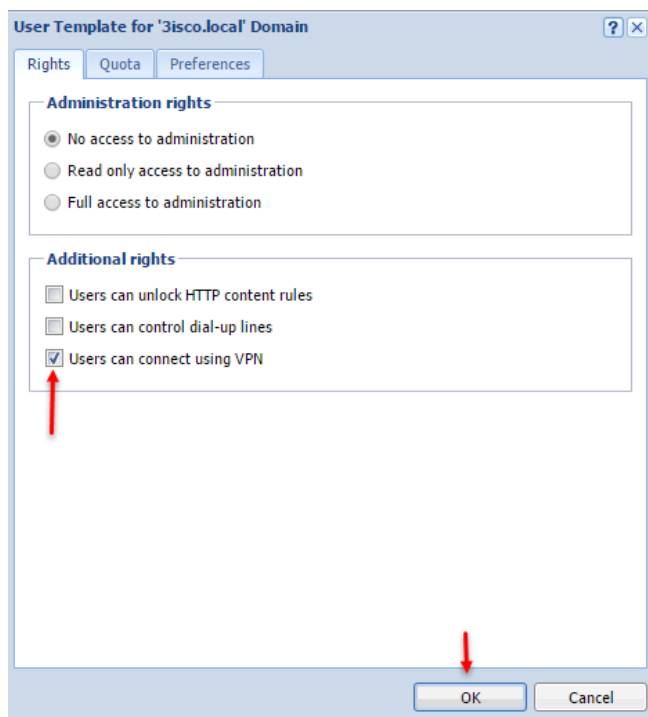
در قسمت شماره‌ی ۵ باید نام کاربری و رمز عبور **Admin** دومین خود را وارد کنید، در قسمت شماره‌ی ۶، گزینه‌ی **Connect to the specified directory service** را انتخاب کنید و هر چندتایی که سرور دومین دارید باید آدرس آن‌ها را در جای مشخص شده وارد کنید که در اینجا، چون یک سرور دومین داشتیم، آدرس آن را وارد کردیم و برای تست برقراری اتصال بر روی **Test Connection** کلیک می‌کنیم؛ همانطور که در تصویر صفحه‌ی قبل مشاهده می‌کنید، تماس برقرار شد که برای تأیید اطلاعات باید بر روی **Apply** کلیک کنید.



برای اینکه اطلاعات دومین را مشاهده کنید، از سمت چپ بر روی **Users** کلیک کنید و در صفحه‌ی باز شده و در قسمت دومین، نام دومین خود را انتخاب کنید تا اطلاعات کاربران برای شما نمایش داده شود؛ در ادامه‌ی کار با استفاده از کاربران دومین و از طریق **VPN** به **Kerio** متصل می‌شویم.

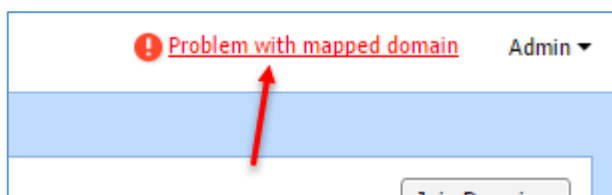


برای اینکه کاربران دومین از طریق **VPN** به کریو متصل شوند باید ابتدا، دومین خود را انتخاب کنید و بعد بر روی **Template** کلیک کنید.

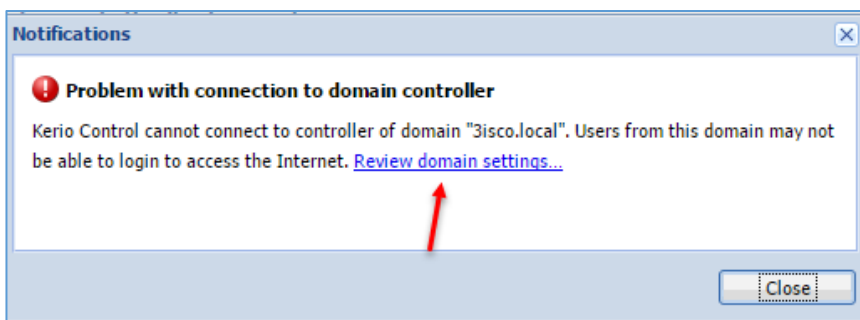


در این قسمت، تیک گزینه‌ی **Users can connect using VPN** را انتخاب و بر روی **ok** کلیک کنید.

بعد از این کار شما می‌توانید با هر کاربری که در **Active Directory** هست، **VPN** بزیند و به اینترنت متصل شوید. خوبی این روش این است که مدیریت کاربران ساده‌تر است و اگر کاربران، رمز عبور خود را تغییر دهند، رمز آن‌ها در **Kerio** نیز تغییر خواهد کرد.



اگر ارتباط دومین با کریو قطع شود در بالای صفحه و از سمت راست در کریو با پیغام **Problem with mapped domain** مواجه خواهید شد. بر روی آن کلیک کنید.



در این صفحه با پیغام متصل نشدن کریو به دومین **3isco.local** مواجه شدیم که باید بررسی کنیم که آیا سرور دومین روشن است یا ارتباط بین دومین و کریو برقرار است، بعد از این کار بر روی

Review domain settings کلیک کنید تا به صفحه‌ی اتصال به دومین انتقال داده شوید؛ در این صفحه به مانند قبل، ارتباط را برقرار می‌کنیم.

بررسی Log در Kerio:

شاید بهترین عملکرد کریو در **Log** گیری از سرور و کاربران باشد؛ در قسمت **Log**، تمام اطلاعات، مانند ورود کاربر به سایت خاص یا تغییر تنظیمات توسط کاربر و ... نمایش داده خواهد شد.

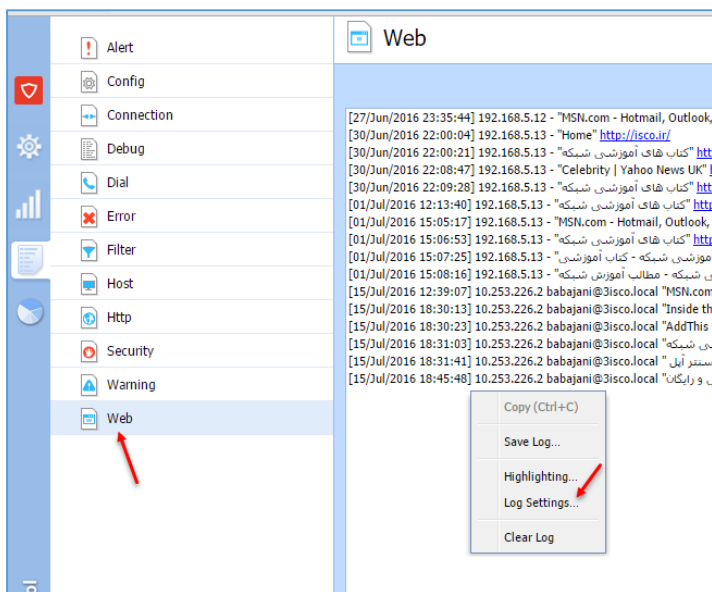
Alert	Web
	[27/Jun/2016 23:35:44] 192.168.5.12 - "MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos" http://www.msn.com/?ocid=iehp
	[30/Jun/2016 22:00:04] 192.168.5.13 - "Home" http://3isco.ir/
	[30/Jun/2016 22:00:21] 192.168.5.13 - "کتاب های آموزشی شبکه" http://3isco.ir/
	[30/Jun/2016 22:08:47] 192.168.5.13 - "Celebrity Yahoo News UK" https://uk.news.yahoo.com/celebrity
	[30/Jun/2016 22:09:28] 192.168.5.13 - "کتاب های آموزشی شبکه" http://3isco.ir/
	[01/Jul/2016 12:13:40] 192.168.5.13 - "کتاب های آموزشی شبکه" http://3isco.ir/
	[01/Jul/2016 15:05:17] 192.168.5.13 - "MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos" http://www.msn.com/?ocid=iehp
	[01/Jul/2016 15:06:53] 192.168.5.13 - "کتاب های آموزشی شبکه" http://3isco.ir/
	[01/Jul/2016 15:07:25] 192.168.5.13 - "کتاب های آموزشی شبکه - کتاب آموزشی" http://3isco.ir/post/419
	[01/Jul/2016 15:08:16] 192.168.5.13 - "کتاب های آموزشی شبکه - مطالب آموزش شبکه" http://3isco.ir/post/category/3
	[15/Jul/2016 12:39:07] 10.253.226.2 babajani@3isco.local "MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos" http://www.msn.com/?ocid=iehp
	[15/Jul/2016 18:30:13] 10.253.226.2 babajani@3isco.local "Inside the Plan to Undo the Iran Nuclear Deal - POLITICO Magazine" http://www.politico.com/story/2016/07/15/iran-nuclear-deal-undo-plan-224881
	[15/Jul/2016 18:30:23] 10.253.226.2 babajani@3isco.local "AddThis Utility Frame" http://s7.addthis.com/static/sh.5db545155503ce07aedcd166.html
	[15/Jul/2016 18:31:03] 10.253.226.2 babajani@3isco.local "کتاب های آموزشی شبکه" http://3isco.ir/
	[15/Jul/2016 18:31:41] 10.253.226.2 babajani@3isco.local "دانلود ها و نرم افزارها ، موزیک ، کتاب و آپلود فایل - 7003 آپلود سنتر آپل" http://www.uploader.net/
	[15/Jul/2016 18:45:48] 10.253.226.2 babajani@3isco.local "آپلود فایل و آپلود عکس بصورت دائمی و رایگان" http://www.uploader.net/

در شکل بالا، وارد صفحه **Log** شدیم که دارای گزینه‌های مختلف است؛ در قسمت **Web** که در شکل بالا هم مشاهده می‌کنید، تمام سایت‌هایی که کاربران وارد آن شده‌اند، نمایش داده شده است، اگر توجه کنید نام کاربر **babajani** را مشاهده می‌کنید که در ساعت‌ها و تاریخ‌های مشخص وارد سایت‌های نمایش داده شده است که به راحتی می‌توان کاربران را در شبکه کنترل کرد؛ در این روش کاربرانی که وارد سایت‌های **HTTPS** می‌شوند، لیست نخواهند شد که برای آن هم روش وجود دارد که در ادامه، آن را بررسی خواهیم کرد.

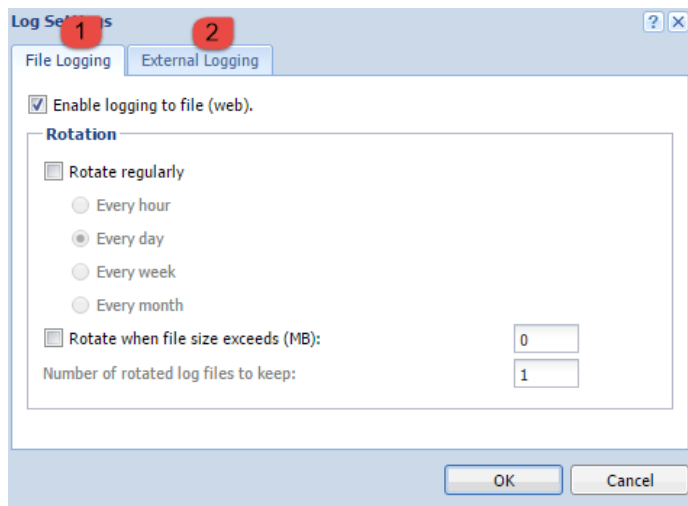
Alert	Http
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://ocsp-sql.certificat2.com/class2primarvca/MFHwUTBPMR0wS2AJBqUrDoHCGoUABR0xU5vwpW9Xf4V8hZM7Xve4nFnqOUgswHfOI" HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://ocsp-sql.certificat2.com/class2primarvca/MFHwUTBPMR0wS2AJBqUrDoHCGoUABR0xU5vwpW9Xf4V8hZM7Xve4nFnqOUgswHfOI" HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://ocsp-sql.certificat2.com/class2primarvca/MFHwUTBPMR0wS2AJBqUrDoHCGoUABR0xU5vwpW9Xf4V8hZM7Xve4nFnqOUgswHfOI" HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://ocsp-sql.certificat2.com/class2primarvca/MFHwUTBPMR0wS2AJBqUrDoHCGoUABR0xU5vwpW9Xf4V8hZM7Xve4nFnqOUgswHfOI" HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://ocsp-sql.certificat2.com/class2primarvca/MFHwUTBPMR0wS2AJBqUrDoHCGoUABR0xU5vwpW9Xf4V8hZM7Xve4nFnqOUgswHfOI" HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:32:22 +0400] "GET http://www.certplus.com/CRL/class2.crl HTTP/1.1" 200 1721
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:45:48 +0400] "GET http://uploader.net/ HTTP/1.1" 301 232
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:45:48 +0400] "GET http://www.uploader.net/ HTTP/1.1" 200 7270
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:45:48 +0400] "GET http://www.uploader.net/ZeroClipboard.min.js HTTP/1.1" 200 9563 +1
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:45:48 +0400] "GET http://www.uploader.net/images/upload_cloud_ico.png HTTP/1.1" 200 980
	10.253.226.2 - babajani@3isco.local [15/Jul/2016:18:45:48 +0400] "GET http://www.uploader.net/main.css HTTP/1.1" 200 6770

اگر وارد قسمت **HTTP** شوید، می‌توانید سایت‌هایی که کاربران به آن مراجعه کردند را به صورت جزء به جزء مشاهده کنید که تمام آدرس‌ها و اطلاعات آن سایت در این قسمت ثبت خواهد شد.

برای تنظیم Log در هر قسمت کلیک راست کنید و گزینه‌ی Log Settings را انتخاب کنید.

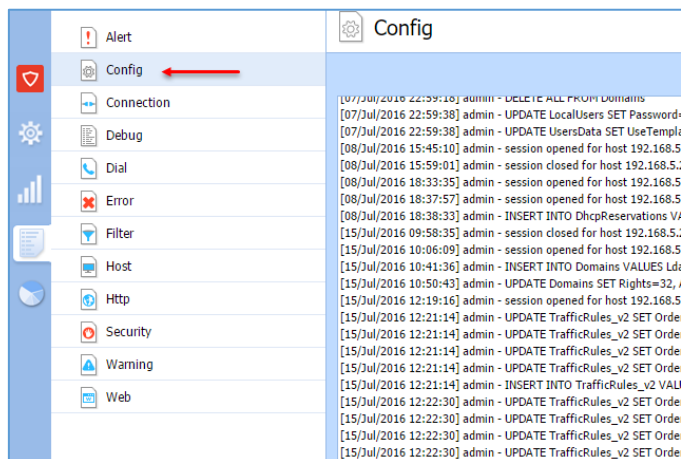


در این صفحه و در قسمت شماره‌ی ۱ می‌توانید با برداشتن تیک گزینه‌ی Enable... قسمت Log مربوط به Web را غیرفعال کنید، در قسمت Rotate regularly هم می‌توانید دوره‌ی چرخشی Log را ساعتی، روزانه، هفتگی و یا ماهانه در نظر بگیرید و اگر بخواهید فایل‌هایی را با حجم مشخص از قسمت Log جدا کنید و Log گرفته نشود باید گزینه‌ی Rotate when file... را انتخاب و حجم آن را مشخص کنید؛ در قسمت شماره‌ی ۲ اگر از



سرور sys log، سرور دیگری برای جمع آوری Log در شبکه استفاده می‌کنید، می‌توانید آدرس آن را وارد کنید تا تمام Log ها برای مدیریت بهتر به آن سرور ارسال شوند.

در قسمت‌های دیگر هم می‌توانید به اطلاعات دیگر دست پیدا کنید، مثلاً در قسمت Config می‌توانید تمام تنظیماتی که در کریو انجام دادید را مشاهده کنید، در قسمت Connection هم می‌توانید ارتباط کاربر با سایت‌های مختلف با آدرس IP را مشاهده کنید.



The screenshot shows the Security log in Kerio Control. The left sidebar has 'Security' selected. The main pane displays a list of log entries, many of which are authentication failures for the user 'rezaei' from IP 192.168.5.13. The entries include timestamps and details of the failed authentication attempts.

در قسمت Security، تغییراتی که در سرویس‌ها ایجاد می‌شود یا خطا در هنگام متصل شدن کاربران از طریق VPN و... را مشاهده کنید که این اطلاعات در یک زمان به کارتان می‌آید که می‌تواند خیلی به شما کمک کند.

The screenshot shows the Host log in Kerio Control. The left sidebar has 'Host' selected. The main pane displays a list of log entries related to network activity, including IP addresses, MAC addresses, and user logins. The entries show various network events such as user logins, host registrations, and IP address leases.

در قسمت Host نیز اطلاعاتی در مورد متصل شدن کاربران از طریق VPN، گرفتن IP از سرویس DHCP و... را مشاهده کنید.

Alert	Filter	Admin
Config	Find:	
Connection	[22/Jul/2016 22:12:07] DENY URL 'Audio and video files' 10.253.226.3 rezaei@3isco.local HTTP GET http://static.3isco.com/staticrep/orcaaudio/vwz/vwz...	
Debug	[22/Jul/2016 22:15:06] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.hackthissite.org/	
Dial	[22/Jul/2016 22:16:15] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.dictionary.com/browse/hack	
Error	[22/Jul/2016 22:16:16] DENY URL 'Audio and video files' 10.253.226.3 rezaei@3isco.local HTTP GET http://static.sfdict.com/staticrep/dictaudio/H00/H0006	
Filter	[22/Jul/2016 22:16:27] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.merriam-webster.com/dictionary/hack	
Host	[22/Jul/2016 22:27:35] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.merriam-webster.com/dictionary/hack	
Http	[22/Jul/2016 22:27:35] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.merriam-webster.com/dictionary/hack	
Security	[22/Jul/2016 22:28:53] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.merriam-webster.com/dictionary/hack	
Warning	[22/Jul/2016 22:28:59] DENY Keyword filter 'hack, hacking' 10.253.226.3 rezaei@3isco.local HTTP GET http://www.merriam-webster.com/dictionary/hack	
Web	[22/Jul/2016 22:44:43] DENY Keyword filter '10.253.226.3 rezaei@3isco.local HTTP GET http://www.msn.com/	
	[24/Jul/2016 21:06:03] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:06:15] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:06:54] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:07:04] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:08:47] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:08:49] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:08:51] Last message repeated 3 times	
	[24/Jul/2016 21:12:54] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://fararu.com/	
	[24/Jul/2016 21:30:28] DENY Keyword filter 'illegal' 10.253.226.4 rezaei@3isco.local HTTP GET http://edition.cnn.com/	
	[24/Jul/2016 21:31:05] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[24/Jul/2016 21:33:08] DENY Keyword filter 'serial, crack,' 10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://p30download.com/	
	[24/Jul/2016 21:34:42] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[25/Jul/2016 19:41:31] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[25/Jul/2016 19:42:09] DENY Keyword filter '10.253.226.4 فوئبان' rezaei@3isco.local HTTP GET http://www.varzesh3.com/	
	[25/Jul/2016 20:21:54] DENY Keyword filter '10.253.226.4 rezaei@3isco.local HTTP GET http://www.msn.com/?ocid=iehp	
	[25/Jul/2016 20:22:55] DENY Keyword filter 'keygen' 10.253.226.4 rezaei@3isco.local HTTP GET https://mail.google.com/_scs/mail-static/_js/k=gmail.ma	

در قسمت Filter نیز سایت‌هایی را مشاهده خواهید کرد که کلماتی در آن‌ها به کار رفته است که ما آن‌ها را در لیست فیلترینگ قرار دادیم که برای درک بهتر این موضوع باید به قسمت Content Filter در ادامه‌ی کتاب مراجعه کنید.

Alert	Error	Admin
Config	Find:	
Connection	[27/Jul/2016 22:28:55] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
Debug	[27/Jul/2016 22:29:01] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
Dial	[27/Jul/2016 22:29:07] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
Error	[27/Jul/2016 22:41:05] Antivirus Server error:(PID: 17018) Internet connection is probably broken. Cannot check for new version.	
Filter	[27/Jul/2016 22:41:05] Unable to perform Sophos update. Error: Internet connection is probably broken. Cannot check for new version.	
Host	[28/Jul/2016 17:34:51] (2) Unable to activate Kerio Control Web Filter: Server returned 403. Categorization will not work.	
Http	[28/Jul/2016 17:35:21] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
Security	[28/Jul/2016 17:35:27] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
Warning	[28/Jul/2016 17:35:52] (2) Unable to activate Kerio Control Web Filter: Server returned 403. Categorization will not work.	
Web	[28/Jul/2016 17:36:01] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
	[28/Jul/2016 17:36:02] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
	[28/Jul/2016 17:36:35] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
	[28/Jul/2016 17:36:36] (-11) Active Directory/LDAP error: 3isco.local: Connect error	
	[28/Jul/2016 17:40:53] (2) Unable to activate Kerio Control Web Filter: Server returned 403. Categorization will not work.	
	[28/Jul/2016 17:43:41] Antivirus Server error:(PID: 4175) Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 17:43:41] Unable to perform Sophos update. Error: Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 17:54:40] IPS rules update check failed: Timeout was reached.	
	[28/Jul/2016 17:56:07] (2) Unable to activate Kerio Control Web Filter: Server returned 403. Categorization will not work.	
	[28/Jul/2016 18:02:45] Antivirus Server error:(PID: 4376) Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 18:02:45] Unable to perform Sophos update. Error: Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 18:03:59] Antivirus Server error:(PID: 4399) Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 18:03:59] Unable to perform Sophos update. Error: Internet connection is probably broken. Cannot check for new version.	
	[28/Jul/2016 18:44:32] (-5) Active Directory/LDAP error: 3isco.local: Timed out	
	[28/Jul/2016 18:56:13] (2) Unable to activate Kerio Control Web Filter: Server returned 403. Categorization will not work.	
	[29/Jul/2016 12:39:35] Antivirus Server error:(PID: 6267) Internet connection is probably broken. Cannot check for new version.	
	[29/Jul/2016 12:39:35] Unable to perform Sophos update. Error: Internet connection is probably broken. Cannot check for new version.	

در قسمت Error نیز خطاهایی را مشاهده می‌کنید، مانند ارتباط کریو با Active Directory و یا ارتباط کریو با سایت آپدیت خود و

Dial Admin

Find:

```
[24/Jul/2016 21:41:55] Kerio VPN client 'rezaei' connected from 192.168.5.13
[24/Jul/2016 21:44:14] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:02:19
[24/Jul/2016 21:44:19] Kerio VPN client 'rezaei' connected from 192.168.5.13
[25/Jul/2016 19:30:14] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 21:45:55
[25/Jul/2016 19:40:56] Kerio VPN client 'rezaei' connected from 192.168.5.13
[25/Jul/2016 20:31:45] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:50:49
[25/Jul/2016 20:32:17] Kerio VPN client 'rezaei' connected from 192.168.5.13
[25/Jul/2016 21:22:10] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:49:53
[25/Jul/2016 21:22:16] Kerio VPN client 'rezaei' connected from 192.168.5.13
[26/Jul/2016 21:26:56] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 1 day 00:04:40
[26/Jul/2016 21:28:32] Kerio VPN client 'rezaei' connected from 192.168.5.13
[26/Jul/2016 21:32:54] Kerio VPN client 'rezaei' connected from 192.168.5.13
[26/Jul/2016 21:32:59] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:04:27
[26/Jul/2016 21:44:14] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:11:20
[26/Jul/2016 21:44:18] Kerio VPN client 'rezaei' connected from 192.168.5.13
[27/Jul/2016 22:18:18] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 1 day 00:34:00
[27/Jul/2016 22:39:29] Kerio VPN client 'rezaei' connected from 192.168.5.13
[28/Jul/2016 17:37:11] Kerio VPN client 'rezaei' connected from 192.168.5.13
[28/Jul/2016 18:30:46] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:53:35
[28/Jul/2016 18:31:05] Kerio VPN client 'rezaei' connected from 192.168.5.13
[28/Jul/2016 18:43:34] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:12:29
[28/Jul/2016 18:48:33] Kerio VPN client 'rezaei' connected from 192.168.5.13
[28/Jul/2016 18:48:47] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:00:14
[29/Jul/2016 12:51:09] Kerio VPN client 'rezaei' connected from 192.168.5.13
[29/Jul/2016 13:34:08] Kerio VPN client 'rezaei' disconnected from 192.168.5.13, connection time 00:42:59
[29/Jul/2016 13:34:41] Kerio VPN client 'rezaei' connected from 192.168.5.13
```

در قسمت Dial نیز تمام ارتباطات کاربران از طریق VPN ثبت می شود.

Debug Admin

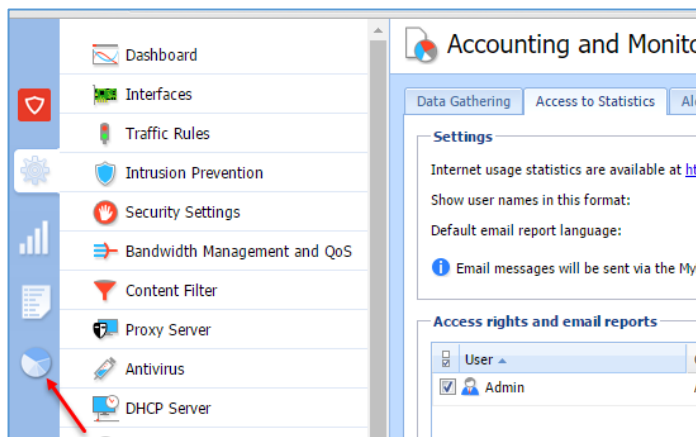
Find:

```
[20/Jul/2016 17:35:32] Service "webinterfaceSSL" started, bound to address 127.0.0.1
[28/Jul/2016 17:34:40] Interface "Local" is UP.
[28/Jul/2016 17:34:40] HW Address: 00-0c-29-7f-ed-f7
[28/Jul/2016 17:34:40] IPv4 Addresses: 192.168.5.1/255.255.255.0
[28/Jul/2016 17:34:40] Service "DNS UDP" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Service "DNS TCP" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Service "DHCP" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Service "WebInterface" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Service "WebInterfaceSSL" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Service "VPN" started, bound to address 192.168.5.1
[28/Jul/2016 17:34:40] Engine was initialized.
[28/Jul/2016 17:34:40] Interface "Internet" is UP.
[28/Jul/2016 17:34:40] HW Address: 00-0c-29-7f-ed-01
[28/Jul/2016 17:34:40] IPv4 Addresses: 192.168.1.254/255.255.255.0
[28/Jul/2016 17:34:41] Service "DNS UDP" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "DNS TCP" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "DHCP" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "WebInterface" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "WebInterfaceSSL" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "VPN" started, bound to address 10.253.226.1
[28/Jul/2016 17:34:41] Service "DNS UDP" started, bound to address 192.168.1.254
[28/Jul/2016 17:34:41] Service "DNS TCP" started, bound to address 192.168.1.254
[28/Jul/2016 17:34:41] Service "DHCP" started, bound to address 192.168.1.254
[28/Jul/2016 17:34:41] Service "WebInterface" started, bound to address 192.168.1.254
[28/Jul/2016 17:34:41] Service "WebInterfaceSSL" started, bound to address 192.168.1.254
[28/Jul/2016 17:34:41] Service "VPN" started, bound to address 192.168.1.254
```

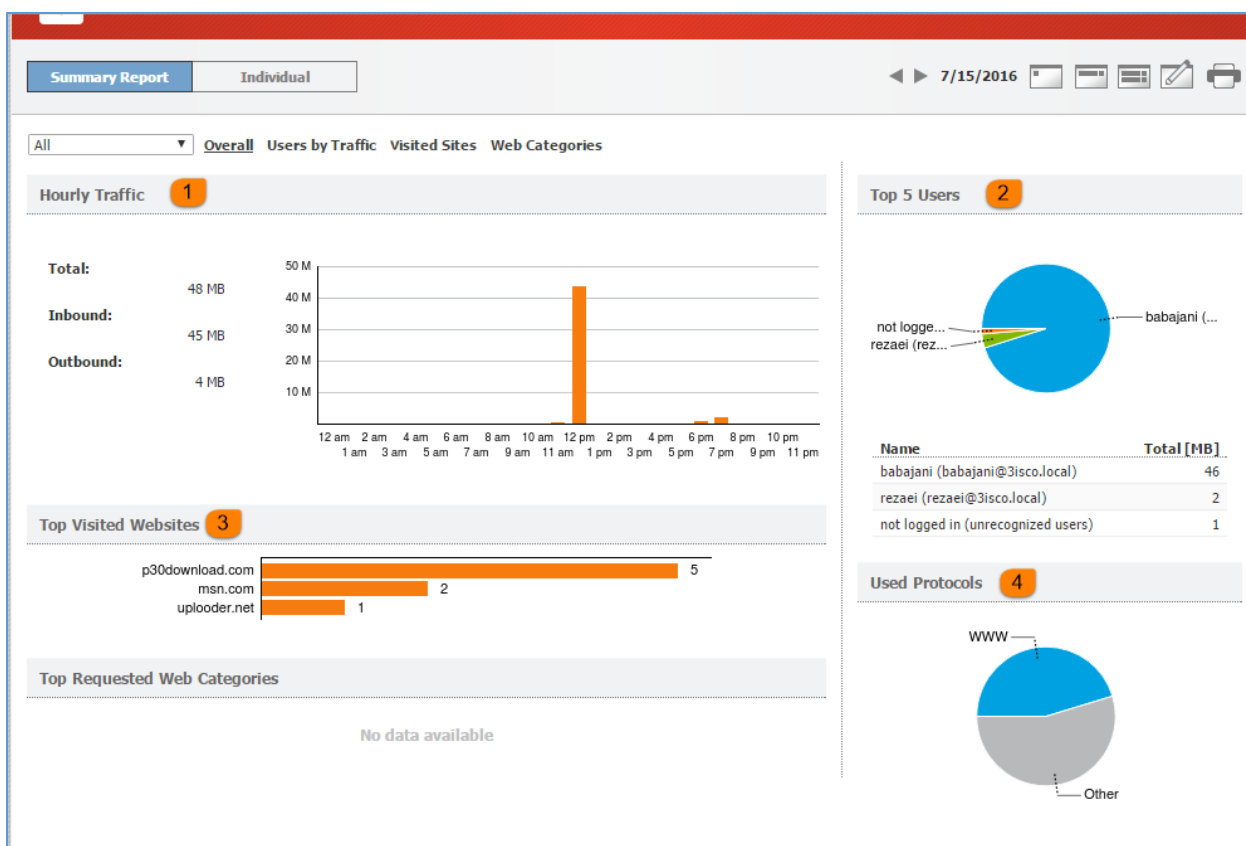
در قسمت Debug می توانید زمان اجرای سرویس ها را مشاهده کنید.

بررسی kerio control statistics

یکی از ابزارهای مفید Kerio که برای مشخص کردن مقدار مصرف کاربران از اینترنت، بیشترین سایت‌هایی که مراجعه کردند، نوع پروتکل ارتباطی و ... کاربرد دارد که به بررسی این قسمت می‌پردازیم.



در کربو از سمت چپ بر روی آیکن kerio control statistics کلیک کنید تا شکل بعد ظاهر شود.



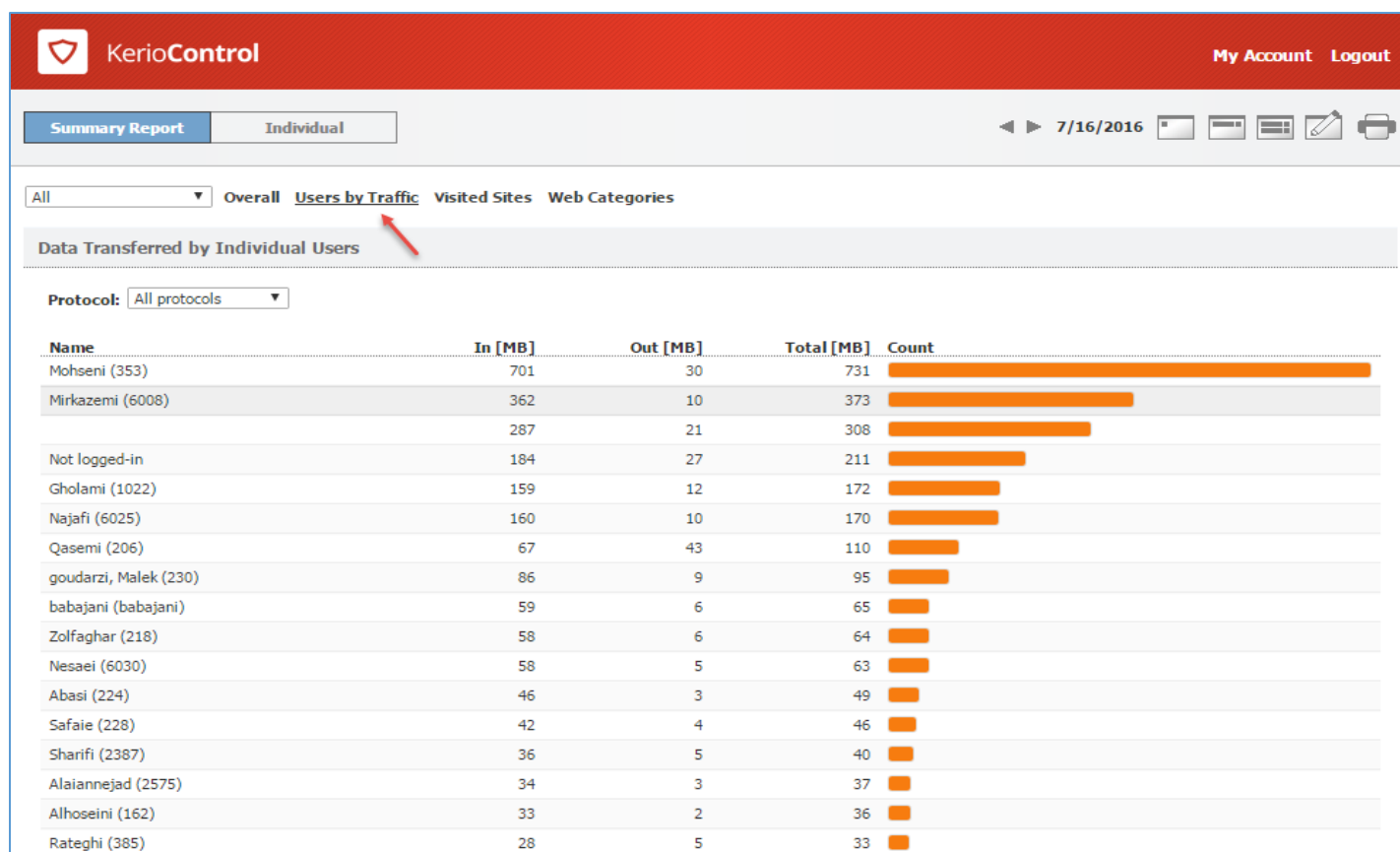
همانطور که مشاهده می‌کنید، صفحه‌ی مانیتورینگ کاربران نمایش داده شده است که بر طبق شماره، قسمت‌های مختلف را بررسی می‌کنیم.

در قسمت شماره‌ی یک، مقدار مصرف اینترنت را در یک روز و در ساعات مختلف نمایش می‌دهد که **Total**، به معنی کل مصرف اینترنت در این روز است و **Inbound**، حجم دریافتی و **Outbound**، مقدار حجم آپلود را مشخص کرده است.

در قسمت شماره‌ی دو، پنج کاربری که بیشترین مصرف را داشته‌اند، به صورت یک نمودار برای شما مشخص می‌کند که در این شکل، کاربری با نام **babajani** بیشترین مصرف را داشته است.

در قسمت شماره‌ی سه، بیشترین سایت‌هایی که کاربران شما به آن مراجعه کرده‌اند، نمایش داده می‌شود.

در قسمت شماره‌ی چهار نیز پروتکل ارتباطی کاربران مشخص شده است.



برای نمایش مقدار مصرف کاربران به صورت لیست شده باید در همین صفحه بر روی **Users by Traffic** کلیک کنید تا شکل بالا ظاهر شود؛ در شکل بالا، تمام کاربران شبکه به ترتیب، بیشترین مصرف به کمترین مصرف لیست شده است.

در نوار بالایی صفحه، گزینه‌های مختلف را مشاهده می‌کنید که شماره‌ی یک برای مصرف روزانه‌ی کاربران، شماره‌ی دو برای مصرف هفتگی و شماره‌ی سه برای مصرف ماهانه‌ی کاربران است، در قسمت شماره‌ی چهار نیز می‌توانید تاریخ را به صورت دستی وارد کنید.

نمایش مقدار کارکرد کاربران توسط خودشان:

کاربران شبکه نیز می‌توانند با ورود به آدرس کریو و وارد کردن نام کاربری و رمز عبور خود، مقدار مصرف اینترنت خود را بررسی کنند و می‌توانند رمز عبور کاربری خود را تغییر دهند.

کاربران می‌توانند در مرورگر خود، آدرس سرور کریو را وارد کنند، مانند:

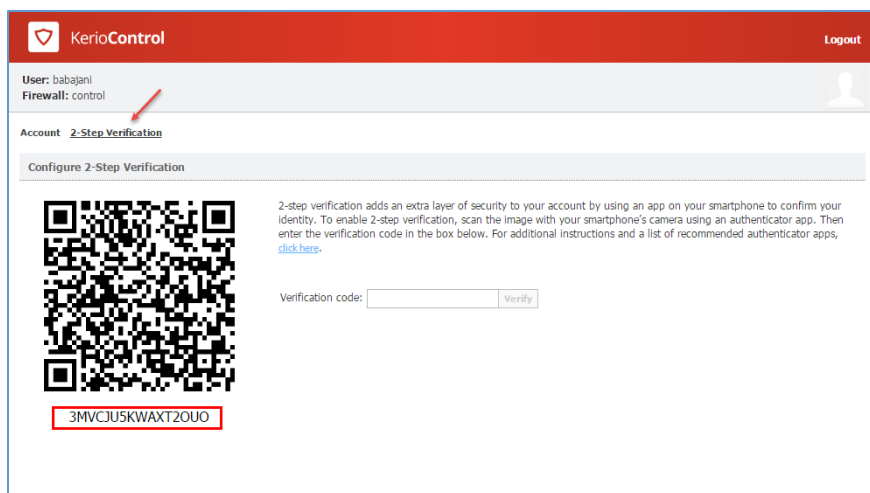
<https://192.168.5.1:4081>

که بعد از ورود از آن‌ها، نام کاربری و رمز عبور دریافت می‌شود که باید وارد کنند و بر روی دکمه Login کلیک کنند.

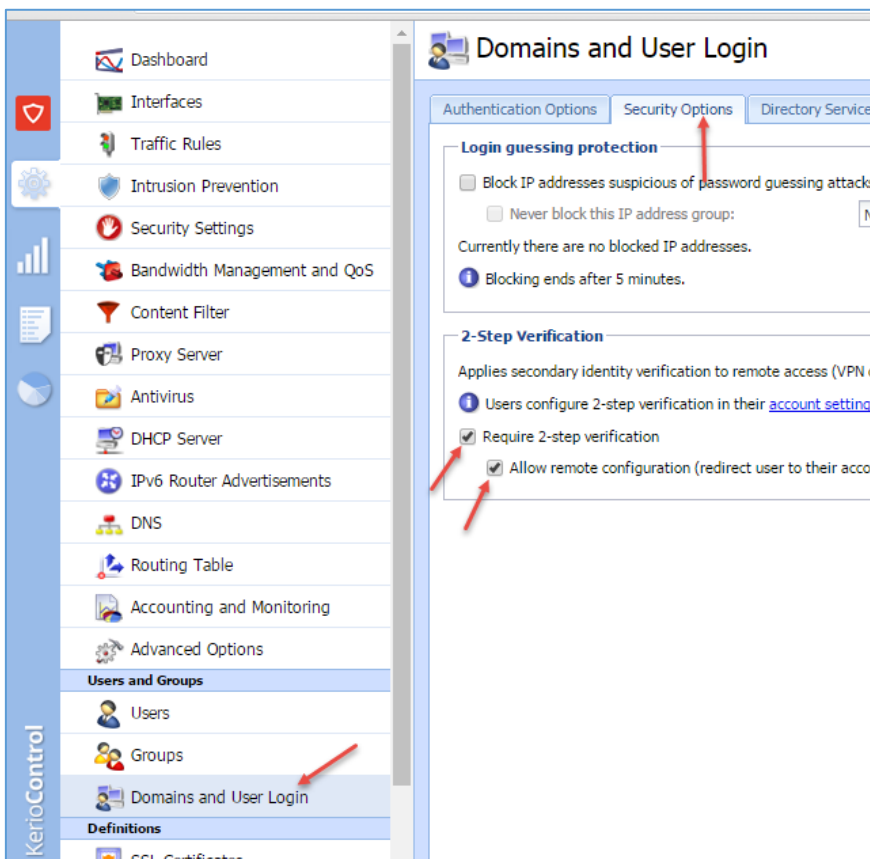
	Data IN	Data OUT	Quota (TOTAL)
Today 7/16/2016	32 MB	3 MB	11.69%
This Week Since 7/16/2016	32 MB	3 MB	No quota
This Month Since 7/1/2016	32 MB	3 MB	No quota

در این صفحه، قسمت‌هایی را مشاهده می‌کنید؛ در قسمت شماره‌ی یک، مقدار مصرف اینترنت به ترتیب روزانه، هفتگی و ماهانه نمایش داده شده است. در قسمت دوم، همه‌ی کاربران می‌توانند رمز عبور کریو خود را برای متصل شدن از طریق VPN تغییر دهند، تنها باید در قسمت Old Password، رمز عبور قدیمی خود و در قسمت

New Password، رمز عبور جدید خود را وارد و بر روی **Change password** کلیک کنند، با این کار رمز عبور آن‌ها به دلخواه خودشان تغییر می‌کند.



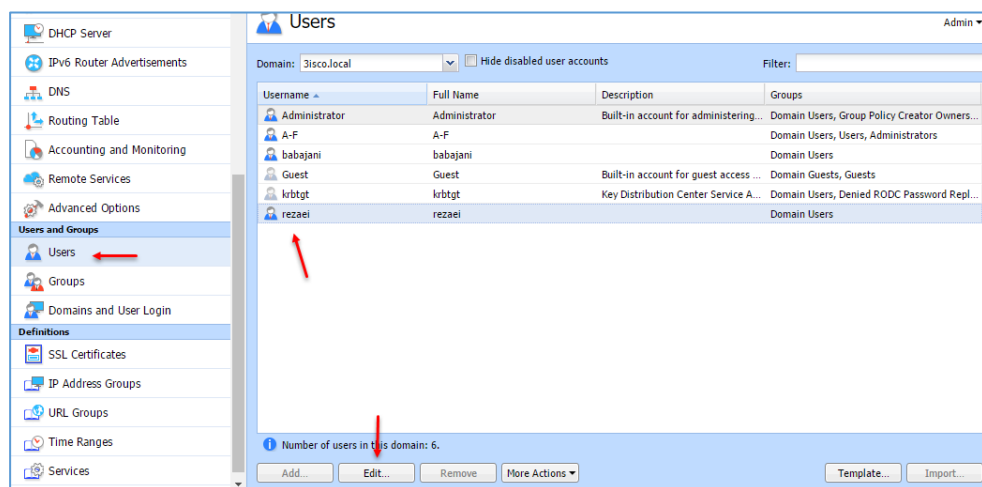
در این صفحه که یک مرحله‌ی امنیتی اضافه‌تر است، یک کد QR برای شما به نمایش داده می‌شود که این کد را باید از طریق نرم‌افزارهای بازکننده‌ی کد به دست آورید و در قسمت ورود به این صفحه وارد کنید.



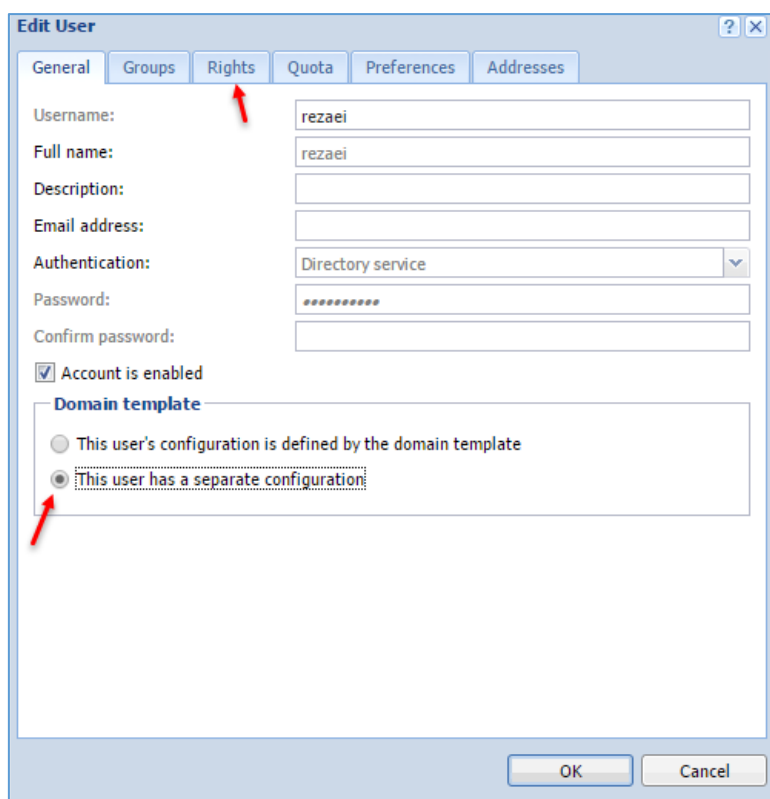
برای اینکه این قابلیت را برای کاربران فعال کنید باید وارد قسمت **Domains and user Login Security Options** باز شده وارد تب **Security Options** شوید که در شکل روبرو این موضوع را مشاهده می‌کنید، بعد از ورود به صفحه تیک گزینه‌ی مورد نظر را انتخاب کنید که کاربران بعد از اینکه بخواهند وارد سایتی شوند به صفحه‌ی وارد کردن کد انتقال داده می‌شوند.

دسترسی کامل کاربر به قسمت kerio control statistics:

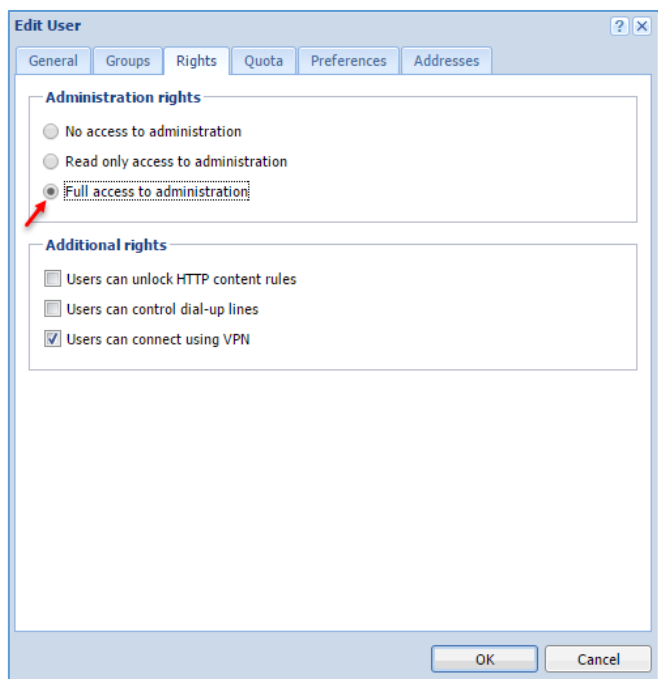
به صورت پیش فرض فقط کاربر admin به قسمت kerio control statistics دسترسی کامل دارد و می تواند تمام آمار کاربران را مشاهده کند، برای اینکه به کاربری خاص، دسترسی بدهید باید به صورت زیر عمل کنید:



به مانند شکل وارد قسمت Users شوید و بر روی کاربر مورد نظر خود کلیک و بعد بر روی Edit کلیک کنید.



در این صفحه برای اینکه فقط به یک کاربر دسترسی دهید باید گزینه‌ی **separate configuration** را انتخاب کنید تا تب **Rights** برای شما فعال شود؛ بعد از فعال شدن وارد تب **Rights** شوید.

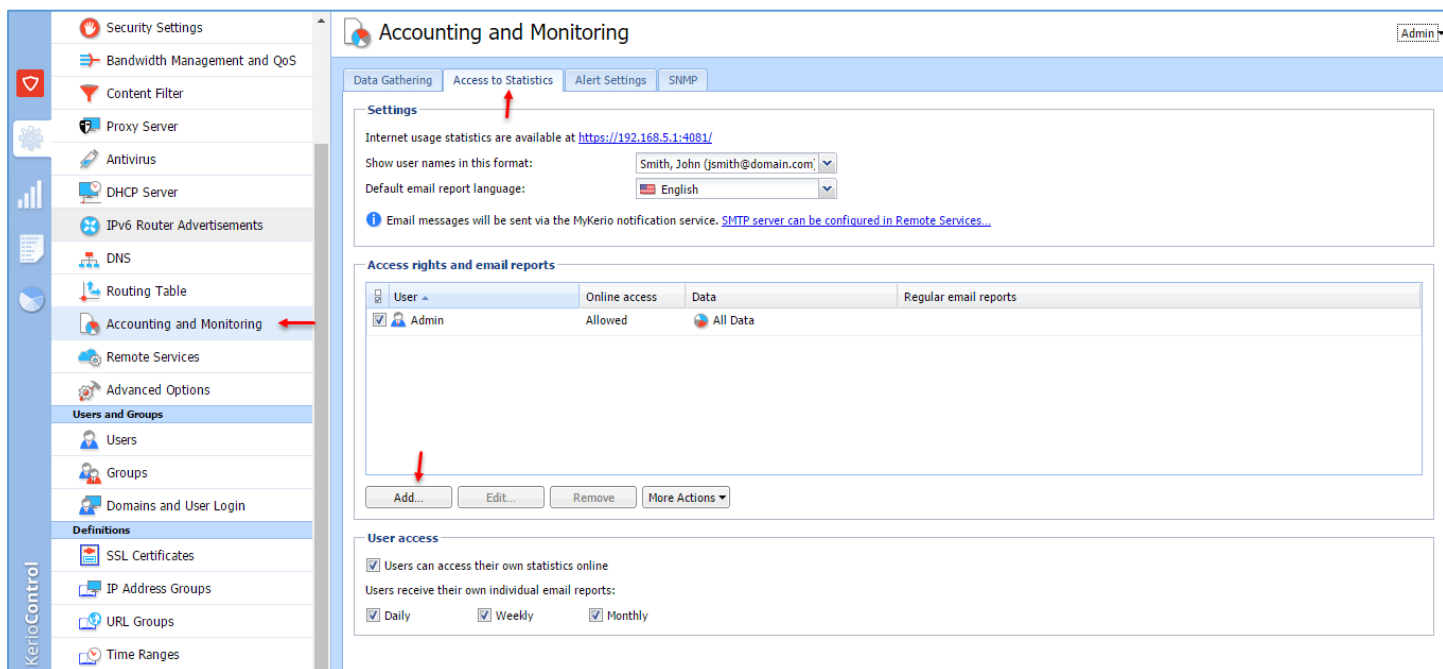


همانطور که در شکل روبرو مشاهده می‌کنید، گزینه‌ی Full Access to Administration انتخاب شده است که با این کار، کاربر مورد نظر دسترسی کامل به کریو خواهد داشت که می‌تواند به قسمت مدیریتی کریو و هم به قسمت مانیتورینگ آن، دسترسی کامل داشته باشد.

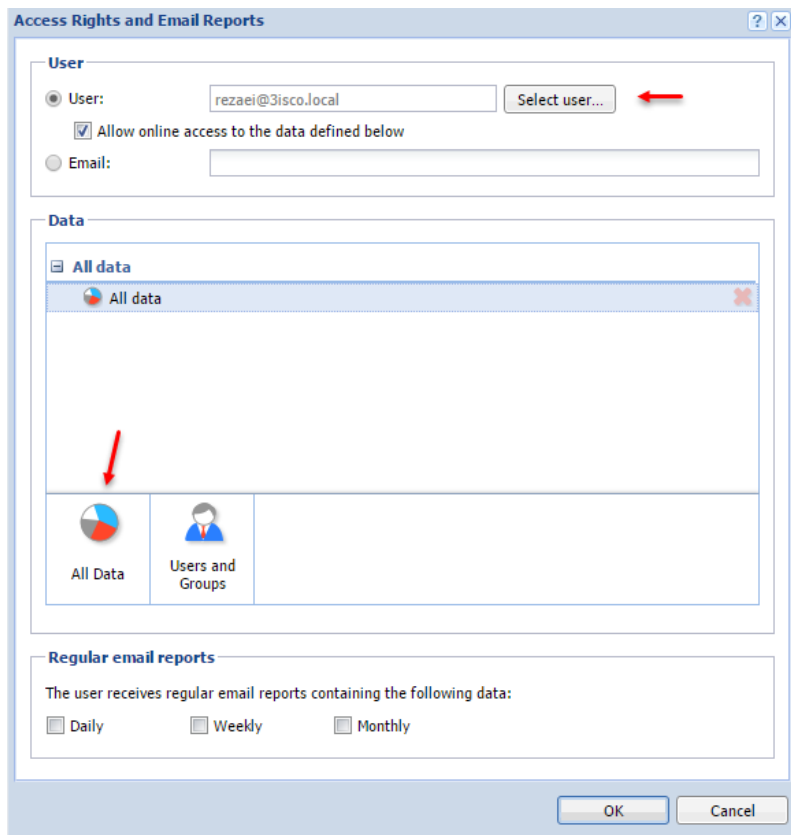
بر روی ok کلیک کنید تا اطلاعات ذخیره شود.

تذکر: با این کار، کاربر دسترسی کامل به بخش Admin خود کریو خواهد داشت و می‌تواند به مانند کاربر Admin عمل کند، اما برای اینکه فقط کاربر به بخش kerio

control statistics دسترسی داشته باشد، به مانند شکل زیر عمل کنید:



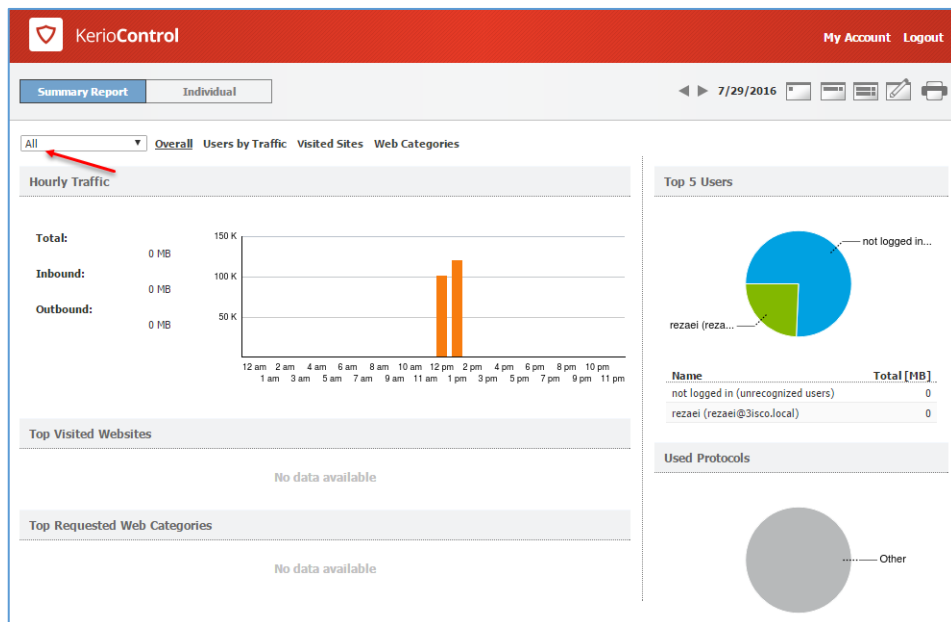
در شکل بالا وارد Accounting and Monitoring شوید و بعد وارد تب Access to Statistics شوید و برای اضافه کردن کاربر جدید به لیست بر روی Add کلیک کنید.



در این صفحه بر روی **Select user** کلیک کنید و کاربر مورد نظر خود را از لیست انتخاب کنید؛ در قسمت **Data** می‌توانید با انتخاب **All Data** دسترسی کامل را به کاربر دهید، با این کار می‌تواند تمامی اطلاعات کاربران را مشاهده کند، اما اگر بخواهید چند کاربر خاص را انتخاب کنید باید در شکل روبرو گزینه‌ی **Users and Groups** را انتخاب و کاربران مورد نظر را به لیست اضافه کنید.

در قسمت **Regular email reports** می‌توانید مشخص کنید که گزارش‌هایی که

برای کاربر ارسال می‌شود به صورت روزانه، هفتگی و ماهانه باشد، بر روی **ok** کلیک کنید تا اطلاعات ذخیره شود.



همانطور که در شکل روبرو مشاهده می‌کنید، کاربر مورد نظر را می‌تواند اطلاعات کاربران را مشاهده و آن‌ها را مدیریت کند.

بررسی قسمت Content Filter:

این قسمت در کریو برای مدیریت کاربران برای دسترسی به منابع خاصی، مانند سایت، IP و ... است که با هم این قسمت را بررسی می‌کنیم.

Name	Detected content	Source	Action	Valid Time
<input checked="" type="checkbox"/> Kerio sites	kerio.com samepage.io	Any	Allow Additional settings	
<input type="checkbox"/> Advertisements and banners	Ads/banners	Any	Drop	
<input type="checkbox"/> Updates and MS Windows activa...	Automatic Updates	Any	Allow Additional settings	
<input checked="" type="checkbox"/> Kerio Control Web Filter category...	Anonymizer Botnet Command and Control Centers Compromised Criminal Skills Hacking Malware Call-Home Malware Distribution Point Phishing/Fraud ...and 3 more	Any	Deny Additional settings	
<input checked="" type="checkbox"/> Audio and video files	Audio files Video files	Any	Deny Additional settings	
<input checked="" type="checkbox"/> Peer-to-Peer traffic	Peer-to-Peer	Any	Deny Additional settings	
<input type="checkbox"/> Allow other traffic	Any	Any	Allow	

Some rules are inactive (Kerio Control Web Filter is disabled).

Buttons: Add, Remove, More Actions, Apply, Reset

در شکل بالا، نمای اولیه‌ی Content Filter را مشاهده می‌کنید که از تب‌های مختلفی تشکیل شده است که به مرور، همه‌ی این تب‌ها را بررسی خواهیم کرد.

در تب Content Rule، یک سری رول‌های پیش‌فرض تعریف شده‌اند، مثلاً Rule با نام Audio and Video Files برای بستن دسترسی کاربران به فایل‌های صوتی و تصویری است، اگر یک کاربر بخواهد یک فایل تصویری یا صوتی را مشاهده و دریافت کند با پیغام خطای زیر مواجه خواهد شد.

Access Denied

Requested page
http://s4.topseda.biz/nevisande/reza/music/5/1/Emad%20-%20Joon%20%5b128%5d.mp3

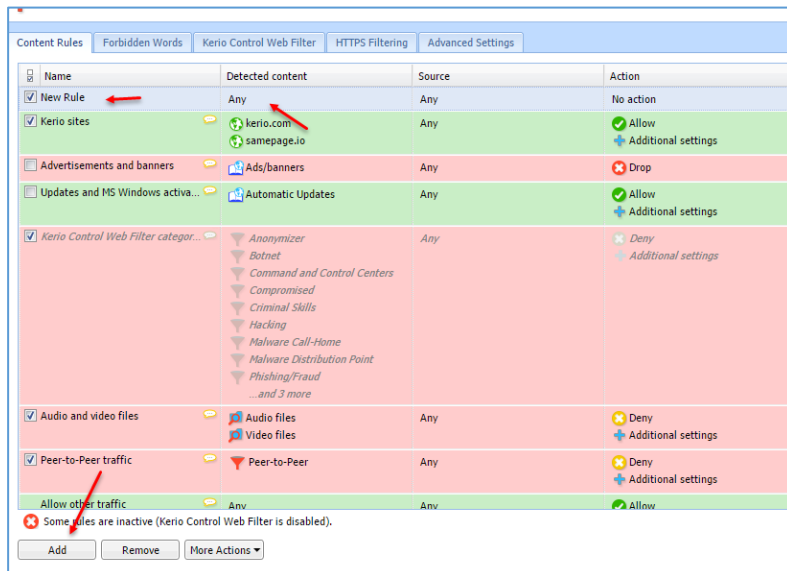
Transfer of the file was denied by firewall policy.

Kerio Control

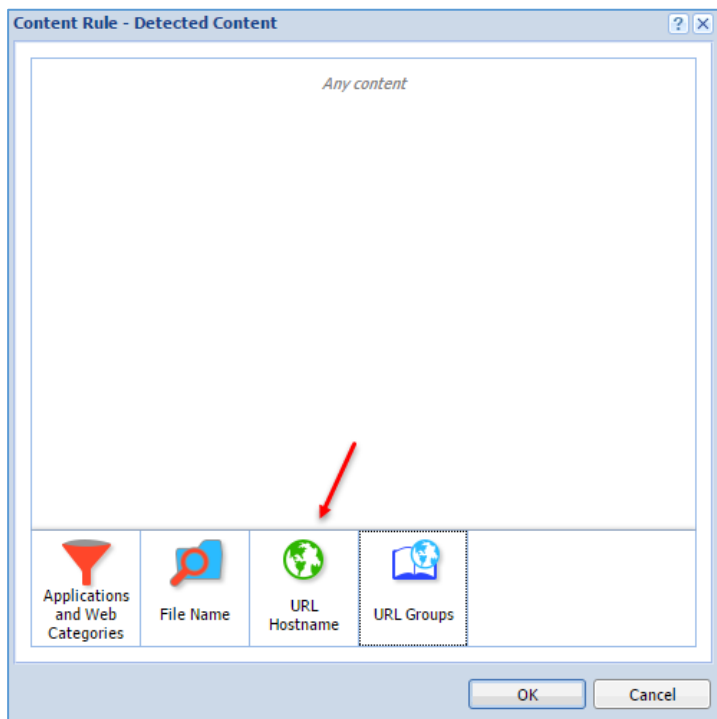
در پیغام روبرو به کاربر اعلام می‌شود که این نوع فایل، یعنی MP3 توسط فایروال کریو بسته شده است و شما دسترسی به این نوع فایل را ندارید.

بستن سایت برای کاربران:

برای اینکه یک یا چند سایت را برای کاربران ببندید به صورت زیر عمل کنید:



برای ایجاد Rule جدید، بر روی add کلیک کنید، بعد از ایجاد در قسمت name، نام رول را وارد کنید و بعد در قسمت Detected content بر روی Any دوبار کلیک کنید تا شکل بعد ظاهر شود.



در این قسمت برای وارد کردن آدرس سایت بر روی URL Hostname کلیک کنید.

در این شکل و در قسمت **Site**، آدرس سایت مورد نظر خود را وارد و بر روی **ok** کلیک کنید.

Content Rules				
Forbidden Words				
Kerio Control Web Filter				
HTTPS Filtering				
Advanced Settings				
<input type="checkbox"/>	Name	Detected content	Source	Action
<input checked="" type="checkbox"/>	Block 3isco.ir	3isco.ir	Any	No action

همانطور که در شکل بالا مشاهده می کنید، سایت **3isco.ir** به قسمت **detected content** اضافه شده است، در قسمت شماره ۱ دو، یعنی **source**، شما می توانید کاربر یا گروه مورد نظر را که باید این **Rule** روی آن اعمال شود را انتخاب کنید که در این قسمت، نباید تنظیمی اعمال کنید و اگر تنظیمی اعمال نکنید، روی تمامی کاربران و گروه ها، این **Rule** اعمال خواهد شد. در قسمت شماره ۳ باید دسترسی را مشخص کنید، برای این کار بر روی **No Action** در قسمت شماره ۳، دو بار کلیک کنید تا شکل بعد ظاهر شود.

در این صفحه و در قسمت **Action**، سه گزینه وجود دارد که اگر گزینه **Allow** را انتخاب کنید، کاربران می توانند سایت مورد نظر را باز کنند، اگر گزینه **Deny** را انتخاب کنید، کاربران نمی توانند وارد سایت شوند و یک صفحه ی کریو برای برای آنها باز خواهد شد که به آنها اعلام می کند، سایت مورد نظر مسدود شده است.

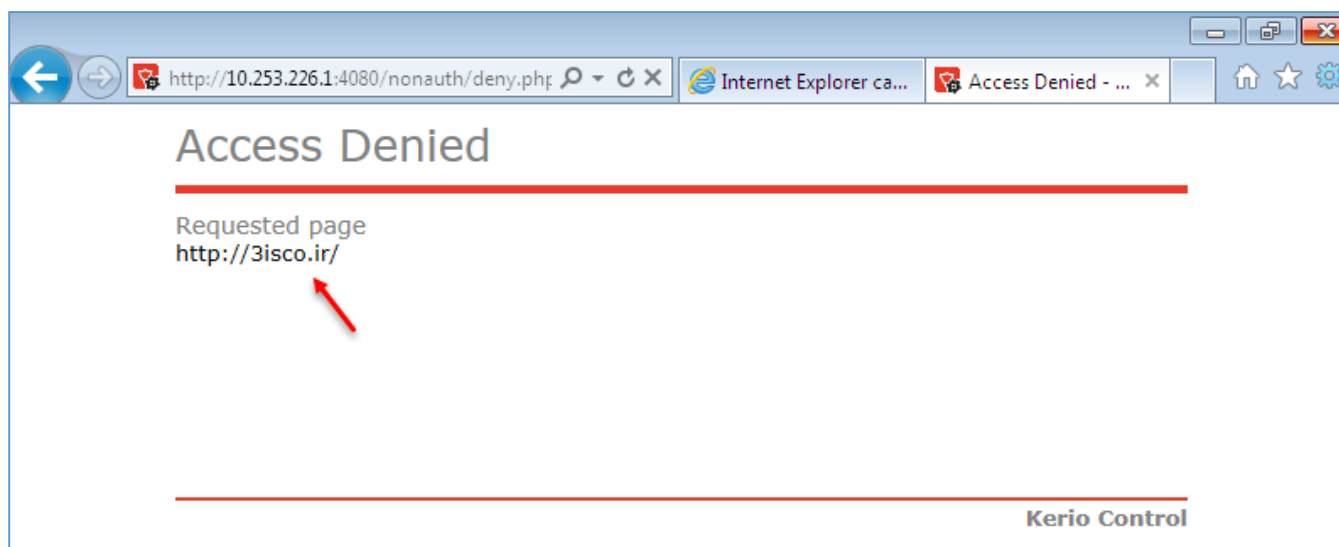
اگر گزینه **Drop** را انتخاب کنید، درخواست باز کردن سایت توسط کاربر رد خواهد شد و **Not Page** برای کاربر مورد نظر، نمایش داده خواهد شد.

Content Filter Admin

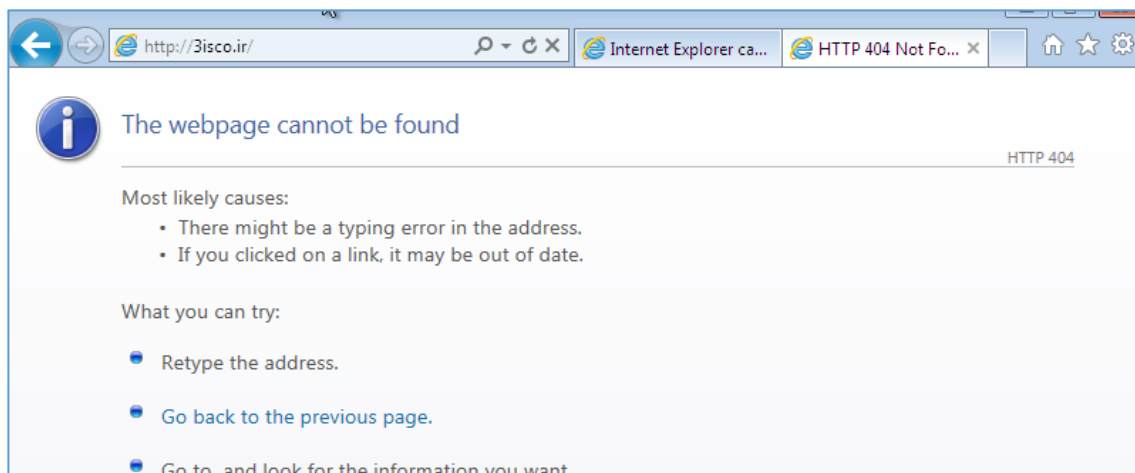
Content Rules Forbidden Words Kerio Control Web Filter HTTPS Filtering Advanced Settings

Name	Detected content	Source	Action	Valid Time
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Deny	
<input checked="" type="checkbox"/> Kerio sites	kerio.com samepage.io	Any	Allow Additional settings	
<input type="checkbox"/> Advertisements and banners	Ads/banners	Any	Drop	
<input type="checkbox"/> Updates and MS Windows activa...	Automatic Updates	Any	Allow Additional settings	
<input checked="" type="checkbox"/> Kerio Control Web Filter categor...	Anonymizer Botnet	Any	Deny Additional settings	

همانطور که در شکل بالا مشاهده می‌کنید، گزینه‌ی **Deny** انتخاب شده است، بعد از انتخاب بر روی **Apply** کلیک کنید تا تنظیمات ذخیره شود.



در صفحه‌ی بالا، کاربر مورد نظر با درخواست بازکردن سایت **3isco.ir** با صفحه‌ی **Access Denied** روبرو شده است که اگر در قسمت قبل، گزینه‌ی **Drop** را انتخاب می‌کردید با صفحه‌ی زیر مواجه می‌شدید:



Content Filter

Content Rules | Forbidden Words | Kerio Control Web Filter | HTTPS Filtering | Advanced Settings

Name	Detected content	Source	Action
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Drop
<input checked="" type="checkbox"/> Kerio sites		Any	Allow + Additional settings
<input type="checkbox"/> Advertisements and banners		Any	Drop
<input type="checkbox"/> Updates and MS Windows ac		Any	Allow + Additional settings
<input checked="" type="checkbox"/> Kerio Control Web Filter cate		Any	Deny + Additional settings

Context menu options: Add, Remove, Duplicate, Change Color, Change Description..., Edit Time Ranges...

در شکل بالا، ما یک Rule در قسمت قبل ایجاد کردیم که برای ایجاد یک نمونه‌ی کپی از Rule قبلی باید بر روی آن کلیک راست کنید و گزینه‌ی Duplicate را انتخاب کنید.

Content Rules | Forbidden Words | Kerio Control Web Filter | HTTPS Filtering | Advanced Settings

Name	Detected content	Source	Action
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Drop
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Allow
<input checked="" type="checkbox"/> Kerio sites	kerio.com samepage.io	Any	Allow + Additional setti

همانطور که مشاهده می‌کنید، دو Rule در لیست وجود دارد که یکی برای بستن سایت 3isco.ir و دیگری برای بازکردن آن است، اما در این لیست، تمام Rule ها به ترتیب اولویت عمل می‌کنند که در این شکل نیز سایت 3isco.ir بسته خواهد شد و قسمت دوم که برای باز کردن سایت ایجاد شده است، عمل نخواهد کرد.

انتقال کاربر از سایت مسدود شده به سایت دیگر:

زمانی که یک سایت را برای کاربر مسدود می‌کنید، می‌توانید یک مسیر جایگزین قرار دهید تا کاربر با درخواست سایت مسدود شده به سایت جدید انتقال داده شود.

Name	Detected content	Source	Action
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Drop
<input checked="" type="checkbox"/> Kerio sites	kerio.com samepage.io	Any	Allow + Additional settings
<input type="checkbox"/> Advertisements and banners	Ads/banners	Any	Drop

در شکل صفحه‌ی قبل و در قسمت **Drop**، دو بار کلیک کنید.
 در صفحه‌ی روبرو در قسمت **Action**، گزینه‌ی **Deny** را انتخاب کنید و در قسمت **HTTP Actions**، تیک گزینه‌ی **Redirect to** را انتخاب و بر روی **ok** کلیک کنید.
 با این کار، کاربرانی که سایت **3isco.ir** را درخواست می‌کنند به سایت **Google.com** انتقال داده خواهند شد.

Content Filter				
Content Rules				
Name	Detected content	Source	Action	Valid Time
<input checked="" type="checkbox"/> Block 3isco.ir	3isco.ir	Any	Deny + Additional settings	
<input checked="" type="checkbox"/> Kerio sites	kerio.com samepage.io	Any	Deny	
<input type="checkbox"/> Advertisements and banners	Ads/banners	Any	Drop	
<input type="checkbox"/> Updates and MS Windows activa...	Automatic Updates	Any	Allow + Additional settings	
<input checked="" type="checkbox"/> Kerio Control Web Filter categor...	Anonymizer Botnet	Any	Deny + Additional settings	

تذکر: در شکل بالا برای اینکه سایت کریو را ببندیم تا احتمال آپدیت کریو کنترلر نیز کم شود، **Rule** مربوط به **Kerio Sites** را بر روی **Deny** قرار می‌دهیم تا با مشکلی در ادامه‌ی کار روبرو نشویم.
 تا به اینجا یک **Rule** ایجاد کردیم که یک سایت را برای کاربران بست، گزینه‌های دیگری هم وجود دارد که خودتان آن‌ها را بررسی کنید، البته در ادامه‌ی کتاب هم سعی می‌کنیم این گزینه‌ها را در صورت نیاز تست کنیم.

بررسی تب Forbidden Words در ContentFilter:

Content Filter

Content Rules | **Forbidden Words** | Kerio Control Web Filter | HTTPS Filtering | Advanced Settings

Settings

Enable Forbidden words filtering

Deny pages if their weight reaches:

Forbidden Words

Item	Weight	Description
Pornography		
Warez/Cracks		

در این تب به صورت پیش فرض، یک سری کلمات در دو گروه تعریف شده است که برای جلوگیری از دسترسی کاربر به سایت‌های مستهجن و دیگر سایت‌ها است که باید کلمات آن را در این صفحه وارد کنید، در قسمت **Deny Pages if their weight reaches**، عدد ۷۰ را مشاهده می‌کنید که این عدد به این نکته اشاره دارد که اگر تعداد کلمات در آن سایت، بیشتر از ۷۰ باشد آن سایت برای کاربر باز نخواهد شد، این موضوع را می‌توانید با کم و زیاد کردن این عدد، تست بگیرید.

اگر به سایت روبرو توجه کنید، در آن کلمه‌ی **Hack** به تعداد ۹۸ بار تکرار شده است و سایت، به راحتی باز شده است، اما اگر سرویس فیلترینگ کلمه فعال باشد، این سایت باز نخواهد شد.

Find: hack 98 matches

Merriam-Webster SINCE 1828 MENU

hack
verb | \ˈhɑk/

Definition of HACK

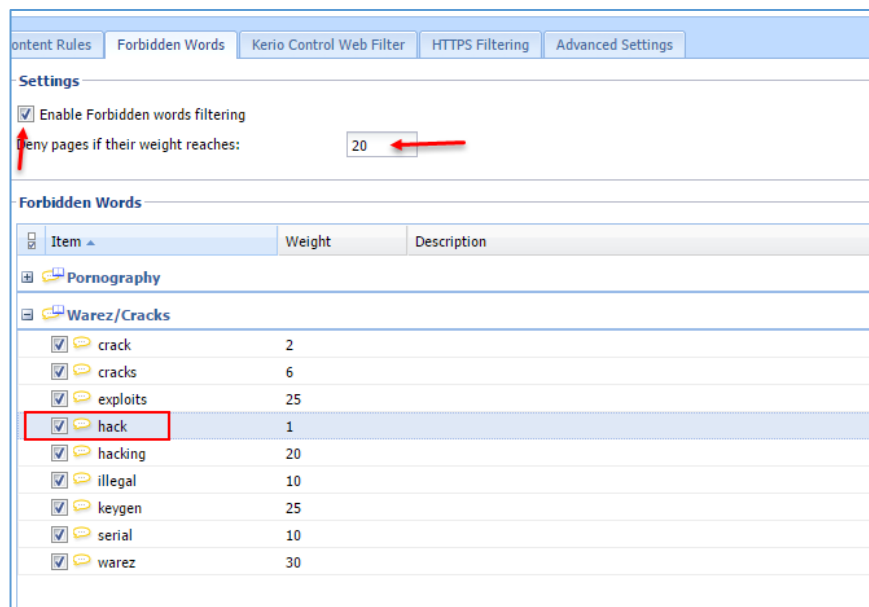
transitive verb

1 a

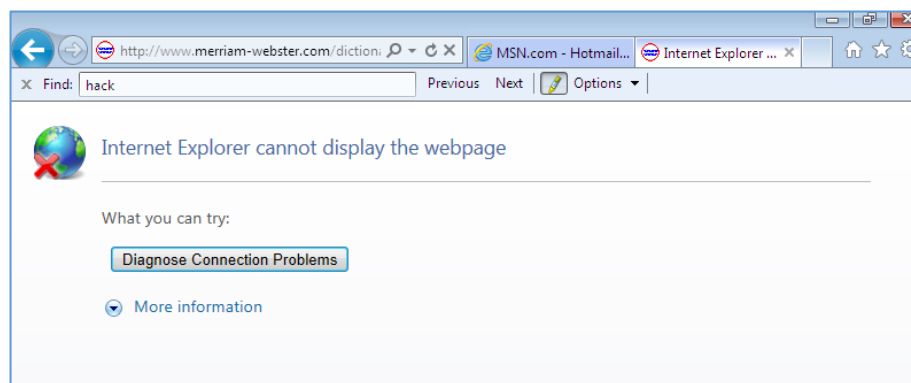
WORD OF THE DAY

10:18 PM 7/22/2016

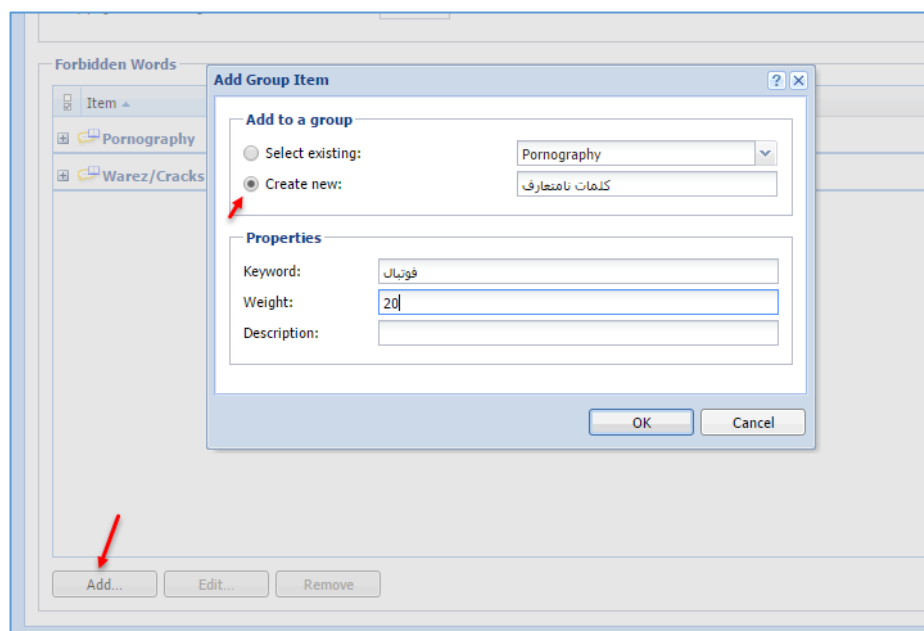
در شکل روبرو سرویس فعال شده است و مقدار **Weight** بر روی ۲۰ قرار داده شده است و کلمه **Hack** نیز در گروه **Warez / Cracks** قرار داده شده است، اگر بر روی **ok** کلیک کنید، سایت مورد نظر باز نخواهد شد.



همانطور که مشاهده می کنید، سایت مورد نظر باز نشد.



برای ایجاد گروه جدید باید بر روی **Add** کلیک کنید و در صفحه‌ی باز شده، گزینه‌ی **Create new**، نام گروه مورد نظر خود را وارد کنید و در قسمت **Keyword**، نام کلمه‌ی خود را وارد کنید و تعداد تکرار آن را نیز بنویسید و بر روی **ok** کلیک کنید.



بررسی تب Kerio Control Web Filter

Content Filter

Content Rules | Forbidden Words | **Kerio Control Web Filter** | HTTPS Filtering | Advanced Settings

Settings

- Enable Kerio Control Web Filter
- Categorize each page regardless of URL rules
- Allow authenticated users to report miscategorized URLs (on the Deny page)

http://

⚠ Kerio Control Web Filter is not activated, categorization is disabled.

Kerio Control Web Filter whitelist

URL ▲	Description
<i>Nothing to display</i>	

در این قسمت که برای فیلترینگ وبسایتها کاربرد دارد، یک دیکشنری از سایت‌هایی که کاربران در سرتاسر دنیا آن را ایجاد کردند، وجود دارد که بنا به رتبه‌ی آن سایت، سایت‌ها فیلتر خواهند شد که برای فعال کردن آن باید سه تا تیک اول را انتخاب کنید، توجه داشته باشید که این سرویس برای فعال شدن نیاز به لایسنس دارد.

بررسی تب HTTPS Filtering:

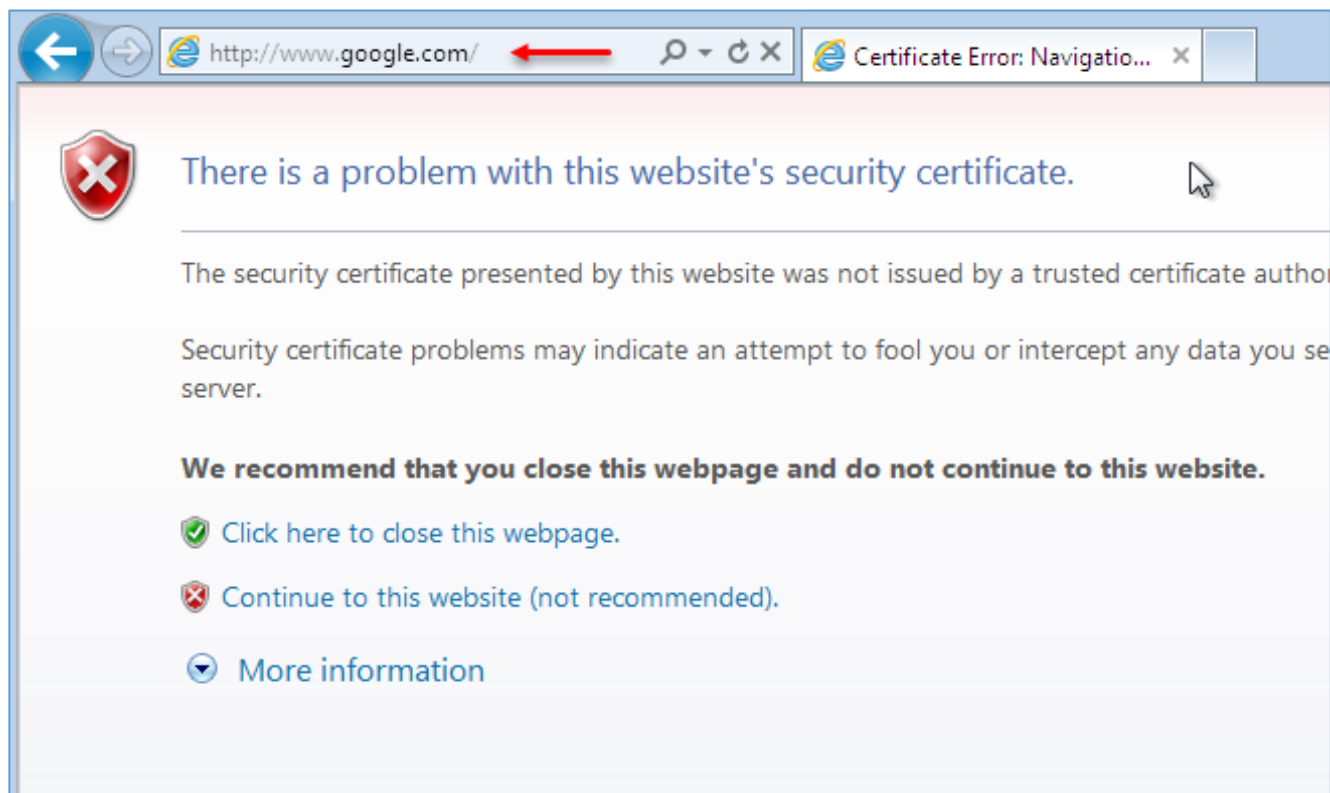
در تمام فایروال‌ها به صورت پیش فرض، ترافیکی که با پروتکل HTTPS رد و بدل می‌شود، کنترل نمی‌شود و نمی‌توانیم سایت‌هایی را که از این پروتکل استفاده می‌کنند را کنترل کنیم، اما اگر بخواهیم این ترافیک را کنترل کنیم، می‌توانیم در کریو، سرویس **HTTPS Filtering** را فعال کنیم، برای فعال کردن این سرویس به شکل زیر توجه کنید:

The screenshot shows the 'Content Filter' configuration page with the 'HTTPS Filtering' tab selected. Under 'HTTPS decryption', the checkbox 'Decrypt and filter HTTPS traffic' is checked. Below it, there are links for 'Learn more about HTTPS filtering and how to install certificate on client OS or via Active Directory®'. Under 'HTTPS Filtering Exceptions', the radio button 'Exclude specified traffic from decryption' is selected. There are also input fields for 'Traffic to/from IP addresses which belong to:' (set to 'HTTPS exclusions') and 'Traffic from the following users:' (set to 'None').

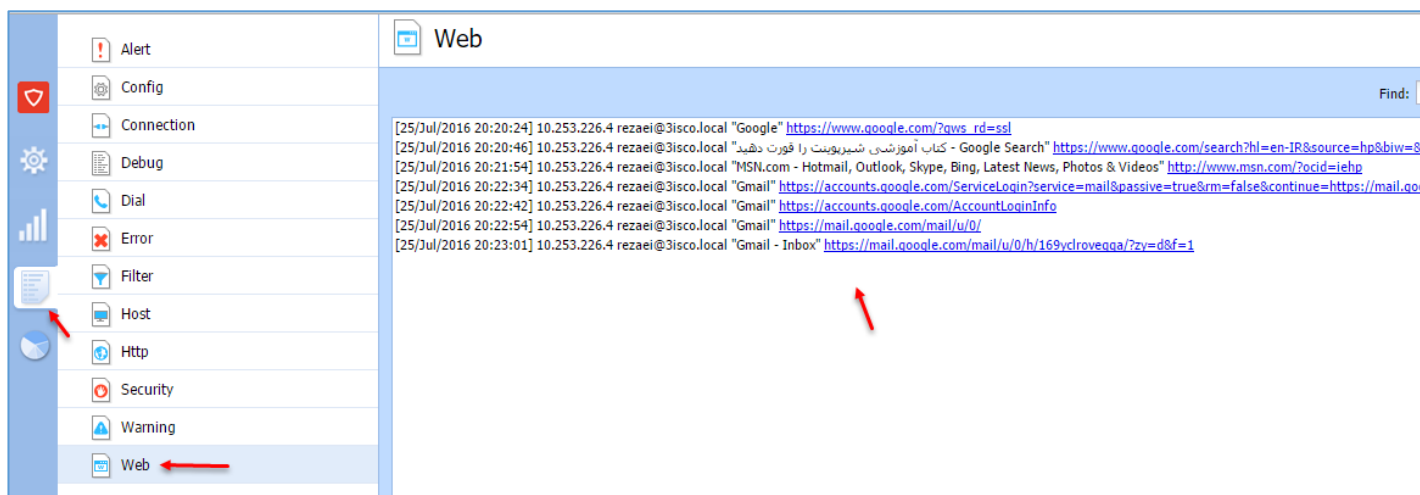
در این قسمت برای فعال کردن، تیک گزینه **Decrypt and filter HTTPS traffic** را انتخاب و بر روی **Apply** کلیک کنید تا اطلاعات ذخیره شود.

با این کار، کریو بین شما و سایت مورد نظر که از پروتکل HTTPS استفاده می‌کند، قرار می‌دهد که اگر شما بخواهید سایتی را باز کنید با پیغام نامعتبر بودن گواهینامه روبرو خواهید شد.

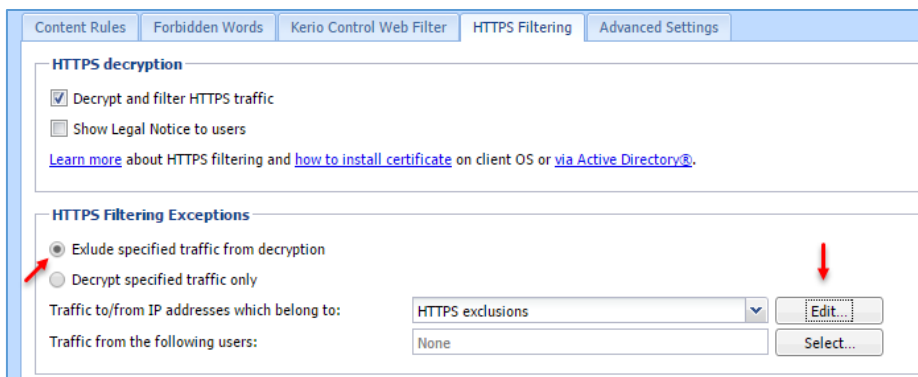
برای مثال، سایت **Google** را که از پروتکل HTTPS استفاده می‌کند را بعد از فعال کردن سرویس، دوباره اجرا کنید.



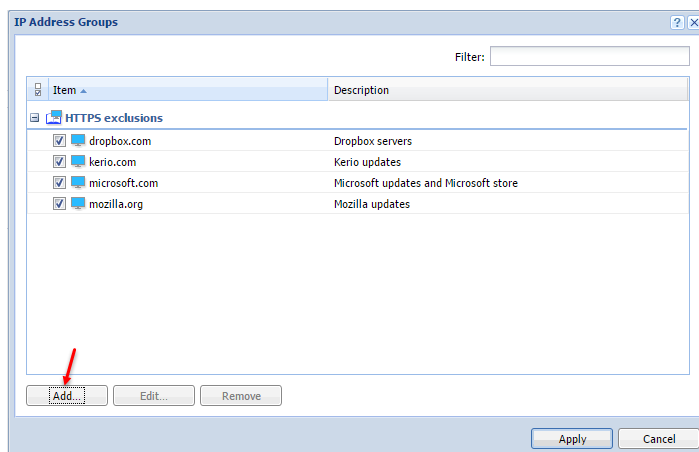
همانطور که در شکل بالا مشاهده می‌کنید، بعد از اجرا شدن سایت **Google** با خطای گواهینامه روبرو شدید که آن نیز به این دلیل است که سرویس **HTTPS Filter**، فعال شده است؛ برای ادامه‌ی کار و ورود به سایت باید بر روی **Continue to this website** کلیک کنید.



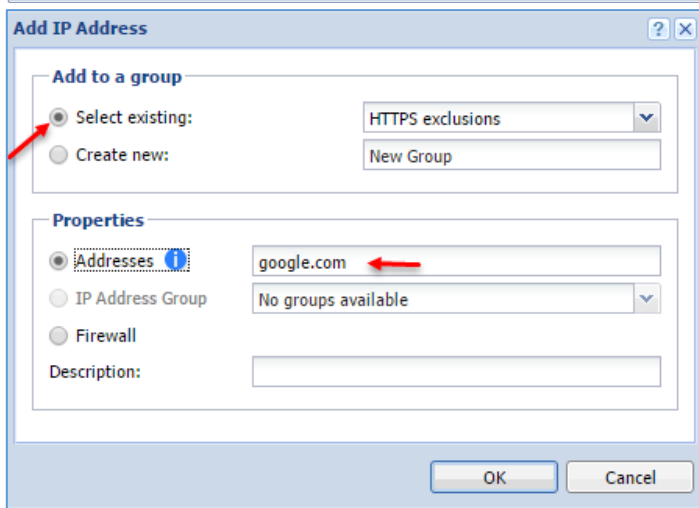
اگر وارد **Log** شوید و به قسمت **Web** مراجعه کنید، مشاهده می‌کنید سایت‌هایی که با پروتکل **HTTPS** باز شده است، در این قسمت لیست شده است و ترافیک آن ثبت خواهد شد.



توجه داشته باشید برای اینکه بخواهید سایت‌های خاصی را از این سرویس خارج کنید و دیگر اطلاعات آن در **Log** ثبت نشود باید به مانند شکل روبرو، گزینه‌ی **Exclude...** را انتخاب و در قسمت لیست بر روی **Edit** کلیک کنید.



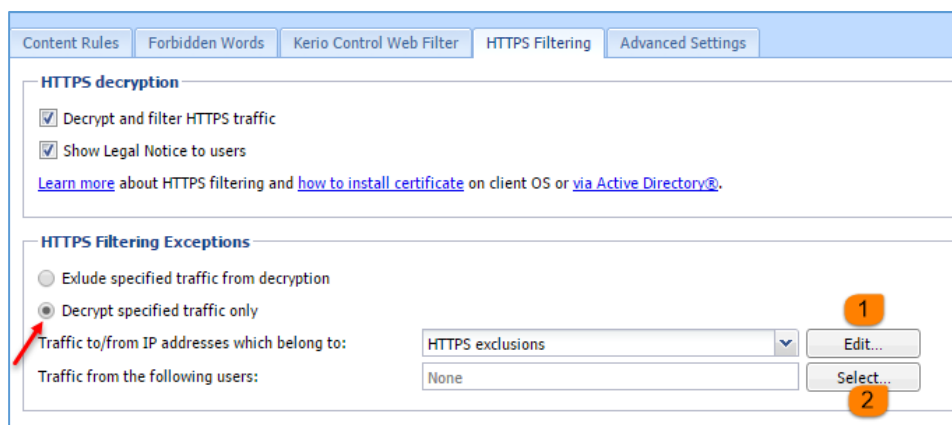
در شکل روبرو، چند سایت به صورت پیش فرض در لیست قرار دارد که برای اینکه سایت دلخواه خود را به لیست اضافه کنید باید بر روی **Add** کلیک کنید.



در شکل روبرو و در قسمت **Add to a group** می‌توانید با انتخاب گزینه‌ی اول، گروه پیش فرض را انتخاب کنید یا گزینه‌ی **Create new** را انتخاب و نام گروه جدید خود را وارد کنید و در قسمت **Addresses**، نام سایت را وارد و بر روی **ok** کلیک کنید.

با این کار، دیگر سایت **Google** در سرویس **HTTPS**

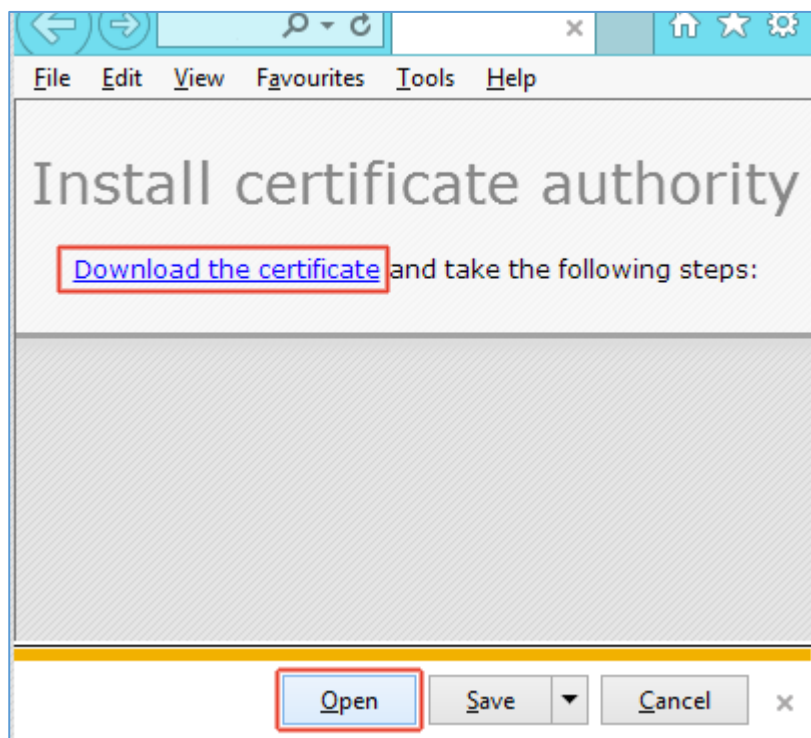
Filter قرار نمی‌گیرد و اگر بعد از این کار، وارد سایت شوید با خطایی مواجه نخواهید شد.



اگر بخواهید، تنها سایت‌های خاصی را کنترل کنید باید گزینه‌ی **Decrypt...** را انتخاب و در گروه مورد نظر، سایت‌های خود را وارد کنید.

نکته: اگر بخواهید این

سرویس‌ها را برای کاربر خاصی فعال کنید، در قسمت شماره‌ی دو باید بر روی **Select** کلیک کنید و کاربر مورد نظر خود را از لیست انتخاب کنید.



اگر در شکل بالا تیک گزینه‌ی **Show Legal Notice to Users** را انتخاب کنید، زمانی که کاربر بخواهد سایت‌های **HTTPS** را باز کند، یک صفحه به مانند شکل روبرو برای او نمایش داده خواهد شد که با دانلود گواهینامه و نصب آن، کار **Trust** برای دسترسی به سایت‌ها انجام می‌شود و دیگر سایت‌ها با خطا باز نخواهند شد.

بررسی Bandwidth Management QOS

در این بخش، می‌توانید برای دسترسی به اینترنت، محدودیت‌هایی از نظر سرعت دانلود و آپلود تعیین کنید تا با این کار، کاربران را محدود کنید، مثلاً اگر کاربری اقدام به دانلود یک فایل کرد، به خاطر اینکه این قسمت فعال نیست، کل پهنای باند شبکه درگیر می‌کند و کاربران دیگر نمی‌توانند به خوبی از اینترنت استفاده کنند، برای حل این مشکل که یکی از این مشکلات است باید Bandwidth Management QOS را برای کل شبکه فعال کنید.

The screenshot shows the 'Bandwidth Management and QoS' configuration page. The left sidebar contains various system settings, with 'Bandwidth Management and QoS' selected. The main area displays a table of 'Bandwidth Management rules' with columns for Name, Traffic, Download, Upload, Interface, and Valid Time. Below the table are buttons for 'Add', 'Remove', and 'More Actions'.

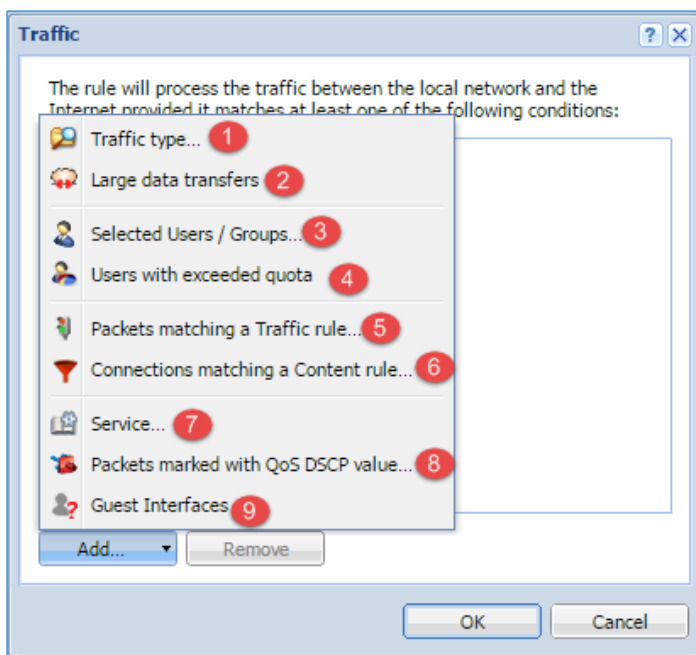
Name	Traffic	Download	Upload	Interface	Valid Time
<input type="checkbox"/> SIP VoIP	<input checked="" type="checkbox"/> SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All	
Other traffic	Any	No limit	No limit	All	

به مانند شکل بالا وارد Bandwidth Management QOS شوید؛ در این صفحه، گزینه‌های مختلفی را مشاهده می‌کنید که با ایجاد یک Rule جدید می‌توانید این گزینه‌ها را بررسی کنید؛ برای ایجاد Rule جدید بر روی Add کلیک کنید.

This close-up shows the 'Bandwidth Management rules' table after a new rule has been added. The 'Traffic Control' rule is selected, and its 'Traffic' type is set to 'Any'.

Name	Traffic	Download
<input checked="" type="checkbox"/> Traffic Control	Any	No limit
<input type="checkbox"/> SIP VoIP	<input checked="" type="checkbox"/> SIP VoIP	Reserve: 24 KB/s
Other traffic	Any	No limit

همانطور که مشاهده می‌کنید، یک Rule با نام Traffic Control ایجاد کردیم که برای اینکه این Rule را به کاربر، گروه و ... ارتباط دهیم در قسمت Traffic و آنجا که نوشته شده، any دو بار کلیک می‌کنیم تا شکل بعد ظاهر شود.



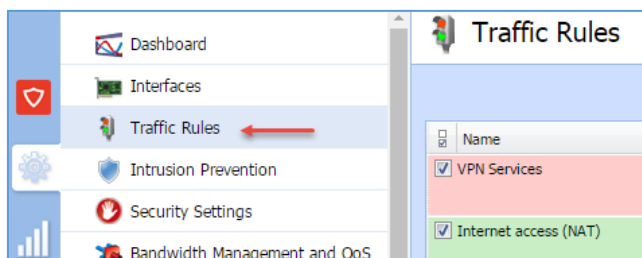
وقتی که بر روی **Add** کلیک کنید، گزینه‌های مختلف را که در شکل روبرو شماره‌گذاری کردیم را مشاهده می‌کنید که با هم آن‌ها را بررسی می‌کنیم:

۱- اگر این گزینه را انتخاب کنید، می‌توانید نوع ترافیک ورودی و خروجی را مشخص و محدود کنید، مثلاً می‌توانید نوع **Multimedia** را انتخاب کنید که فایل‌های صوتی و تصویری محدود خواهد شد.

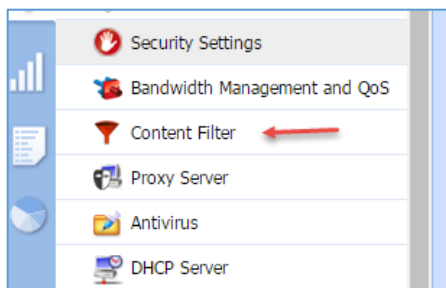
۲- این قسمت برای محدود کردن فایل‌هایی با حجم زیاد است.

۳- در این قسمت، شما می‌توانید کاربران و گروه‌های خود را به لیست اضافه کنید تا محدودیت روی آن‌ها اعمال شود.

۴- با فعال کردن این قسمت، همه‌ی کاربران محدود خواهند شد که در ادامه‌ی کار، این قسمت را تست خواهیم گرفت.



۵- این قسمت مربوط به **Rule** هایی است که در قسمت **Traffic Rule** نوشته‌اید که در شکل روبرو مشخص شده است.

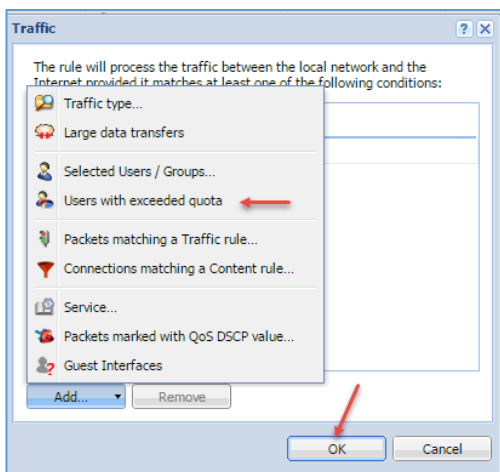


۶- این قسمت مربوط به **Content Rule** است که عکس آن را مشاهده می‌کنید.

۷- با انتخاب این گزینه، لیست سرویس‌ها برای شما ظاهر خواهد شد و شما می‌توانید سرویس خاصی را به لیست اضافه و روی آن محدودیت تعریف کنید.

۸- این قسمت برای **Packet Marked** است که اگر نیاز بود به شما توضیح خواهیم داد.

۹- این قسمت هم مربوط به **interface Guest** یا همان مهمان است که در اوایل کتاب توضیح دادیم.



برای تست کار، از گزینه‌های موجود بر روی **Users with exceeded quota** کلیک کنید، با این کار هر محدودیتی که در این Rule تعریف کنید برای تمامی کاربران تعریف خواهد شد.
بر روی **ok** کلیک کنید تا کار ادامه یابد.

The Bandwidth Management allows you to fine-tune your Internet bandwidth utilization. You can reserve as well as limit bandwidth for selected traffic.

Bandwidth Management rules

Name	Traffic	Download	Upload	Interface	Valid Time
<input checked="" type="checkbox"/> Traffic Control	Exceeded quota	Limit: 100 KB/s	Limit: 100 KB/s	All	
<input type="checkbox"/> SIP VoIP	SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All	
Other traffic	Any	No limit	No limit	All	

Download Bandwidth Policy

Apply the following bandwidth policy:

Reserve at least: 0 Mbit/s

Do not exceed: 100 KB/s

Buttons: Add, Remove, OK, Cancel

VPN tunnels

در شکل بالا برای تعریف سرعت دانلود و آپلود باید در جایی که مشخص شده، دو بار کلیک کنید تا شکل بالایی آن ظاهر شود؛ در این قسمت، دو گزینه وجود دارد که گزینه **Reserve at least** برای اختصاص دادن یک سرعت یا همان رزرو کردن سرعت برای کاربران است، مثلاً می‌توانید حداقل سرعت کاربران در هنگام دانلود، ۱۰۰ کیلوبایت باشد، یعنی همیشه سرعت کاربر بیشتر از سرعت ۱۰۰ کیلوبایت خواهد بود، اما گزینه **Do not exceed** که در این قسمت شما می‌توانید حداکثر سرعت کاربران را مشخص کنید که در شکل بالا، سرعت ۱۰۰ کیلوبایت برای کاربران مشخص شده است، بعد از وارد کردن سرعت بر روی **ok** کلیک کنید و بعد بر روی **Apply** کلیک کنید.

you to fine-tune your Internet bandwidth utilization. You can reserve as well as limit bandwidth for selected traffic.

Traffic	Download	Upload	Interface	Valid Time	Chart
Exceeded quota	Limit: 100 KB/s	Limit: 100 KB/s	All		<input type="checkbox"/>
SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All		<input checked="" type="checkbox"/>
Any	No limit	No limit	All		

1% 14300.1000.160324-1723.RS1_RELEASE_S...ISO

وضعیت دانلود | محدود کننده سرعت | گزینه های اتمام دانلود

http://care.dlservice.microsoft.com/dl/download/8/9/2/89284B3B-BA51-49C8-90F8-59C0A58D0E7

وضعیت: در حال دریافت ...

حجم فایل: 4.842 GB

حجم دانلود شده: 98.696 MB (1.99 %)

سرعت دانلود: 99.241 KB/sec

زمان باقیمانده: 13 ساعت و 25 دقیقه

قابلیت ایست: دارد

انصراف | ایست | پنهان کردن جزئیات <<

نقاط شروع و دانلود به ترتیب اتصال

Download: 15 Mbit/s

همانطور که در شکل بالا مشاهده می کنید، کاربر در حال دانلود یک فایل است که سرعت آن، زیر ۱۰۰ کیلوبایت است و هیچ وقت سرعت آن بیشتر از این نخواهد شد، البته در بعضی اوقات، اگر شما سرعت را بر فرض مثال ۱۰۰ کیلوبایت در نظر بگیرید، شاید سرعت تا چند کیلوبایت بالاتر از این هم تغییر کند که این مورد از تغییرات عادی است.

serve as well as limit bandwidth for sele

Upload	Int
Limit: 100 KB/s	
Reserve: 24 KB/s	
No limit	

در قسمت آپلود هم می توانید سرعت خود را مشخص کنید که این موضوع را در شکل روبرو مشاهده می کنید.

The Bandwidth Management allows you to fine-tune your Internet bandwidth utilization. You can reserve as well as limit bandwidth for selected traffic.

Bandwidth Management rules

Name	Traffic	Download	Upload	Interface	Valid Time	Chart
<input checked="" type="checkbox"/> Traffic Control	Exceeded quota	Limit: 100 KB/s	Limit: 100 KB/s	All	New Time Range	<input type="checkbox"/>
<input type="checkbox"/> SIP VoIP	SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All		<input checked="" type="checkbox"/>
Other traffic	Any	No limit	No limit	All		

VPN tunnels

Use rules for VPN tunnels before

Internet bandwidth

Ethernet 2
Download: 2.7 Mbit/s
Upload: 3 Mbit/s

در قسمت **Valid Time** نیز شما می‌توانید محدودیتی را که برای کاربران ایجاد کردید را در ساعت مشخصی اجرا کنید، برای ست کردن ساعت در قسمت **Valid Time**، یک گزینه با نام **New Time Range** است که برای اینکه ساعتی که در آن مشخص شده است را مشاهده و تنظیم کنید باید در قسمت **More Actions** بر روی **Edit Time Ranges** کلیک کنید.

Time Ranges

Filter:

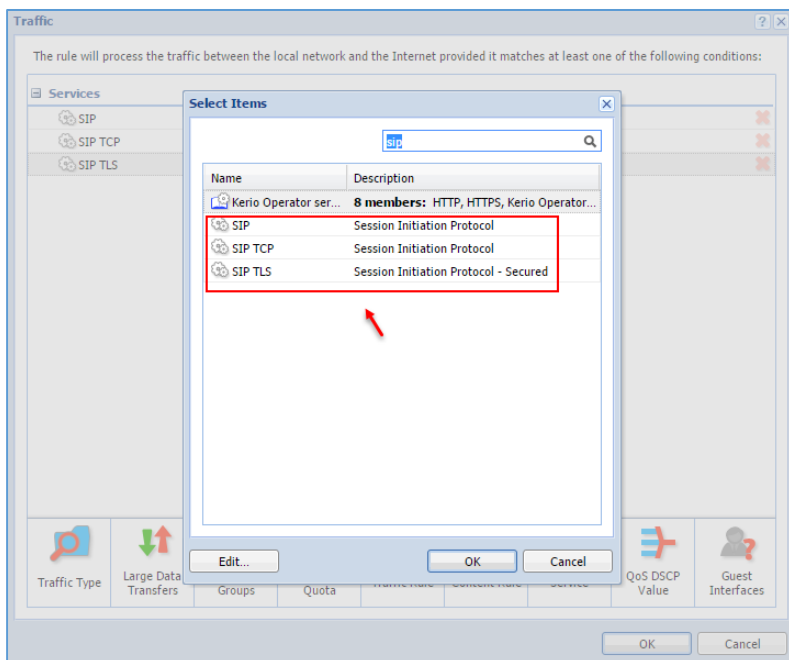
Item	Description	Valid on
New Time Range		
<input checked="" type="checkbox"/> Daily from 00:00 to 23:59		All days

در شکل روبرو و در قسمت **New Time Range**، ساعت دسترسی کاربران مشخص شده است که برای تنظیم کردن آن باید به صورت دلخواه بر روی **Edit** کلیک کنید.

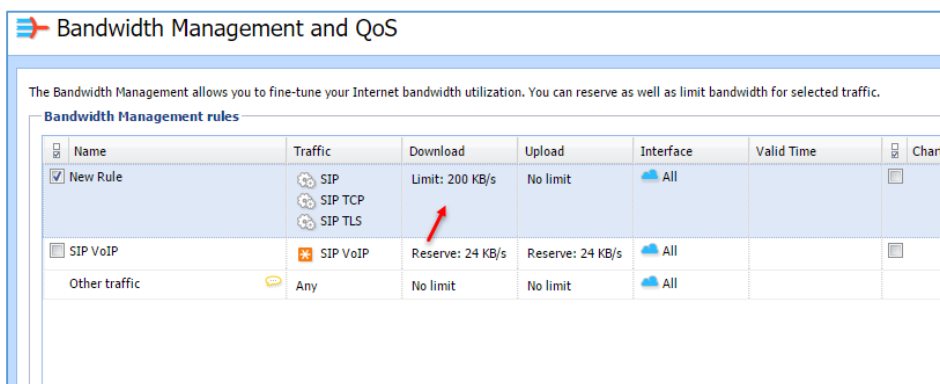
در این قسمت، شما می‌توانید روزانه، هفتگی و ماهانه را در قسمت **Type** مشخص کنید و در قسمت **From**، ساعت شروع محدودیت و در قسمت **To**، ساعت پایان محدودیت را مشخص کنید، در آخر نیز می‌توانید روزهای هفته را مشخص و بر روی **ok** کلیک کنید.

محدودیت سرعت بر روی سرویس خاص:

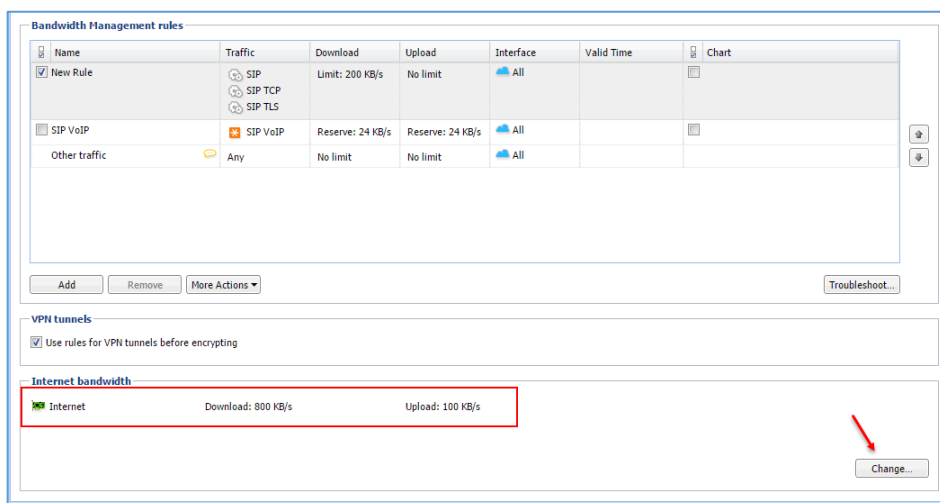
در قسمت **Traffic** بر روی **Service** کلیک کنید تا شکل بعد ظاهر شود.



در این صفحه، بر فرض می‌خواهیم پروتکل SIP که برای ارتباط صوتی و تصویری کاربرد دارد را محدود کنیم؛ در قسمت جستجو، کلمه‌ی SIP را وارد و همه‌ی گزینه‌ها را به لیست اضافه و بر روی OK کلیک کنید.



بعد از اضافه کردن Rule در قسمت Download می‌توانید به مانند قبل، سرعتی را برای آن مشخص کنید.



برای اینکه پهنای باند کل شبکه را کنترل کنید باید به مانند شکل روبرو به قسمت Internet Bandwidth بروید و می‌توانیم مقدار دانلود و آپلود را برای کل شبکه مشخص کنید، برای این کار باید بر روی Change کلیک کنید و سرعت دانلود و آپلود را مشخص کنید.

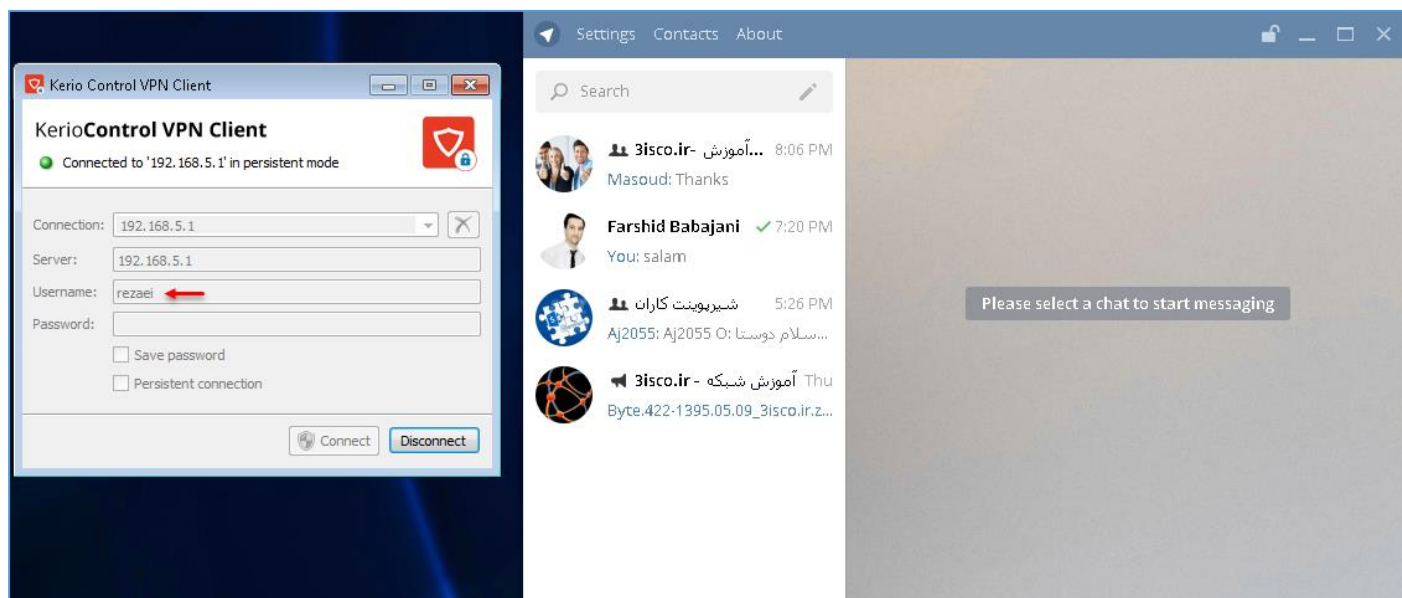
مدیریت و بستن تلگرام در کریو:

یکی از مشکلاتی که مدیران شبکه با آن روبرو هستند، آن است که کاربران در شبکه از نرم‌افزارهای مسنجر استفاده می‌کنند که پهنای باند زیادی را مصرف می‌کند و قابل کنترل نیست، اما روش‌هایی وجود دارد تا بتوان آن را به کنترل خود درآورد یا این کار را انجام داد؛ طبق مراحل کتاب پیش بروید:

مرحله اول – پیدا کردن IP نرم‌افزار تلگرام:

برای اینکه بتوانید نرم‌افزار تلگرام را در شبکه قطع کنید باید آدرس آن را بدست آورید، توجه داشته باشید کاربران بر روی سیستم‌های خود از دو ورژن تحت ویندوز و تحت وب تلگرام استفاده می‌کنند که باید آدرس آن‌ها را بدست آورید.

با یکی از کاربرانی که در **Active Directory** ایجاد کردید، از طریق **VPN** به اینترنت متصل شوید و بعد از آن، نرم‌افزار تلگرام را اجرا کنید و وارد حساب خود شوید.



همانطور که در شکل بالا مشاهده می‌کنید، کاربر **Rezaei** از طریق **VPN** به کریو و اینترنت متصل شده است و بعد از متصل شدن به اینترنت، تلگرام را هم اجرا کرده است که با این کار می‌توانید در کریو، اطلاعات **IP** را بدست آورید.

Active Connections

1 item (0 selected) Filter:

Traffic Rule	Service	Source	Destination	Bandwidth Management Ru...	Load Bal...
Internet access (NAT)	HTTPS	10.253.226.4	91.108.4.163		Internet

Select a connection to view its details

2 Hide local connections Show DNS names Auto-refresh

در شکل بالا وارد Kerio Controller و بعد وارد Status شوید و بر روی Active Connections که در قسمت شماره‌ی یک مشخص شده است، کلیک کنید که این قسمت، تمام ارتباطات کاربر را به صورت کلی نمایش می‌دهد، از آنجایی که ما احتیاج به ارتباط داخلی نداریم و می‌خواهیم آدرس IP تلگرام را بدست آوریم، بهتر است تیک گزینه‌ی شماره‌ی دو را انتخاب کنیم تا ارتباطات داخلی در لیست نمایش داده نشود، همانطور که در قسمت شماره‌ی سه مشاهده می‌کنید، یک Connection از نوع HTTPS مشخص شده است که این همان ارتباط تلگرام است و IP آن 91.108.4.163 می‌باشد، ما باید روی این IP، یک Rule در قسمت Traffic Rule تعریف کنیم و این آدرس را

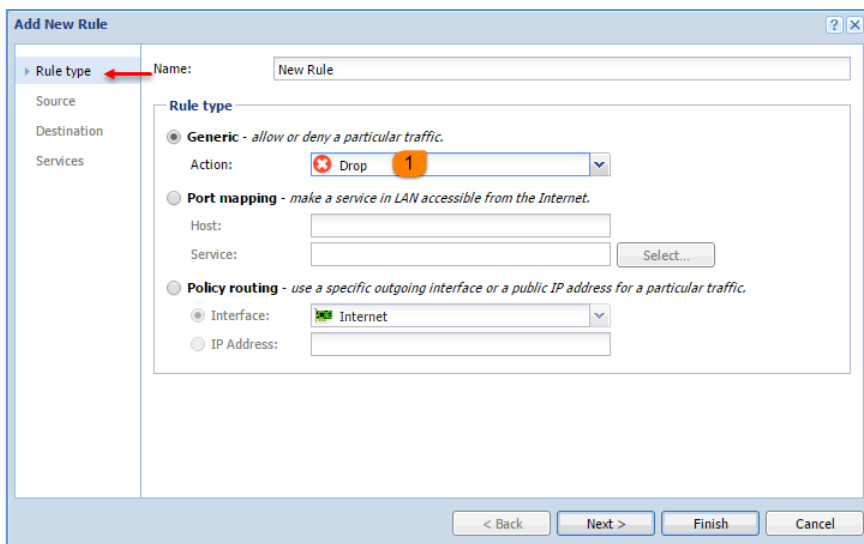
بیندیم.

وارد Traffic Rules شوید و برای ایجاد Rule جدید بر روی Add کلیک کنید.

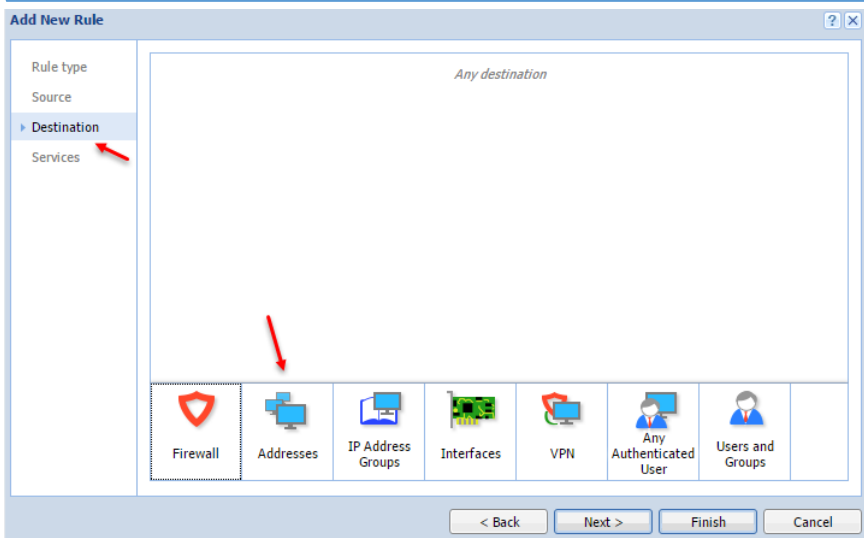
Traffic Rules

Search:

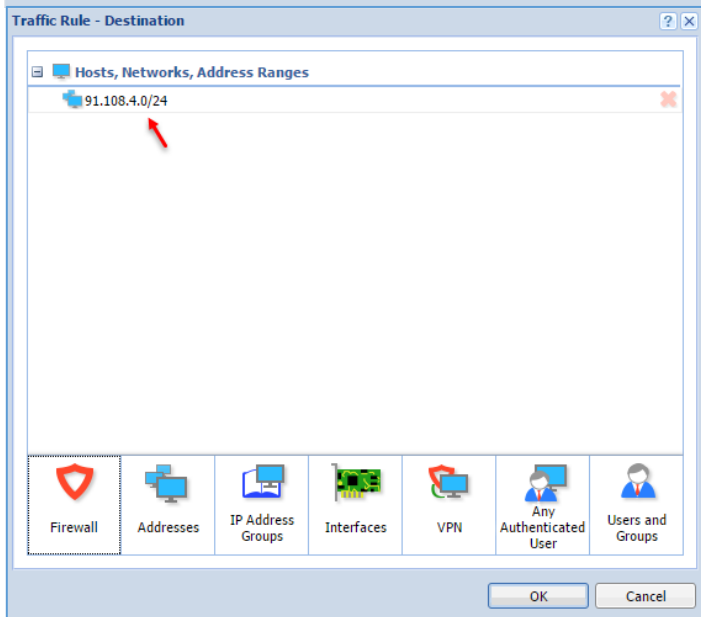
Name	Source	Destin
<input type="checkbox"/> VPN Services	Any	Fi
<input type="checkbox"/> Web Services	Any	Fi
<input checked="" type="checkbox"/> Internet access (NAT)	VPN clients	In
<input checked="" type="checkbox"/> Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Fi Tr Vi Al
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any
<input checked="" type="checkbox"/> Guests traffic	Guest Interfaces	Fi
<input type="checkbox"/> Block other traffic	Any	Any



در قسمت Rule Type، گزینه‌ی Generic را انتخاب کنید و از لیست کشویی، گزینه‌ی Drop را انتخاب کنید تا همه‌ی ارتباطات به طرف این IP رد شود.

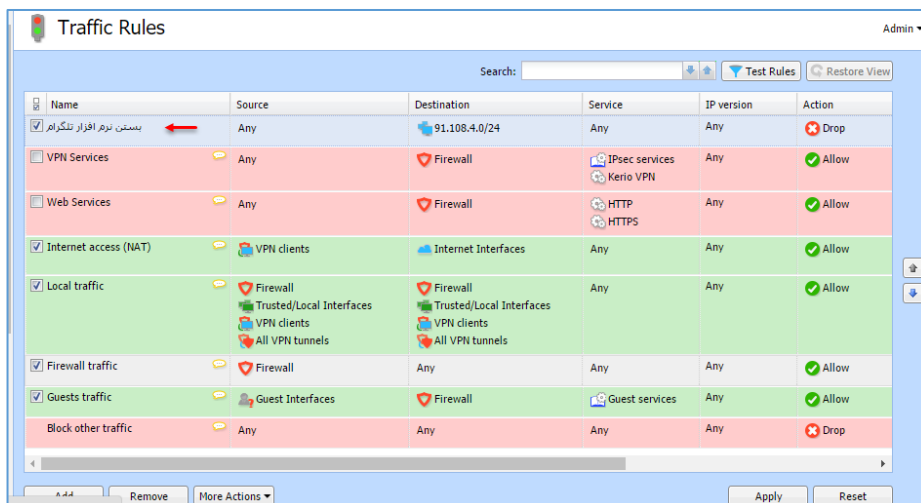


در مرحله‌ی بعد وارد قسمت Destination شوید و بر روی Address کلیک کنید.

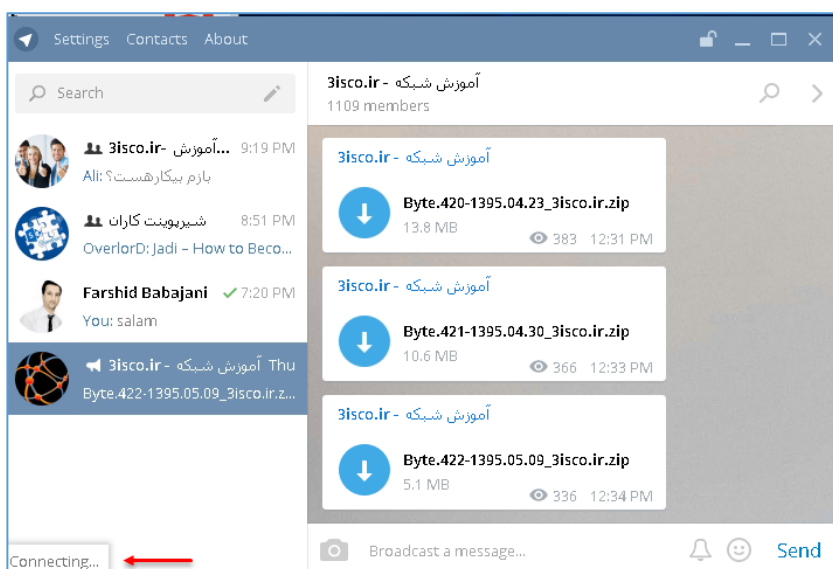


توجه داشته باشید در قسمت Source، نیازی به اضافه کردن گزینه‌ای نیست، اگر این کار را انجام ندهیم، یعنی همه‌ی ارتباطات (any) انتخاب می‌شود.

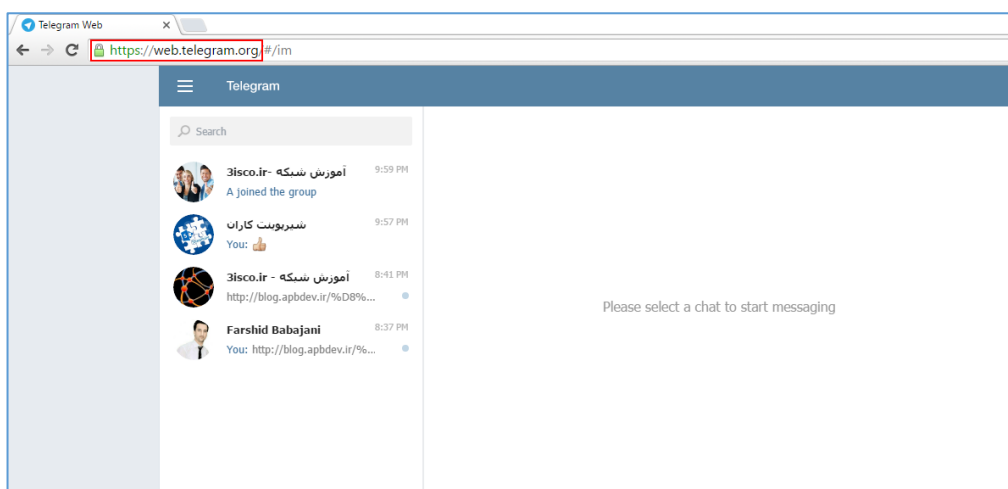
همانطور که مشاهده می‌کنید، آدرس IP وارد شده است، اما به صورت Networks وارد شده است، /24 یعنی ۲۵۵,۲۵۵,۲۵۵,۰ که این اعداد به این اشاره دارد که تمام آدرس‌ها در رنج 91.108.4 انتخاب می‌شود؛ این کار به این دلیل است که شاید تلگرام آدرس خود را در همین رنج تغییر دهد که اگر تغییر کند با این کار، تلگرام دوباره بسته خواهد شد.



همانطورکه مشاهده می کنید یک Rule ایجاد شده است و IP آدرس 91.108.4.0/24 برای کل شبکه Drop شده است؛ بر روی Apply کلیک کنید تا Rule بر روی شبکه اعمال شود.



همانطورکه مشاهده می کنید، ارتباط کاربر با تلگرام قطع شده است و کاربر دیگر نمی تواند به تلگرام متصل شود. با این کار، اینترنت کاربر قطع نخواهد شد، تنها ارتباط آن با تلگرام قطع خواهد شد.



برای اینکه تلگرام تحت وب را نیز ببندید، با کاربر مورد نظر وارد تلگرام تحت وب شوید و بعد از آن به مانند قبل وارد تلگرام شوید.

Traffic Rule	Service	Source	Destination	Bandwidth Management Ru...	Load Balancing	Type
Internet access (NAT)	HTTPS	10.253.226.4	149.154.167.118		Internet	Outbound conne...
Internet access (NAT)	HTTPS	10.253.226.4	149.154.167.118		Internet	Outbound conne...
Internet access (NAT)	HTTPS	10.253.226.4	91.108.4.163		Internet	Outbound conne...

Connection information

Source IP: 10.253.226.4 Destination IP: 149.154.167.118
 Source hostname: 10.253.226.4 Destination hostname: 149.154.167.118

در شکل بالا، هم‌زمان، هر دو ورژن تلگرام تحت وب و Desktop توسط کاربر اجرا شده است که آدرس آن‌ها مشخص شده است، برای اینکه ورژن تحت وب را ببندید باید به مانند ورژن Desktop که قبلاً انجام دادیم آدرس 149.154.167.118 را ببندید.

Name	Source	Destination	Service	IP version	Action
بستن نرم افزار تلگرام	Any	91.108.4.0/24	Any	Any	Drop
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow
Internet access (NAT)	VPN clients	Internet Interfaces	Any	Any	Allow
Local traffic	Firewall Trusted/Local Interfaces	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow
Firewall traffic	Any	Any	Any	Any	Allow
Guests traffic	Firewall	Guest services	Any	Any	Allow
Block other traffic	Any	Any	Any	Any	Drop

برای اینکه Rule را دوباره ایجاد نکنید، می‌توانید از Rule قبلی که برای بستن تلگرام ایجاد کردیم، استفاده کنید و یک کپی از آن تهیه کنید، برای این کار به مانند شکل بالا، Rule مورد نظر و از قسمت More Actions، گزینه Duplicate را انتخاب کنید.

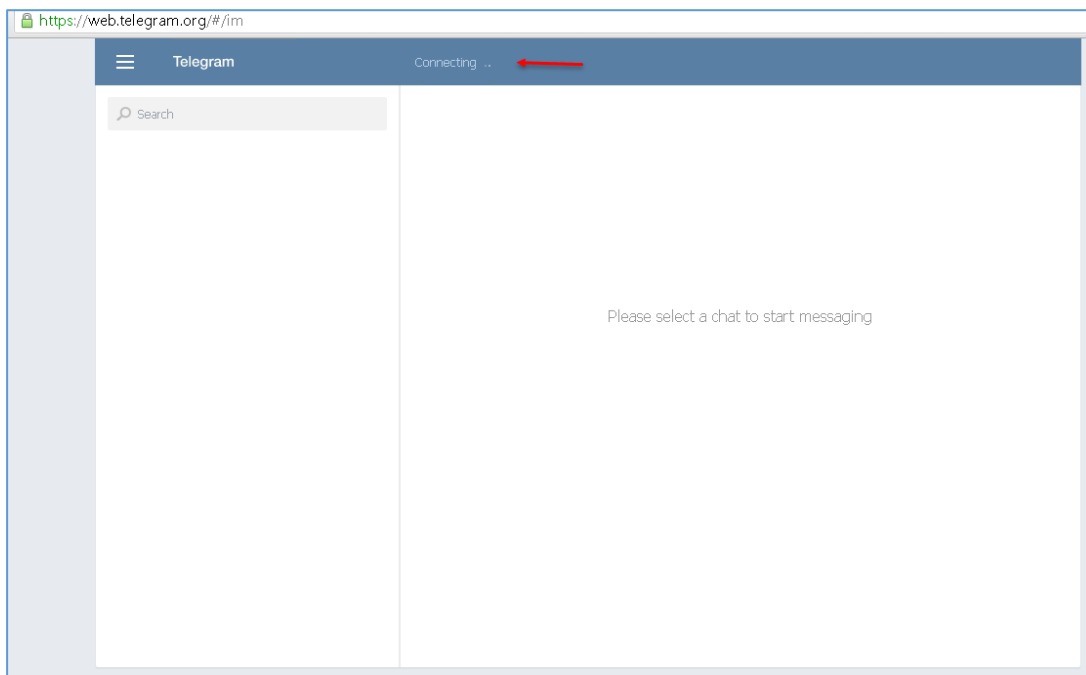
Traffic Rules

Search: Test Rules Restore View

Name	Source	Destination	Service	IP version	Action
بستن نرم افزار تلگرام	Any	91.108.4.0/24	Any	Any	Drop
بستن تلگرام تحت وب	Any	149.154.167.0/24	Any	Any	Drop
VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow
Web Services	Any	Firewall	HTTP HTTPS	Any	Allow
Internet access (NAT)	VPN clients	Internet Interfaces	Any	Any	Allow
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow
Firewall traffic	Firewall	Any	Any	Any	Allow
Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow

Add Remove More Actions Apply Reset

در شکل روبرو، دو Rule ایجاد شده است که نام آنها مشخص شده است؛ در قسمت تحت وب، آدرس 149.154.167.0/24 وارد شده است که همگی آدرسها در رنج ۱۴۹،۱۵۷،۱۶۷ بسته خواهد شد.

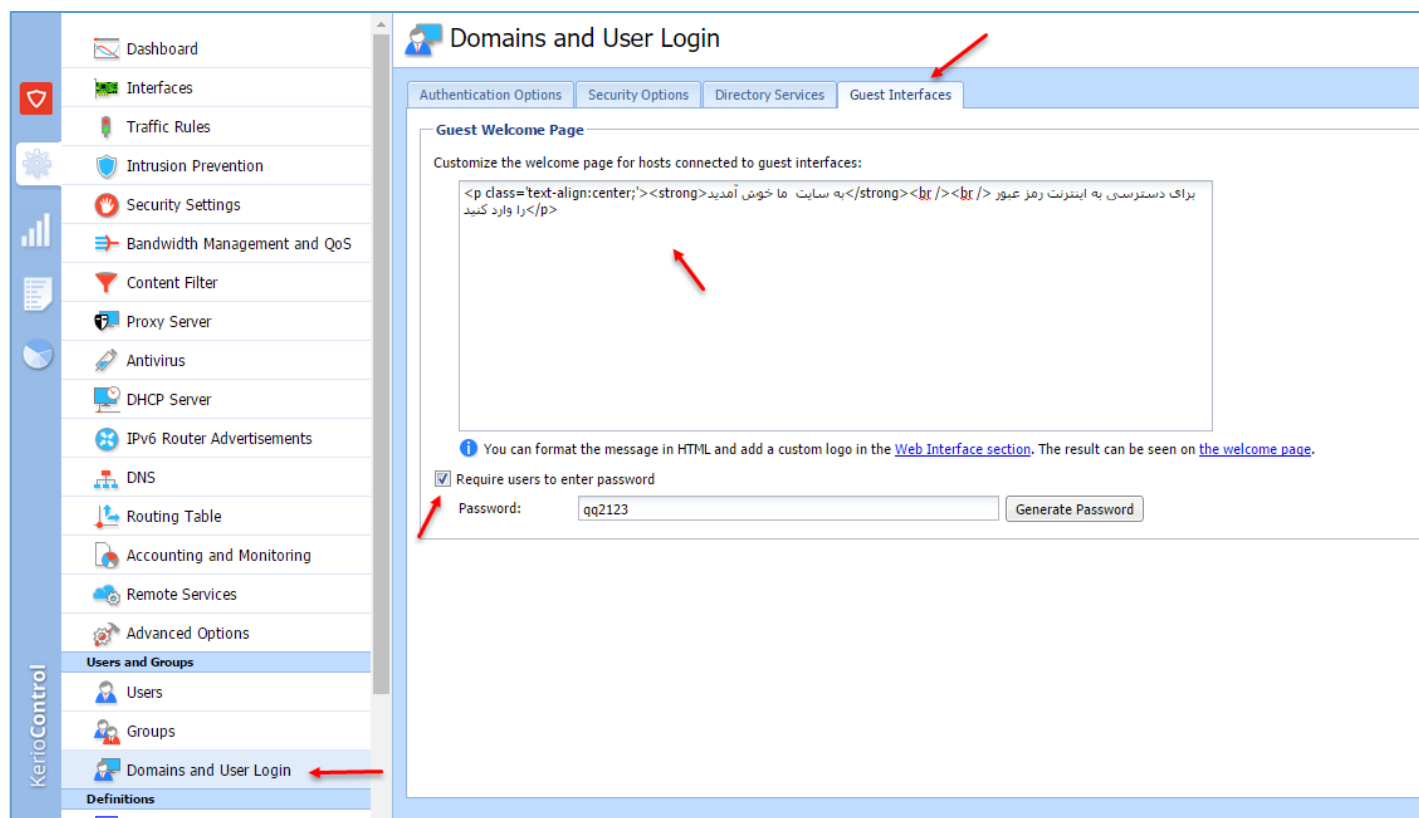


بعد از فعال کردن Rule، ارتباط کاربر با تلگرام تحت وب قطع شده است.

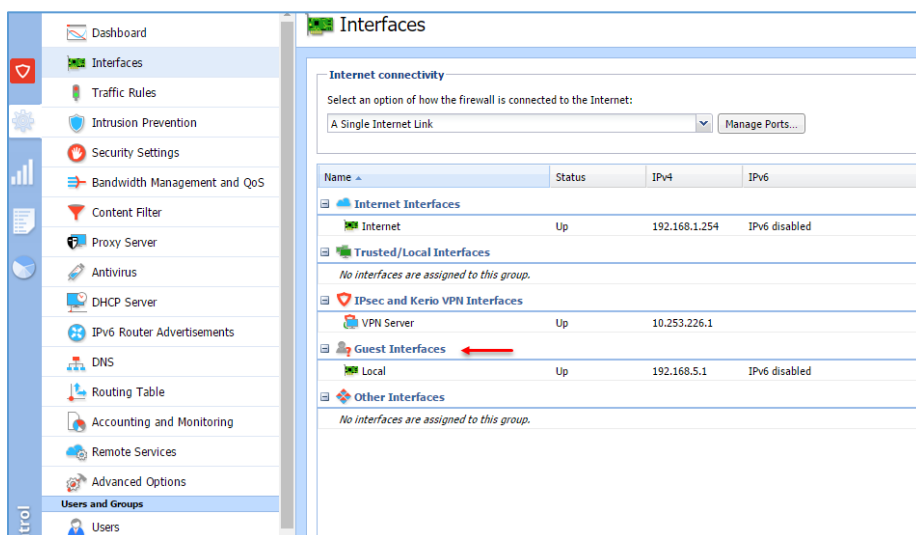
بررسی Guest Interfaces:

در کریو، یک امکان وجود دارد تا بتوانیم برای مهمانان خود یک اینترفیس تعریف کنیم تا آن‌ها بتوانند با استفاده از یک رمز عبور وارد اینترنت شوند، این موضوع می‌تواند شبیه به Hot Spot در میکروتیک باشد که برای مهمان‌ها یک مسیر جداگانه با زمان مشخص تعریف می‌شد تا آن‌ها نیز به اینترنت دسترسی داشته باشند.

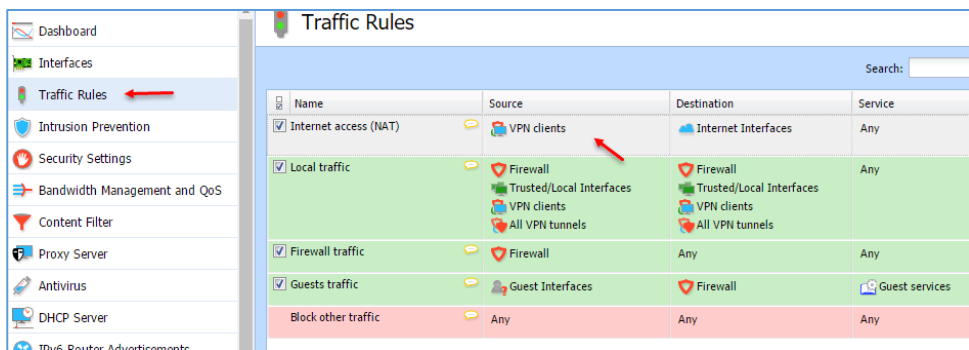
برای فعال کردن Guest Interface، به مانند شکل بالا وارد Advanced Options شوید و بعد وارد تب Web Interface شوید و برای اینکه یک صفحه برای ورود کاربر به اینترنت مهمان ظاهر شود باید تیک گزینه Use Custom logo on... را انتخاب کنید؛ در قسمت Page title، عنوان صفحه را وارد کنید و در قسمت Logo می‌توانید با کلیک بر روی دکمه Change، آرم شرکت خود را وارد و در قسمت Favicon، یک آیکون به دلخواه خود وارد کنید، بعد از انجام کارهای بالا بر روی Apply کلیک کنید.



در مرحله‌ی دوم به مانند شکل بالا، از سمت چپ بر روی **Domains and User Login** کلیک کنید و وارد تب **Guest Interfaces** شوید؛ در این صفحه شما می‌توانید صفحه‌ای که برای کاربر نمایش داده می‌شود را ویرایش کنید که این کار را در کد HTML انجام دادیم، اگر تیک گزینه **Require users to enter password** را انتخاب کنید از کاربر درخواست رمز عبوری می‌شود که در قسمت **Password** وارد کرده‌اید. بر روی **Apply** کلیک کنید و به ادامه‌ی کار توجه کنید.



در مرحله‌ی بعد برای اینکه کاربران، زمانی که سایتی را باز می‌کنند وارد صفحه‌ی ورود شوند، می‌توانید **Interface** داخلی شبکه را که با نام **Local** قرار دادیم را وارد قسمت **Guest Interface** کنید، بر روی **Apply** کلیک کنید.

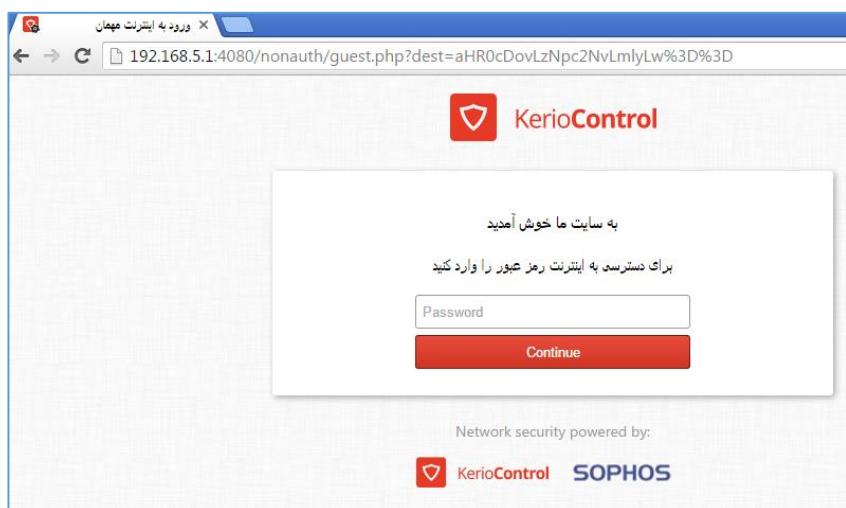
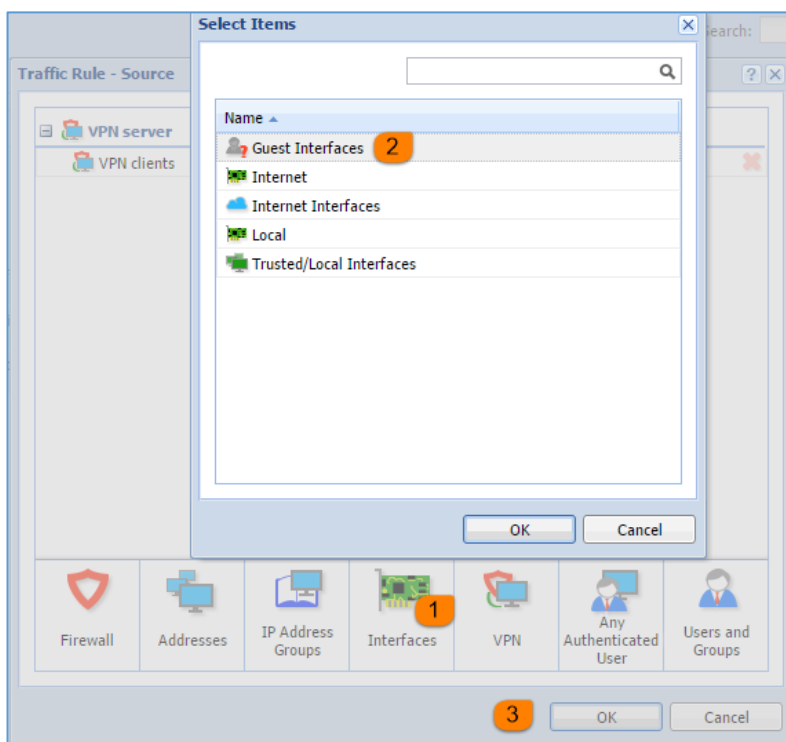


در مرحله‌ی آخر باید Interface Guest را در Rule مربوط به اینترنت قرار دهید، برای انجام این کار در قسمت Source مربوط به Access (NAT) Internet

دو بار کلیک کنید.

به مانند شکل بر روی گزینه‌ی یک، یعنی Interface کلیک کنید و در پنجره‌ی باز شده بر روی Guest Interfaces کلیک کنید و در آخر نیز بر روی ok کلیک کنید تا این Interface به لیست اضافه شود.

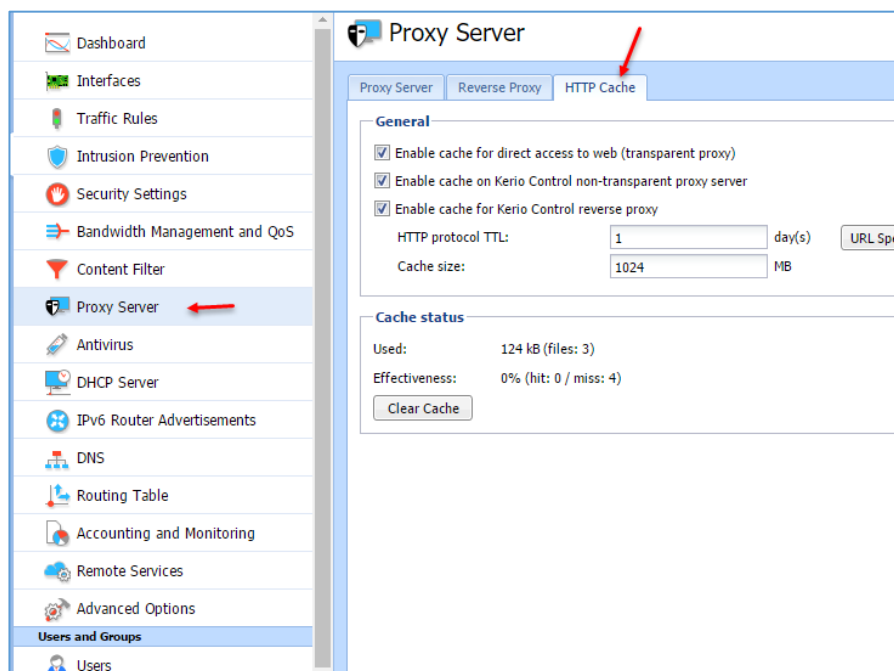
بر روی Apply کلیک کنید تا همه چیز ok شود.



همانطور که در شکل روبرو مشاهده می‌کنید، زمانی که کاربر مورد نظر سایتی را درخواست می‌کند، برای او صفحه‌ی Kerio Control ظاهر می‌شود که باید رمز عبور را وارد کند تا وارد اینترنت شود.

فعال سازی کش سرور در کریو:

سرویس Cash یک Proxy Server برای صرفه جویی در پهنای باند و هزینه است؛ بر فرض اگر کاربری، یک سایت، مثلاً google.com را باز کرد، اطلاعات این سایت در کش سرور ذخیره خواهد شد و اگر کاربران دیگر، سایت Google.com را درخواست کنند، دیگر کریو به ISP مراجعه نمی کند، بلکه در خود سرور، سایت را برای کاربر اجرا می کند که این کار، سرعت عمل را افزایش می دهد و صرفه جویی حداقل ۵۰ درصدی را در مصرف پهنای باند انجام می دهد.



برای فعال کردن کش سرور وارد Proxy Server شوید و در صفحه‌ی باز شده وارد تب HTTP Cache شوید و تیک هر سه گزینه را فعال کنید، در قسمت Cache size می توانید حداکثر فضای کش را وارد کنید که به صورت پیش فرض ۱۰۲۴ مگابایت در نظر گرفته شده است.

بعد از این کار بر روی Apply کلیک کنید تا اطلاعات ذخیره شود، بعد از

آن، اگر کاربران وارد سایتی شوند اطلاعات آن سایت در سرویس کش ذخیره خواهد شد و کاربران بعدی می توانند با سرعت بیشتری به سایت دسترسی داشته باشند.

مزایای این روش را در قسمت قبل بیان کردیم، اما این روش معایبی نیز دارد، اگر سایتی در سرویس کش سرور ذخیره شود و آن سایت در هر لحظه در حال تغییر و آپدیت باشد، مانند سایت های خبری، کاربران نمی توانند در همان لحظه، سایت آپدیت شده را مشاهده کنند، بلکه سایت قدیمی تر را مشاهده خواهند کرد که برای رفع این مشکل می توانند از کلید ترکیبی CTRL + F5 استفاده کنند.

فعال‌سازی آنتی ویروس در کریو:

این سرویس یکی از سرویس‌های پرکاربرد در کریو است که می‌تواند تا حدود زیادی، امنیت شبکه‌ی شما را حفظ کند و فایل‌های مختلف را کنترل کند، برای فعال‌سازی این سرویس به صورت زیر عمل کنید:

برای فعال‌سازی **Antivirus**، به مانند شکل بالا وارد قسمت **Antivirus** شوید و تیک گزینه **Use the integrated antivirus engine** را انتخاب کنید، با این کار بعد از ۱ یا ۲ دقیقه، سرویس آنتی ویروس فعال خواهد شد؛ قسمت شماره‌ی دو، مربوط به آپدیت کردن آنتی ویروس است که اگر سرور **Kerio** شما اصل باشد، این کار با کلیک بر روی **Update Now** انجام خواهد شد، اما اگر کرک کرده باشید، این کار به علت بسته بودن سایت کریو انجام نخواهد گرفت. در قسمت شماره‌ی سه، پروتکل‌هایی که توسط این سرویس بررسی می‌شود،

انتخاب شده است، در قسمت شماره‌ی چهار نیز، تنها فایل‌هایی اسکن می‌شوند که حجم آن‌ها کمتر از ۴۰۹۶ کیلوبایت باشد که این مقدار را می‌توانید به دلخواه خود تغییر دهید.

Antivirus

Antivirus Engine | **HTTP, FTP Scanning** | Email Scanning

If a virus is found

- Alert the client (1)
- Email messages will be sent via the MyKerio notification service. [SMTP server can be configured in Remote Services...](#)

If a transferred file cannot be scanned (e.g. corrupted or encrypted)

- Deny transmission of the file (2)
- Allow transmission of the file

Scanning rules

Type	Content	Action	Description
<input checked="" type="checkbox"/> File type	Archive files	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	Web files (3)	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	Executable files	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	Embedded objects	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	System files	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	Documents	<input checked="" type="checkbox"/> Scan	
<input type="checkbox"/> File type	Image files	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> File type	Mail message files	<input checked="" type="checkbox"/> Scan	
<input checked="" type="checkbox"/> HTTP MIME type	application/x-rtsp-tunnelled	<input type="radio"/> Do not scan	Tunnelled RTSP

در تب HTTP, FTP Scanning می‌توانید مشخص کنید که چه نوع فایل‌هایی اسکن شوند.

در قسمت شماره‌ی یک، اگر تیک گزینه‌ی Alert the client را انتخاب کنید، زمانی که یک ویروس در فایل‌های کاربر پیدا شود، یک

ایمیل ارسال خواهد شد که برای ارسال ایمیل باید SMTP را فعال کنید که در ادامه، این کار را انجام خواهیم داد؛ در قسمت شماره‌ی دو، اگر آنتی ویروس فایلی را نتوانست بررسی کند، مثلاً اگر آن فایل قفل‌گذاری شده یا خراب باشد با انتخاب گزینه‌ی Deny tra...، فایل انتقال داده نمی‌شود و اگر گزینه‌ی Allow tra... را انتخاب کنید، فایل انتقال داده خواهد شد؛ در قسمت شماره‌ی سه نیز می‌توانید نوع فایل برای اسکن را انتخاب کنید.

Antivirus

Antivirus Engine | HTTP, FTP Scanning | **Email Scanning**

If a virus is found

- Note that it is not possible to drop whole email messages. Such an action might have caused problems in communication.
- Prepend message subject with this text: (1)
- ***VIRUS**

TLS connection (cannot be scanned by antivirus)

- Allow clients to use encrypted TLS connections (2)
- This option works even when no antivirus is enabled; you can still block TLS connections if you want to.

If an attachment cannot be scanned (e.g. corrupted or encrypted)

- Remove the attachment from the email message (3)
- Allow delivery of the attachment

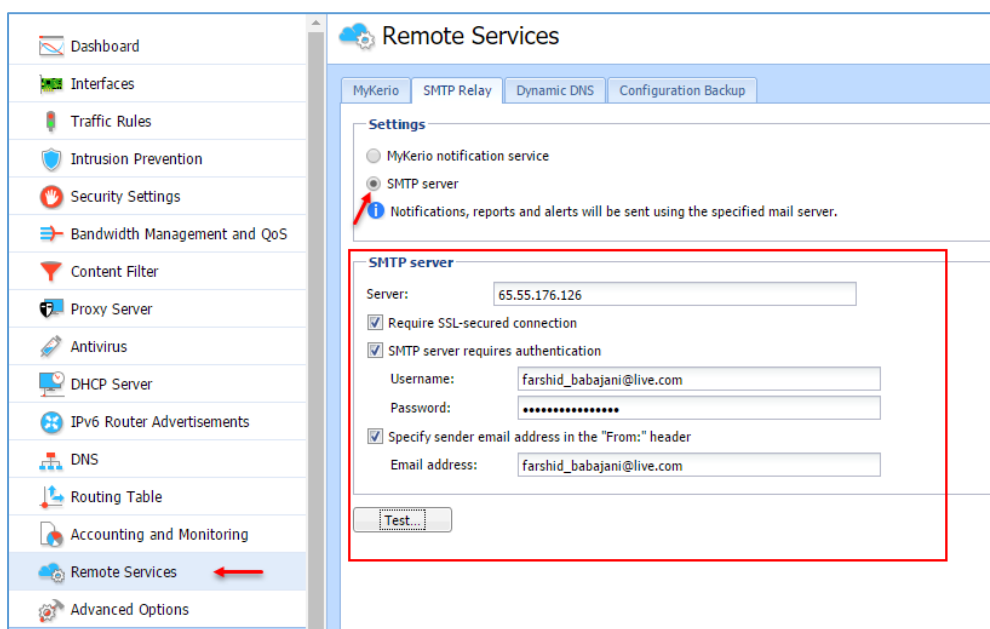
در تب Email Scanning و در قسمت شماره‌ی یک، اگر در عنوان ایمیل، Virus نوشته شده باشد آن ایمیل، Drop خواهد شد، شما می‌توانید به جای Virus، یک نام به دلخواه خود وارد کنید.

در قسمت شماره‌ی دو به کاربر اجازه داده خواهد شد که از پروتکل TLS

برای استفاده از سرور ایمیل خود استفاده کند، اگر کاربر از پروتکل TLS استفاده کند، دیگر آنتی ویروس نمی تواند ایمیل های کاربر را بررسی کند.

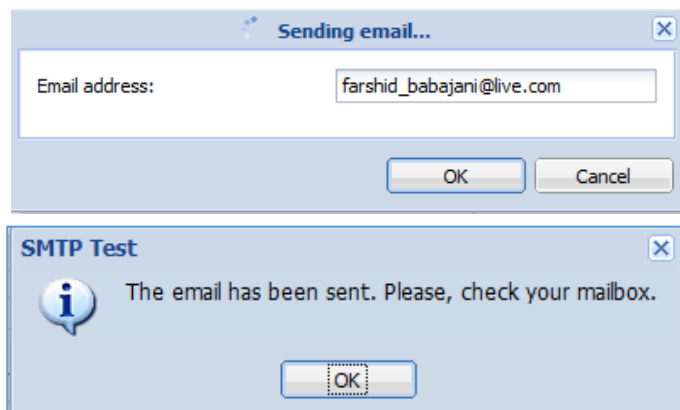
در قسمت شماره ی سه، اگر ایمیلی دارای فایل پیوست باشد و آنتی ویروس نتواند آن را اسکن کند، پیوست مورد نظر از ایمیل حذف خواهد شد، اگر نمی خواهید این کار انجام شود، گزینه ی دوم را انتخاب کنید.

برای فعال سازی ایمیل و سرویس SMTP به مانند زیر عمل کنید:



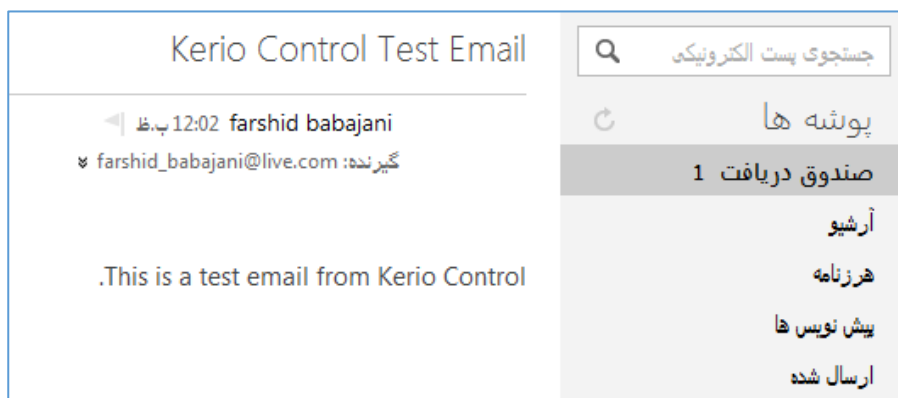
وارد قسمت Remote Services و بعد وارد SMTP Relay شوید و گزینه ی SMTP Server را انتخاب کنید و آدرس سرور ایمیل خود را در قسمت Server وارد کنید، اگر سرور ایمیل شما از پروتکل SSL یا TLS استفاده می کند، تیک گزینه ی Require SSL-

secures را انتخاب و برای وارد کردن نام کاربری و رمز عبور خود، تیک گزینه ی SMTP server را انتخاب و نام کاربری و رمز عبور مربوط به ایمیل خود را وارد کنید و در قسمت Specify Sender email، آدرس ایمیل خود را دوباره وارد و بر روی Test کلیک کنید.



در حال ارسال ایمیل....

اگر ایمیل درست کار کند با پیغام روبرو مواجه خواهید شد.



محتوای ایمیل را نیز در صندوق دریافت مشاهده می کنید.

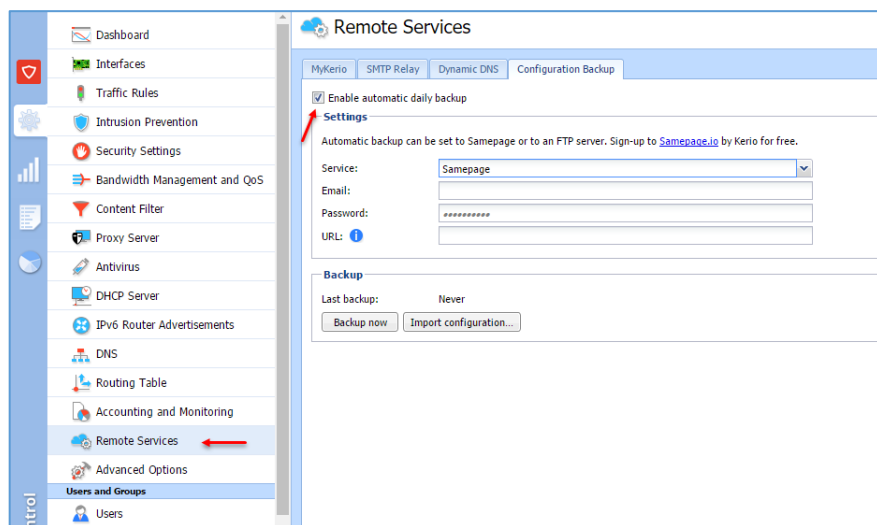
بررسی سرویس Intrusion Prevention:

این سرویس یک سیستم تشخیص نفوذ و پیشگیری (IDS / IPS) است که روی ترافیک شبکه کار می کند و تمامی حملات به شبکه را تشخیص می دهد.

برای فعال سازی این سرویس باید به مانند شکل بالا وارد Intrusion Prevention شوید و تیک گزینهی Enable Intrusion Prevention را انتخاب کنید؛ در این سرویس بر اساس بررسی های کنترلی IPS و IDS، اطلاعات کنترل و اگر با سایتی مواجه شود که خطر ساز است آن سایت را Drop می کند؛ برای تست این موضوع می توانید بر روی [این لینک](#) کلیک کنید.

Backup و Restore در Kerio Control

برای حفظ تنظیمات و اطلاعات سرور کریو باید از آن، یک فایل پشتیبان تهیه کنید تا در موقع از دست رفتن اطلاعات، دوباره بتوانید اطلاعات قبلی را به سرور برگردانید.

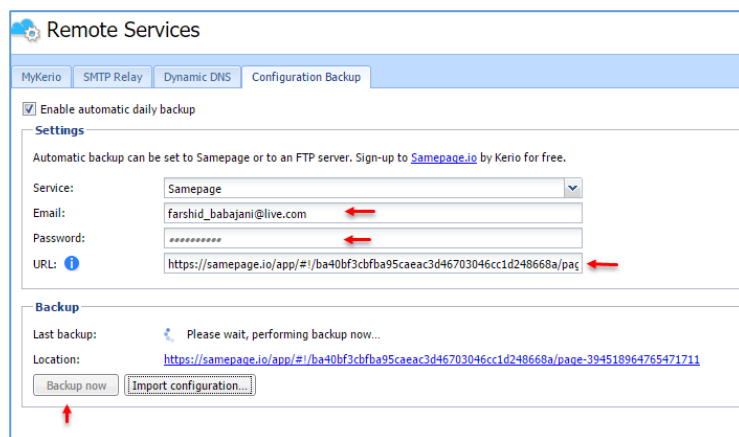


برای فعال‌سازی Backup در کریو به مانند شکل روبرو وارد قسمت Remote Services و بعد از آن وارد تب Configuration Backup شوید؛ در این قسمت، دو گزینه در قسمت Service وجود دارد که باید برای Backup استفاده کنید، یکی سایت samepage است که یکی از ابزارهای

کریو برای این کار است که با ثبت نام در این سایت، یک فضا به شما داده خواهد شد و می‌توانید اطلاعات را در آن قرار دهید، گزینه‌ی دیگر در این قسمت، گزینه‌ی FTP است که شما می‌توانید یک سرور FTP راه‌اندازی کنید و آدرس آن را به کریو دهید تا بتواند اطلاعات را در آن قرار دهد.

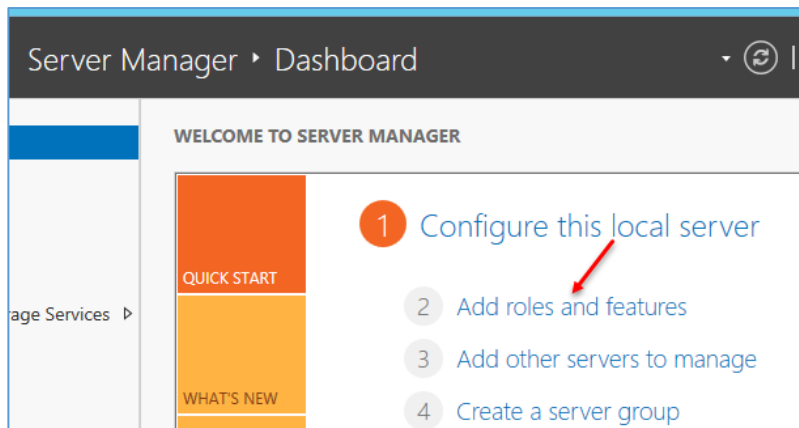
برای شروع از سایت Samepage.io استفاده کنید، برای کار با این سایت باید وارد لینک زیر شوید و ثبت نام را انجام دهید:

<https://www.samepage.io/sign-up>

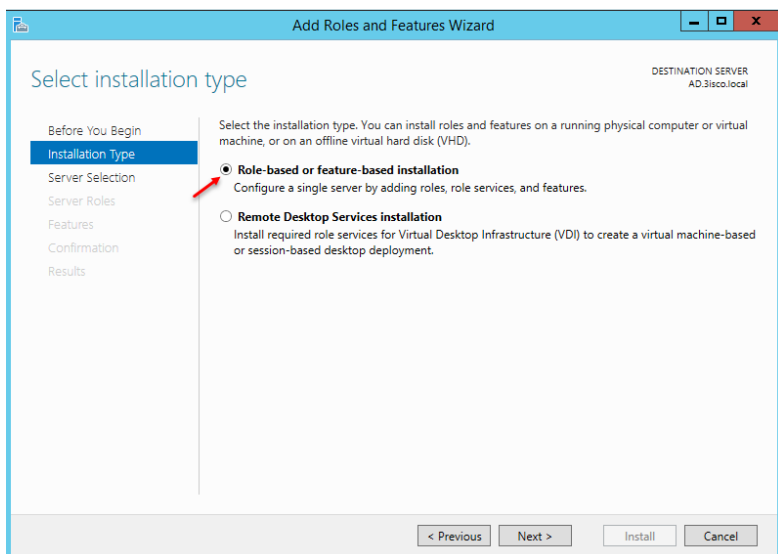


بعد از ثبت نام در سایت باید اطلاعات خود را به مانند شکل روبرو وارد کنید و در قسمت URL، آدرس یک صفحه در سایت مورد نظر که ایجاد می‌کنید را وارد و بر روی Backup now کلیک کنید تا اطلاعات به سایت مورد نظر ارسال شود.

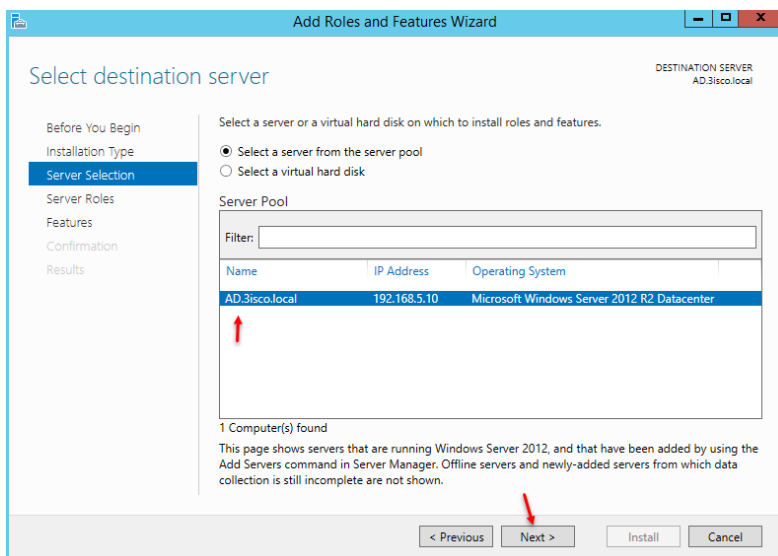
برای ارسال اطلاعات از طریق FTP باید یک سرور برای این کار در شبکه ایجاد کنید؛ برای این کار به صورت زیر عمل کنید.



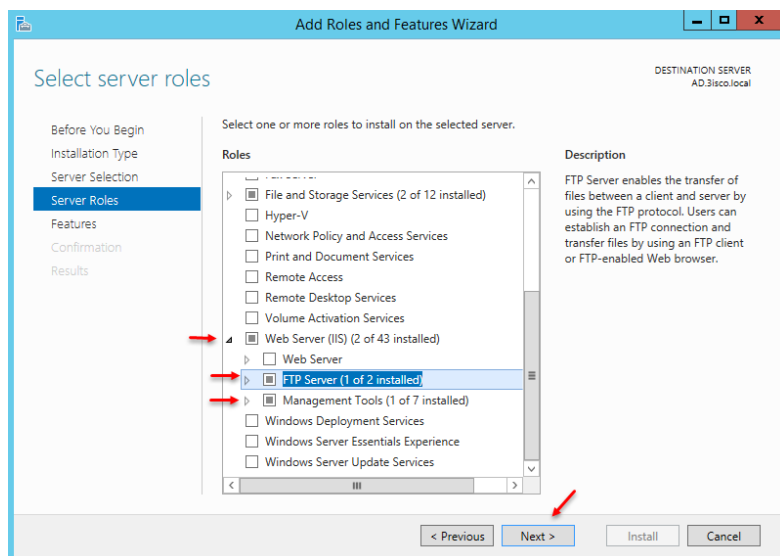
برای راه‌اندازی سرویس FTP از ویندوز سرور ۲۰۱۲ استفاده کنید؛ برای شروع وارد ویندوز سرور ۲۰۱۲ شوید و ابزار server Manager را اجرا و بر روی Add roles and features کلیک کنید.



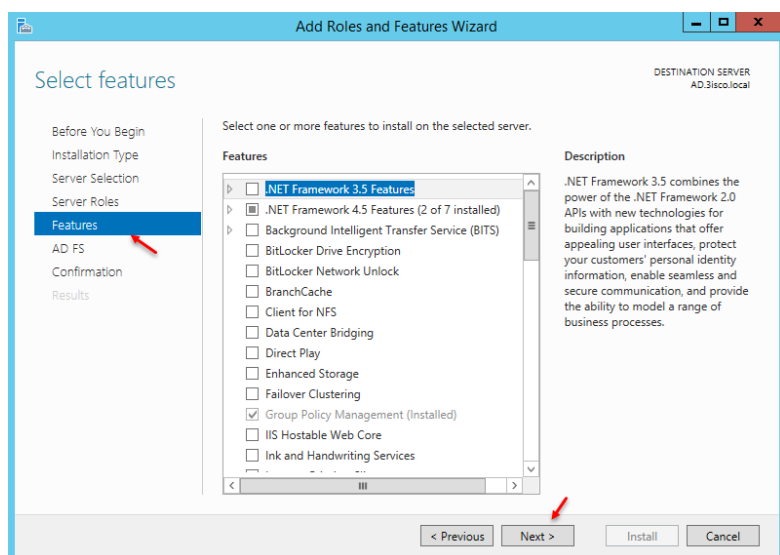
در این صفحه، گزینه‌ی Role-based or ... را انتخاب و بر روی Next کلیک کنید.



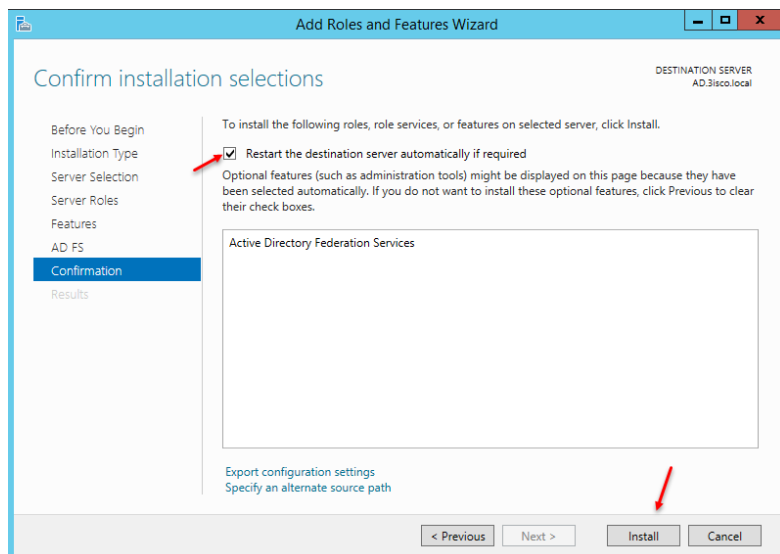
در این صفحه، نام سرور خود را انتخاب و بر روی Next کلیک کنید.



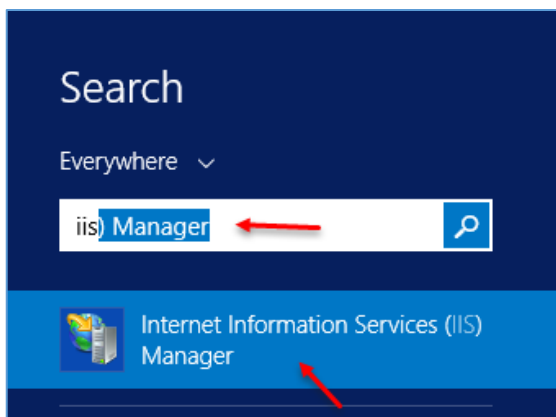
در این صفحه باید سرویس IIS را به مانند شکل روبرو فعال کنید، در قسمت مورد نظر فقط کافی است گزینهی FTP Server را انتخاب کنید، چون نیازی به Web Server نداریم، بعد از انتخاب بر روی Next کلیک کنید.



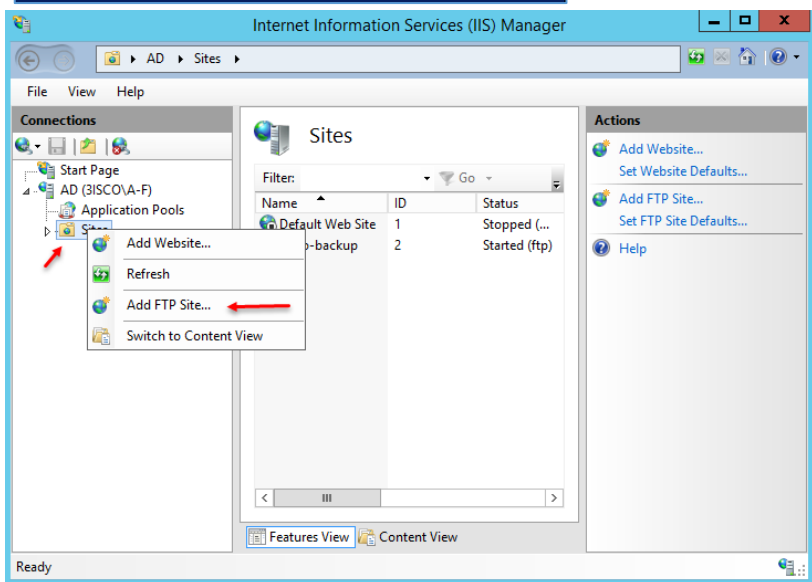
در این صفحه، تنها بر روی Next کلیک کنید.



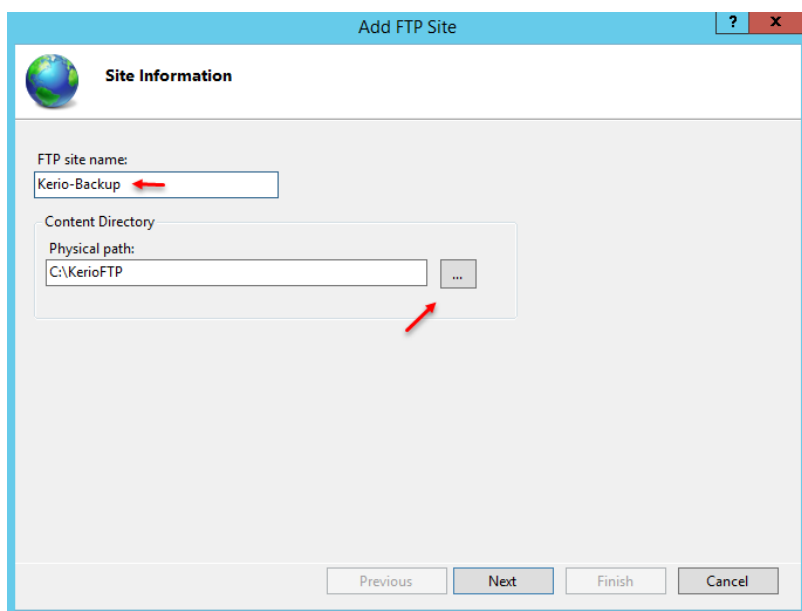
در این قسمت، تیک گزینهی Restart the... را انتخاب و بر روی install کلیک کنید تا بعد از نصب سرویس سرور Restart شود، البته در صورت نیاز Restart می شود.



بعد از نصب سرویس وارد Search شوید و سرویس iis را اجرا کنید.



همانطور که مشاهده می کنید، سرویس مورد نظر اجرا شده است، به مانند شکل بر روی Sites کلیک راست کنید و گزینه Add FTP Site را انتخاب کنید.



در این صفحه و در قسمت Ftp site name، نام دلخواه خود را وارد کنید و در قسمت Physical Path، یک آدرس برای ذخیره کردن اطلاعات انتخاب کنید و بر روی Next کلیک کنید.

Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned Port: 21

Enable Virtual Host Names:
Virtual Host (example: ftp.contoso.com):

Start FTP site automatically

SSL

No SSL
 Allow SSL
 Require SSL

SSL Certificate: Not Selected [Select...] [View...]

[Previous] [Next] [Finish] [Cancel]

در این صفحه، پورت مربوط به سرویس FTP را مشاهده می‌کنید که می‌توانید آن را تغییر دهید، اما پورت پیش‌فرض آن ۲۱ است، در قسمت SSL می‌توانید پروتکل SSL را برای ارتباط FTP فعال کنید تا ارتباط به صورت امن انجام شود؛ در این لحظه، گزینه‌ی No SSL را انتخاب و بر روی Next کلیک کنید.

Add FTP Site

Authentication and Authorization Information

Authentication

Anonymous
 Basic

Authorization

Allow access to: Specified users

administrator

Permissions

Read
 Write

[Previous] [Next] [Finish] [Cancel]

در این صفحه که مربوط به تأیید هویت است، گزینه‌ی Basic را انتخاب کنید و در قسمت Authorization، گزینه‌ی Specified Users را انتخاب کنید و یک کاربر که برای دسترسی به FTP نیاز دارید را وارد کنید و تیک گزینه‌ی Read و Write را انتخاب کنید و بر روی Finish کلیک کنید.

Remote Services

MyKerio SMTP Relay Dynamic DNS Configuration Backup

Enable automatic daily backup

Settings

Automatic backup can be set to Samepage or to an FTP server. Sign-up to [Samepage.io](#) by Kerio for free.

Service: FTP

Username: administrator

Password: *****

URL: ftp://192.168.5.10/

Backup

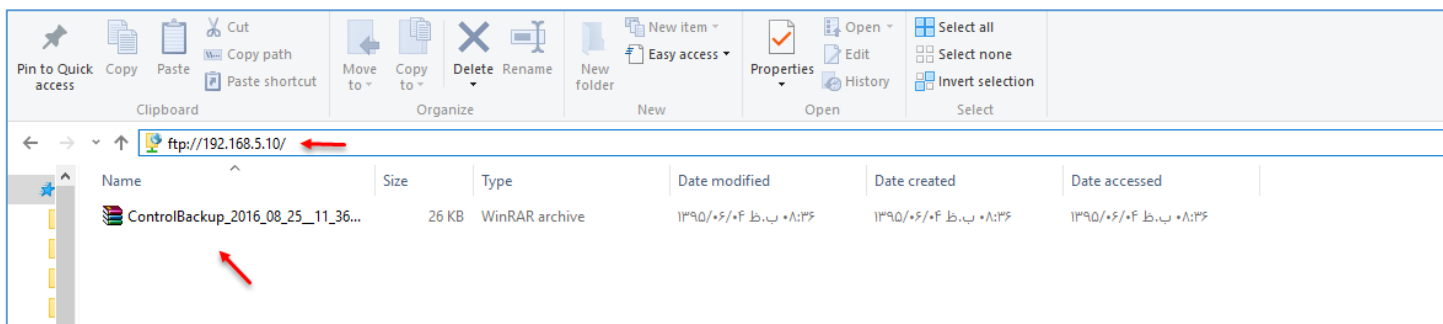
Last backup: less than a minute ago

Location: ftp://192.168.5.10/

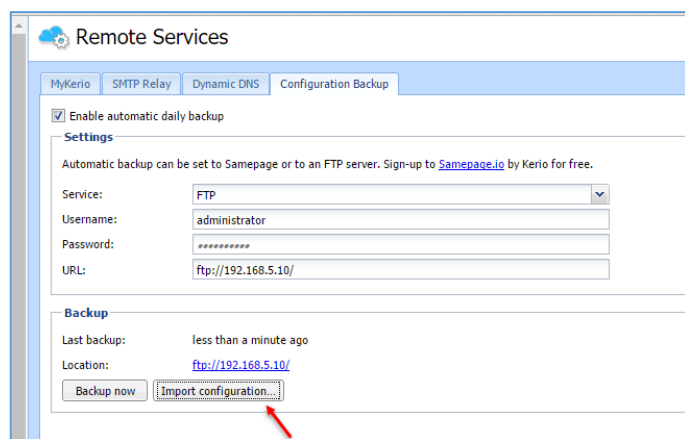
[Backup now] [Import configuration...]

بعد از اینکه سرویس FTP را راه‌اندازی کردید به‌مانند شکل روبرو وارد Remote Services شوید و تیک گزینه‌ی Enableautomatic... را انتخاب کنید تا سرویس backup فعال شود؛ در قسمت شماره‌ی یک، گزینه‌ی FTP را انتخاب کنید و در قسمت

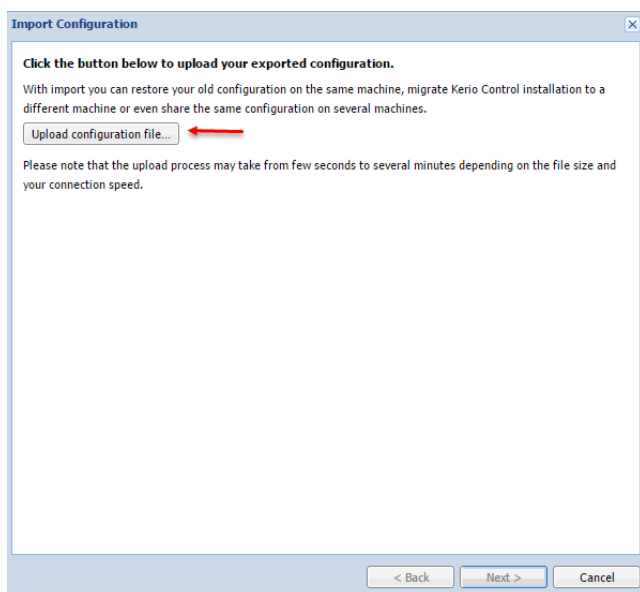
شماره‌ی دو، نام کاربری که در قسمت ایجاد سایت در FTP وارد کردیم را در این قسمت وارد کنید و در قسمت شماره‌ی سه، آدرس سرور FTP را به صورت [FTP://192.168.5.10/](ftp://192.168.5.10/) وارد کنید که به جای ۱۹۲,۱۶۸,۵,۱۰ آدرس سرور خود را وارد و در پایان بر روی **Apply** کلیک کنید تا اطلاعات ذخیره شود؛ بعد از این کار بر روی **Backup New** کلیک کنید تا کار ایجاد پشتیبان انجام شود.



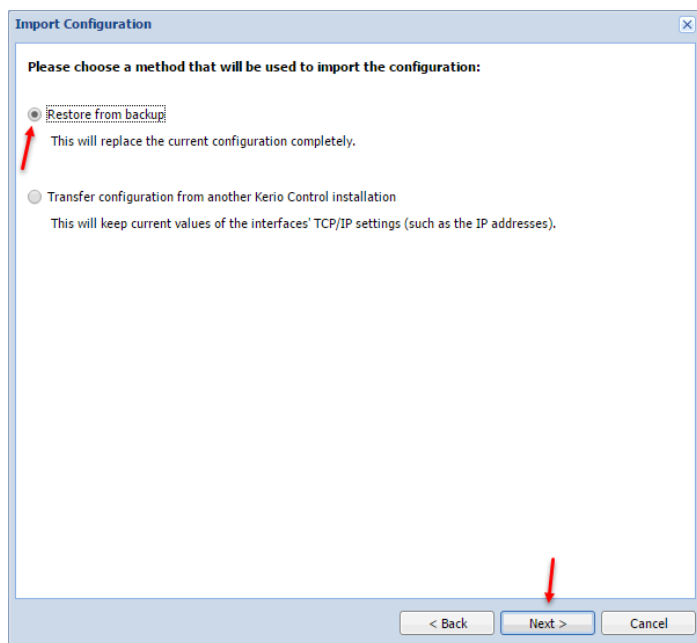
بعد از ایجاد Backup، اگر وارد آدرس FTP به مانند شکل بالا شوید، فایل مورد نظر را که با پسوند gz است را مشاهده می‌کنید.



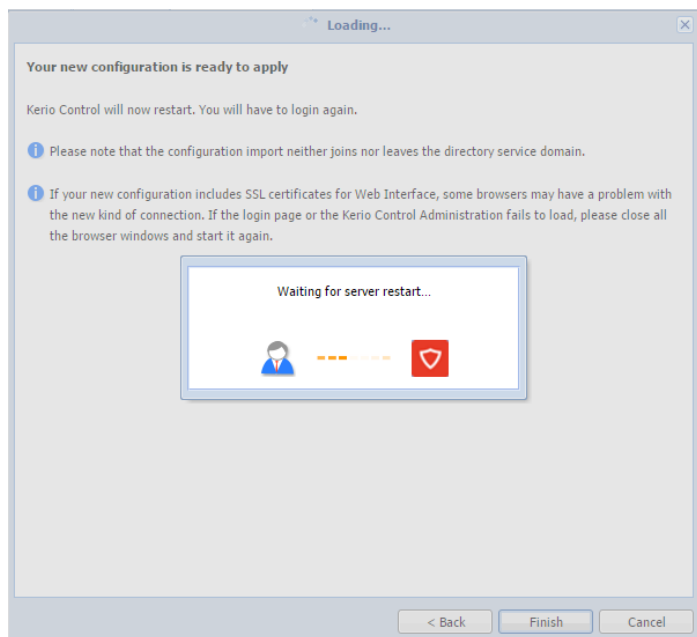
برای اینکه بتوانید Backup ایجاد شده را Restore کنید باید به مانند شکل روبرو بر روی **Import Configuration** کلیک کنید.



در این صفحه بر روی **Upload Configuration File** کلیک کنید و فایل Backup ایجاد شده در سرور Ftp را انتخاب کنید.



در این صفحه، گزینه‌ی **Restore from backup** را انتخاب و بر روی **Next** کلیک کنید.



همانطورکه مشاهده می‌کنید، فایل مورد نظر در حال **Restore** شدن است.

کار با Kerio Connect:

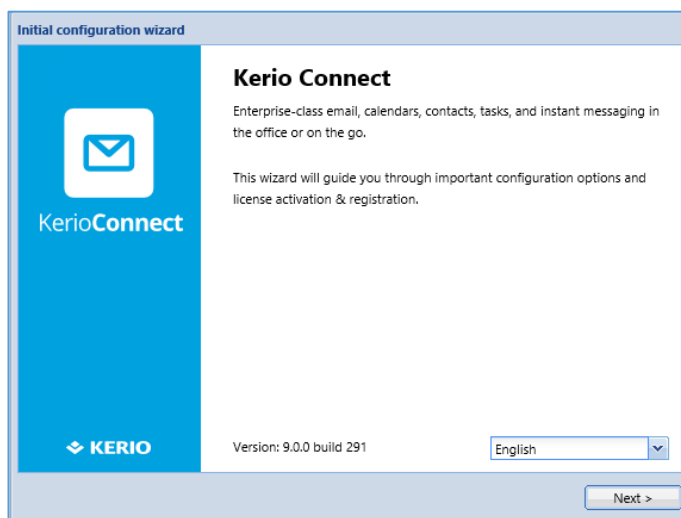
Kerio Connect، یکی دیگر از محصولات شرکت کریو تکنولوژی است که برای دریافت و ارسال ایمیل در سازمان‌های کوچک و متوسط استفاده می‌شود.

برای راه‌اندازی نرم‌افزار Kerio Connect می‌توانید از نسخه‌های لینوکس، مک یا ویندوز استفاده کنید که برای دریافت آن باید به سایت کریو مراجعه کنید. در این کتاب با نسخه‌ی تحت ویندوز آن کار خواهیم کرد که برای دریافت آن می‌توانید از لینک زیر استفاده کنید:

<http://www.farstak.com/%D8%AF%D8%A7%D9%86%D9%84%D9%88%D8%AF-kerio-connect-9-0-1-394/>

بعد از دانلود، آن را به صورت زیر اجرا و نصب کنید:

در صفحه‌ی اول، زبان مورد نظر خود را انتخاب و بر Next کلیک کنید.



اگر توافقنامه را قبول دارید، گزینه‌ی **I accept** را انتخاب و بر روی **Next** کلیک کنید.



Initial configuration wizard

Server identification

Please enter a fully qualified domain name of the Kerio Connect computer. This name should match the MX record in DNS and is used for the server identification in SMTP connections. [Learn more...](#)

Internet hostname:

Please enter a name of the primary email domain that will be created. [Learn more...](#)

Email domain:

< Back Next >

DNS Manager

File Action View Help

DNS

- AD
 - Global Logs
 - Forward Lookup Zones
 - _msdcs.3isco.local
 - 3isco.local
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[31], ad.3isc
(same as parent folder)	Name Server (NS)	ad.3isco.loc
(same as parent folder)	Host (A)	192.168.5.11
ad		192.168.5.11

Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...

New Resource Record

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) of mail server:

Mail server priority:

OK Cancel Help

در این صفحه باید در قسمت Internet Hostname، نام کامل سرور به همراه نام دومین را بنویسید و در قسمت Email domain با نام MX Record در سرویس DNS ایجاد کنید تا ارتباط سرویس SMTP، اوکی شود؛ این MX Record با نام Mail در سرویس DNS قبلاً ایجاد شده است که باید در قسمت مورد نظر وارد کنید، برای اینکه دریافت روش ایجاد MX Record را با هم یاد بگیریم به صورت زیر عمل کنید:

برای ایجاد MX Record به مانند شکل روبرو سرویس DNS خود را که در سرور Active Directory قرار دارد، اجرا کنید و در صفحه‌ی مربوط به دومین که در اینجا دومین 3isco.local است، کلیک راست کنید و گزینه‌ی New Mail Exchanger (MX) را انتخاب کنید.

در این صفحه و در قسمت Host or child domain، یک نام برای ایمیل خود وارد کنید و در قسمت FQDN بر روی Browse کلیک کنید و نام سروری که این نرم افزار بر روی آن در حال نصب است را انتخاب و بر روی OK کلیک کنید.

تذکر: اگر Mx Record را ایجاد نکردید، می‌توانید فقط نام دومین را به تنهایی وارد کنید.

Initial configuration wizard

Administrator password

Please provide username and password for an account which will have full access to the administration.

Username:

Password:

Confirm password:

i The password cannot be empty and should be at least 8 characters long.

< Back Next >

بعد از انجام مراحل قبل و تکمیل اطلاعات بالا بر روی **Next** کلیک کنید تا این صفحه ظاهر شود، رمز عبوری را برای کاربر **Admin** وارد کنید و بر روی **Next** کلیک کنید.

Initial configuration wizard

Message store directory

Kerio Connect will store messages in the selected directory.

The disk drive on which the directory will be located should have enough space.

i If any antivirus software is installed on the Kerio Connect's host, make sure an exclusion rule for the store directory is created in the antivirus software. Otherwise, Kerio Connect may work incorrectly.

< Back Next >

در این صفحه باید مسیر نصب را مشخص کنید، در قسمت پایین همین صفحه به این نکته اشاره شده است که اگر بر روی سروری که ایمیل بر روی آن نصب است، آنتی ویروس دارید، سعی کنید این آدرس را در آنتی ویروس **Exclusion** کنید تا ایمیل سرور بتواند به راحتی به کار خود ادامه دهد و با مشکلی مواجه نشود؛ بر روی **Next** کلیک کنید.

Initial configuration wizard

Licensing

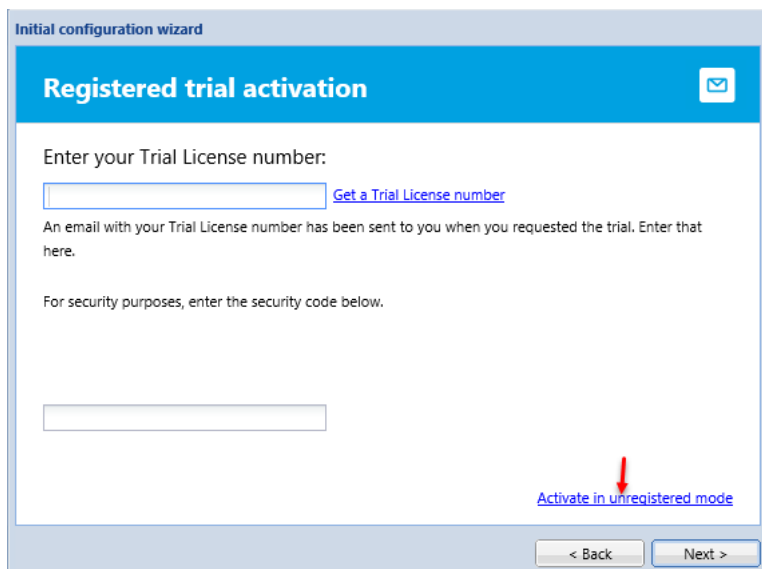
How do you plan to use Kerio Connect?

I will use a commercial or NFR license

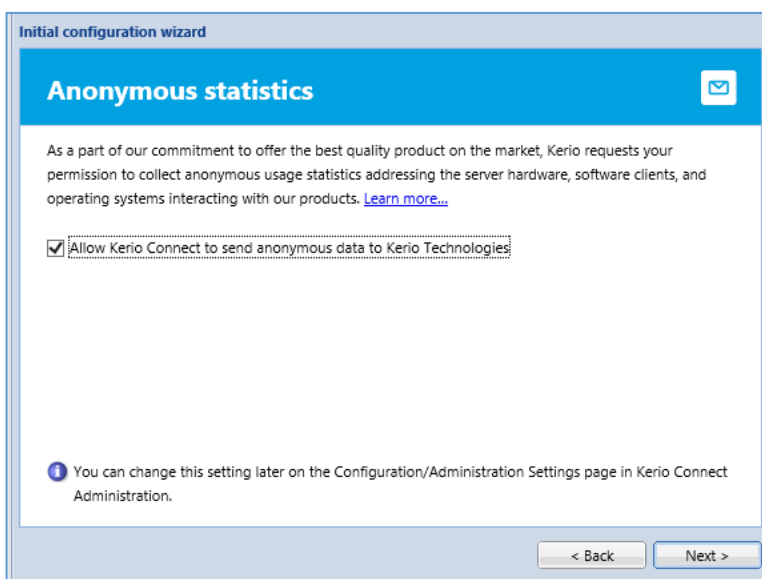
I want to try it free for 30 days

< Back Next >

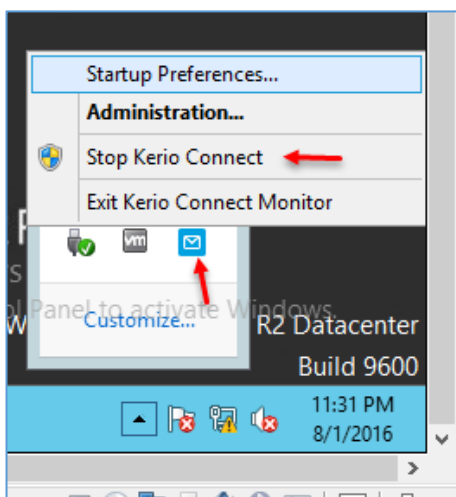
در این صفحه باید لایسنس نرم افزار را معرفی کنید که اگر لایسنس را خریداری کردید، **Licence** را انتخاب کنید و اگر می خواهید از نسخه ی آزمایشی استفاده کنید باید بر روی **Trial** کلیک کنید.



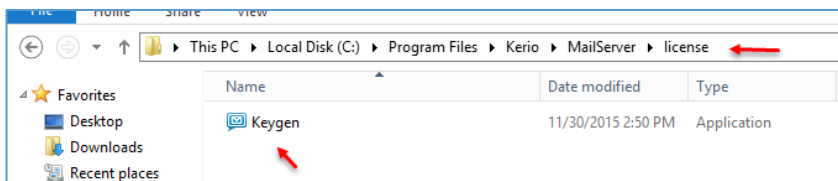
در این صفحه برای دریافت لایسنس آزمایشی بر روی **Get a Trial License Number** کلیک کنید و در سایت کریو ثبت نام کنید و لایسنس را دریافت کنید، اگر می‌خواهید نرم‌افزار را با کرک موجود در فایل دانلود، کرک کنید، **Active in Unregistered mode** را انتخاب کنید.



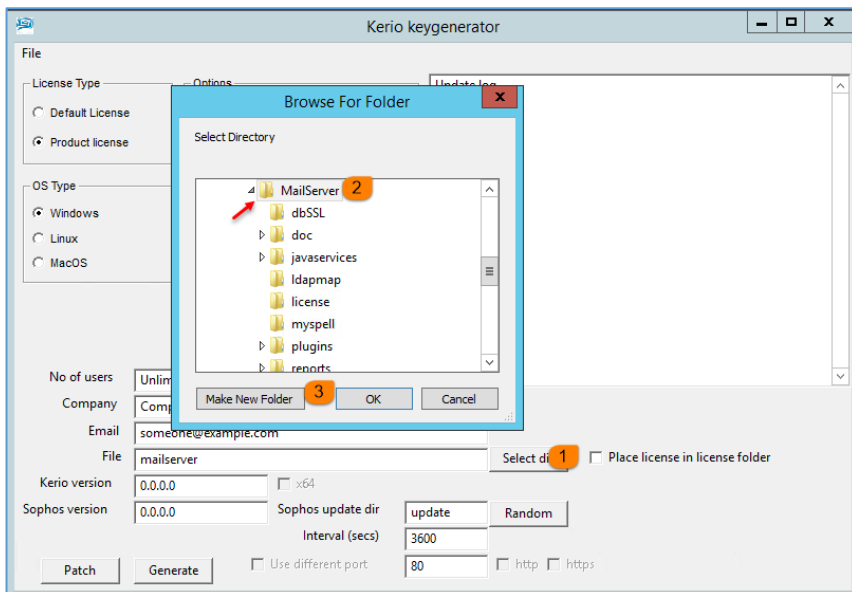
بر روی **Next** کلیک کنید و در پایان بر روی **Finish** کلیک کنید تا نصب به اتمام برسد.



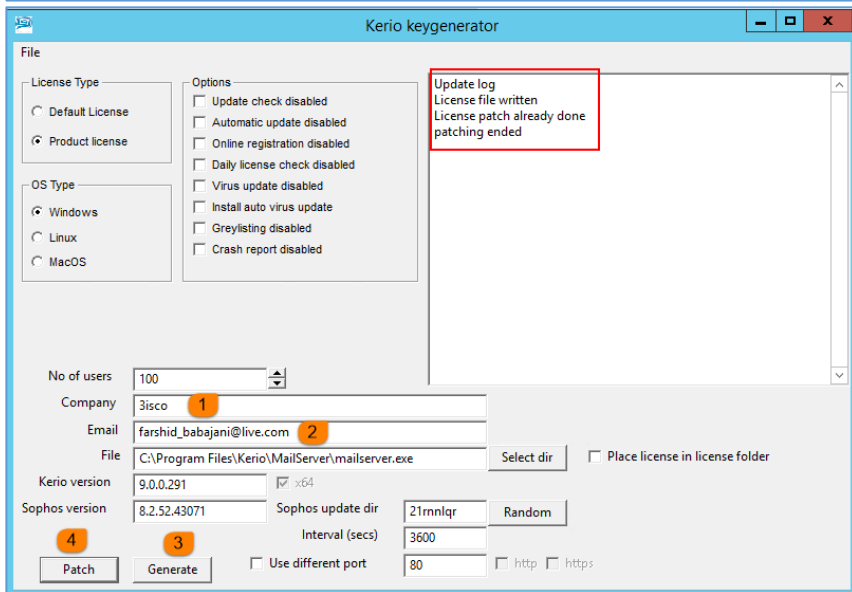
برای کرک کردن **Kerio Connect 9** می‌توانید از فایل کرک درون فایل دانلود استفاده کنید، برای انجام این کار به مانند شکل روبرو بر روی آیکون **Kerio Connect** کلیک راست کنید و گزینه **Stop Kerio Connect** انتخاب کنید تا سرویس مربوط به آن **Stop** شود.



برای فعال کردن KerioConnect، برنامه‌ی Keygen را از فایل دانلودشده، دریافت و در آدرس روبرو کپی کنید.

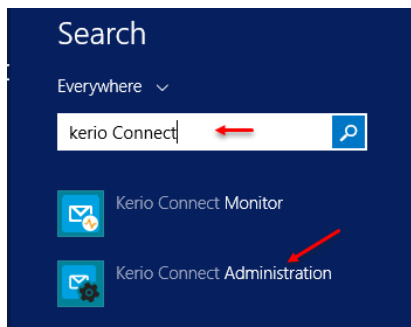


در شکل روبرو برای فعال‌سازی برنامه بر روی شماره‌ی یک، یعنی Select dir کلیک کنید و مسیر نصب را به مانند شکل انتخاب و بر روی ok کلیک کنید تا اطلاعات نرم‌افزار به Keygen داده شود.



بعد از اینکه اطلاعات نرم‌افزار دریافت شد، در قسمت شماره‌ی یک و دو، نام و ایمیل خود را وارد کنید؛ در قسمت شماره‌ی سه، Generate را کلیک کنید تا فایل لایسنس ساخته شود و در مرحله‌ی بعد بر روی شماره‌ی چهار، Patch کلیک کنید تا نرم‌افزار به مانند شکل روبرو فعال شود.

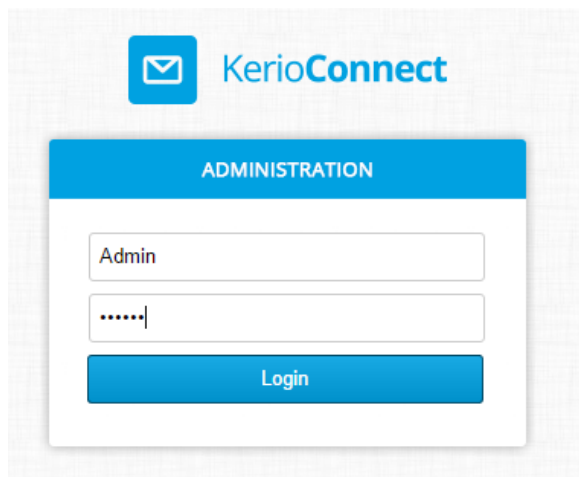
بعد از فعال‌سازی، سیستم را Restart کنید.



بعد از فعال‌سازی نرم‌افزار وارد Search شوید و kerio Connect را وارد کنید و نرم‌افزار Kerio Connect Administration را اجرا کنید یا می‌توانید مرورگر خود را باز و آدرس زیر را وارد کنید:

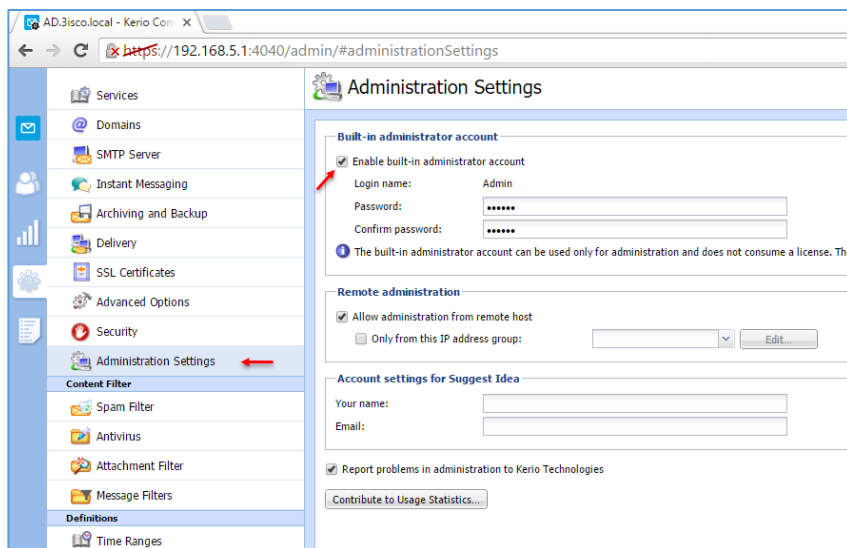
<https://192.168.5.1:4040/admin/login>

در آدرس صفحه‌ی پیش، شما باید به جای 192.168.5.1، آدرس سروری که Kerio Connect در آن نصب کردید را وارد کنید.



در صفحه‌ی Login باید نام کاربری و رمز عبور را که در هنگام نصب وارد کردید را در این قسمت وارد کنید و بر روی Login کلیک کنید.

نرم افزار با موفقیت اجرا شده است که در شکل بالا این موضوع را مشاهده می کنید، اگر به قسمت License Details توجه کنید، لایسنس مورد نظر تا سال ۲۰۳۰ فعال شده است و می توانید از نرم افزار استفاده کنید.

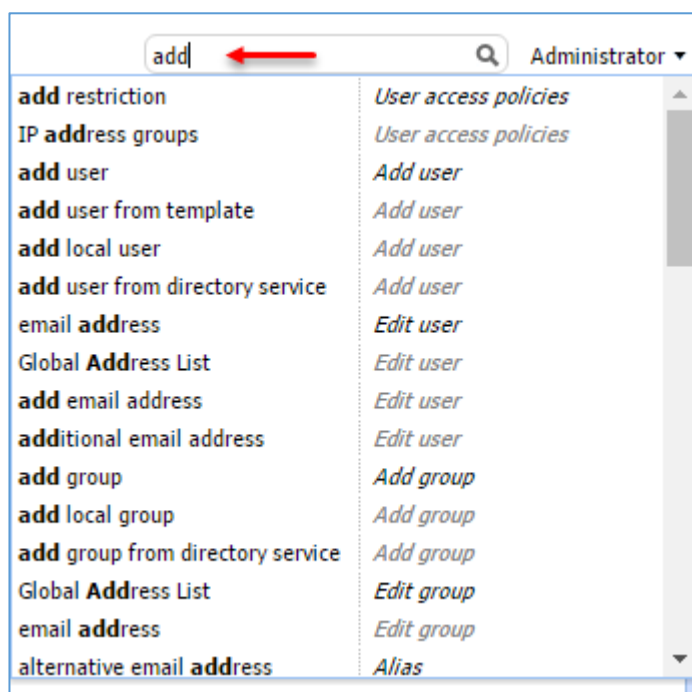


برای شروع کار و برای دسترسی از راه دور می‌توانید اکانت Admin که با نام Built-in administrator account شناخته می‌شود را فعال کنید، برای فعال‌سازی به مانند شکل روبرو وارد Administration Settings شوید و تیک گزینه Built-in administrator account را انتخاب و بر روی Apply کلیک کنید.

توجه داشته باشید، اکانت Admin در این قسمت ربطی به امانت admin ندارد و این اکانت فقط برای ورود به صفحه‌ی مدیریتی کاربرد دارد.

استفاده از قابلیت Search در Kerio Connect:

یکی از قابلیت‌های جالب Kerio Connect، استفاده از قابلیت Search یا همان جستجوی آن است که با نوشتن یک کلمه، اطلاعات آن در نرم‌افزار برای شما نمایش داده می‌شود که با هم این موضوع را بررسی می‌کنیم.

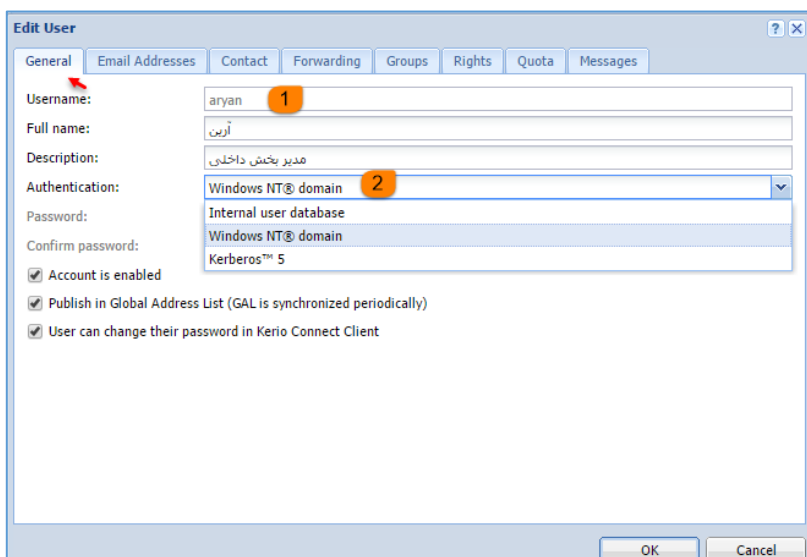
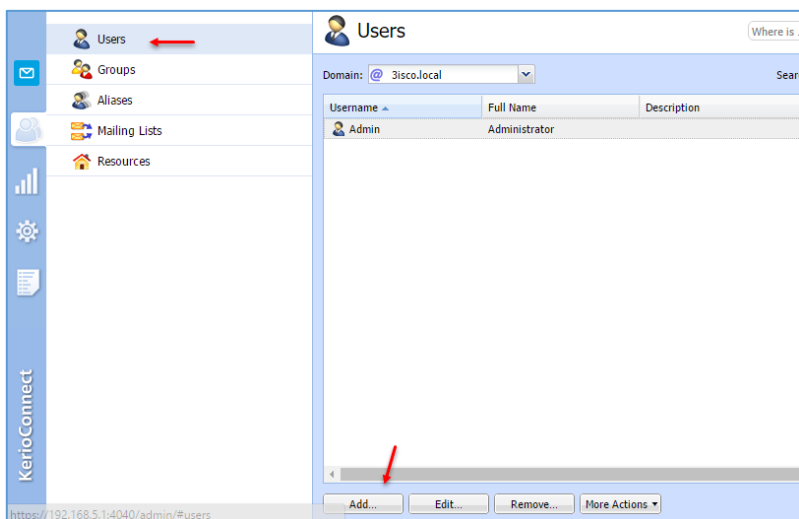


اگر در قسمت جستجو، یک کلمه وارد کنید، تمام قسمت‌هایی که این کلمه در آن وجود دارد برای شما به نمایش گذاشته خواهد شد، مثلاً در شکل روبرو کلمه‌ی Add وارد شده است که تمام اطلاعات مربوط به این کلمه برای شما به نمایش گذاشته شده است.

مثلاً در قسمت بعد می‌خواهیم نحوه‌ی تعریف کاربر جدید را انجام دهیم که با بررسی گزینه‌های موجود در شکل روبرو گزینه‌ی add user را مشاهده می‌کنید که با کلیک بر روی آن به صفحه‌ی مورد نظر انتقال داده خواهید شد.

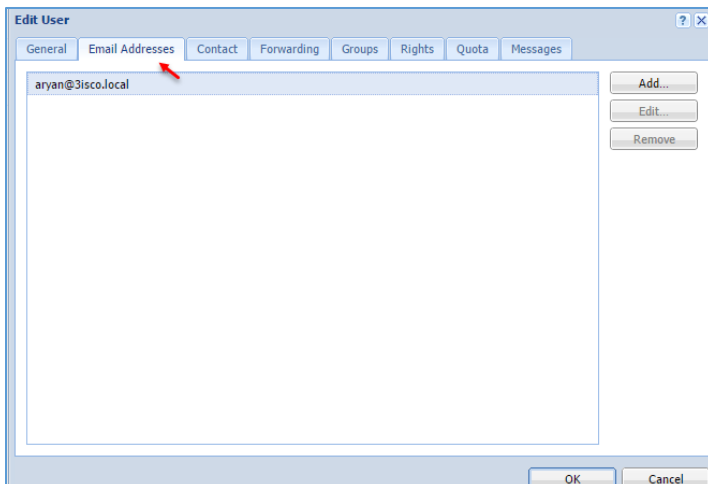
تعریف کاربر در Kerio Connect:

برای تعریف کاربر جدید به مانند شکل روبرو وارد قسمت Accounts شوید و بر روی users کلیک کنید؛ برای تعریف کاربر جدید بر روی Add کلیک کنید.

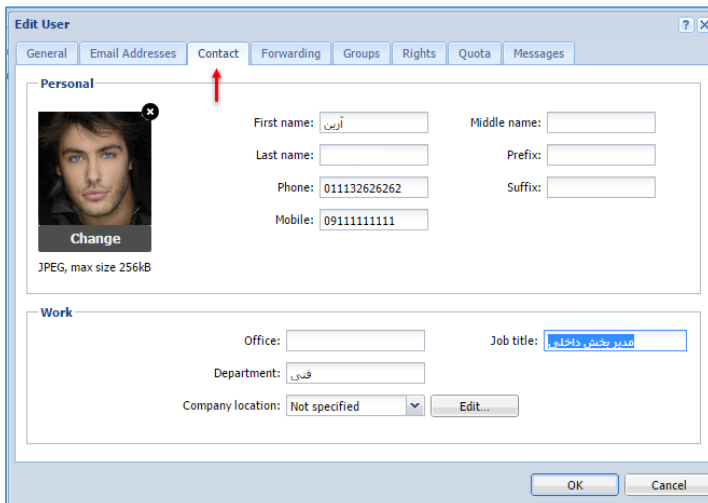


در این صفحه و در قسمت General، نام کاربری را در قسمت شماره‌ی یک، Username وارد کنید و در قسمت Full Name می‌توانید نام کامل کاربر را بنویسید؛ در قسمت Authentication می‌توانید نوع تأیید اعتبار را مشخص کنید، اگر گزینه‌ی Internal user database را انتخاب کنید می‌توانید یک کاربر داخلی مربوط به Kerio Connect را ایجاد کنید، اما اگر Windows NT

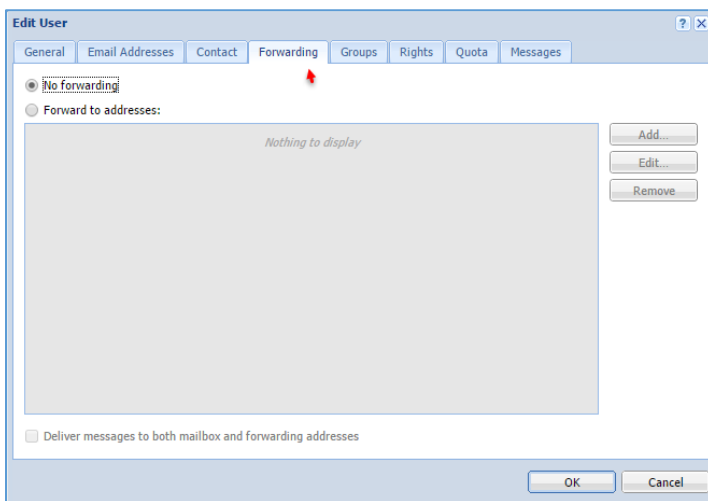
domain را انتخاب کنید، می‌توانید کاربری که در دومین خود تعریف کردید را در این قسمت وارد کنید، توجه داشته باشید که اگر گزینه‌ی Windows NT domain را انتخاب کنید، رمز عبور، همان رمزی است که در دومین برای کاربر تعریف کردید که این به نظر بهتر خواهد بود. در سه گزینه‌ی آخر، **Account is enabled** برای فعال کردن کاربر مورد نظر است، گزینه‌ی **Publish in Global...** برای انتقال آدرس ایمیل کاربر به لیست آدرس که در ادامه روی آن بحث خواهیم کرد و گزینه‌ی سوم برای دسترسی به کاربر برای تغییر رمز عبور است.



در تب **Email Addresses** می‌توانید آدرس ایمیل کاربر را مشاهده کنید که از همین آدرس باید برای ارتباط کاربر با سرور ایمیل استفاده کنید.

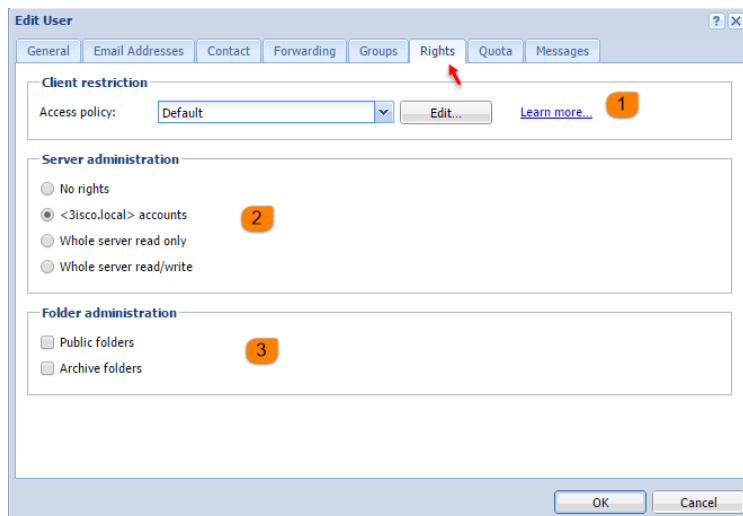


در قسمت **Contact** می‌توانید عکس کاربر و مشخصات آن را به صورت کامل وارد کنید.



در تب **Forwarding** می‌توانید ایمیل کاربر را به ایمیلی دیگر، **Forward** کنید که برای این کار باید گزینه **Forward to address** را انتخاب و بر روی **Add** کلیک کنید و آدرس ایمیل جدید را وارد کنید تا ایمیل کاربر به ایمیل دیگر ارسال شود.

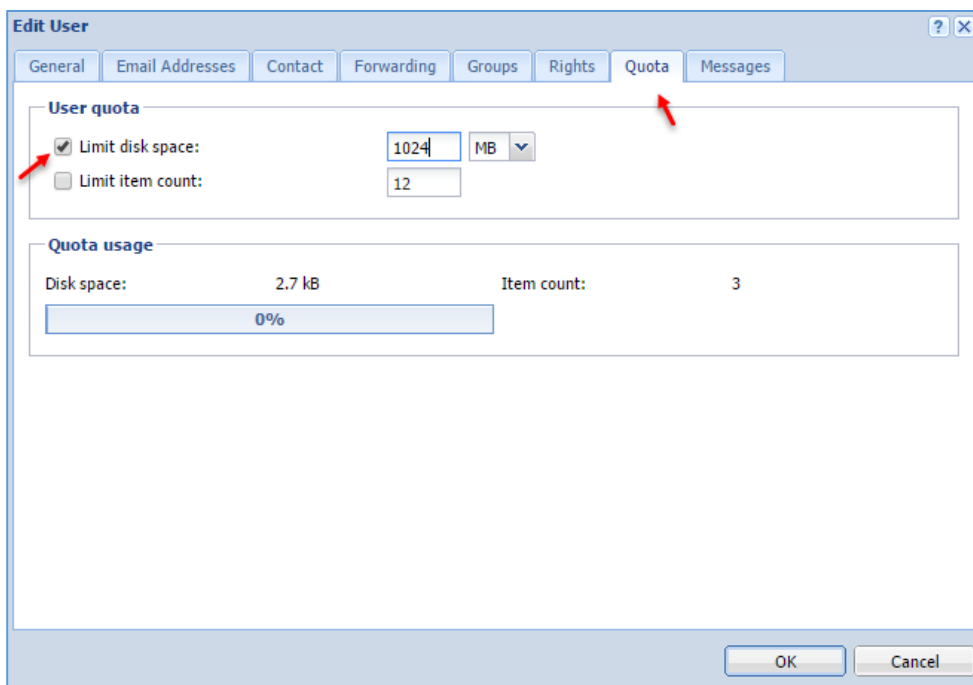
در تب **Groups** می‌توانید یک گروه انتخاب کنید تا کاربر، عضو آن گروه شود؛ در ادامه در مورد ایجاد گروه به بحث خواهیم پرداخت.



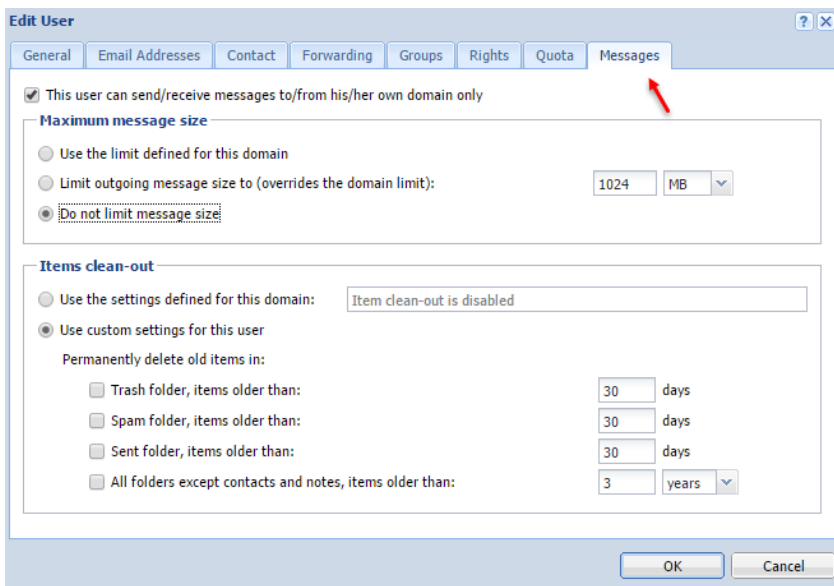
در قسمت **Rights**، سه قسمت وجود دارد که در قسمت شماره‌ی یک، یک سری **Policy** به صورت پیش‌فرض تعریف شده است که می‌توانید یکی از آن‌ها را با کلیک بر روی **Edit** انتخاب کنید که به صورت پیش‌فرض بر روی **Default** قرار دارد که تمامی دسترسی‌ها را به کاربر می‌دهد؛ در قسمت شماره‌ی ۲ باید یک سری دسترسی‌ها به کاربر دهید تا به قسمت مدیریتی **Kerio Connect** دسترسی

داشته باشد، اگر گزینه‌ی **<3isco.local>accounts** را انتخاب کنید، کاربر می‌تواند به قسمت مدیریتی **Kerio connect** وارد شود که این دسترسی محدود است، اگر گزینه‌ی **Whole server read only** را انتخاب کنید، کاربر تمامی گزینه‌های قسمت مدیریتی را مشاهده می‌کند، اما نمی‌تواند گزینه‌ای را تغییر دهد، البته اگر گزینه‌ی **Whole server read/write** انتخاب کنید به مانند کاربر **admin** به قسمت مدیریتی دسترسی کامل خواهید داشت.

در قسمت شماره‌ی سه می‌توانید دسترسی کاربر را به فولدر **Public** و **Archive** مشخص کنید.

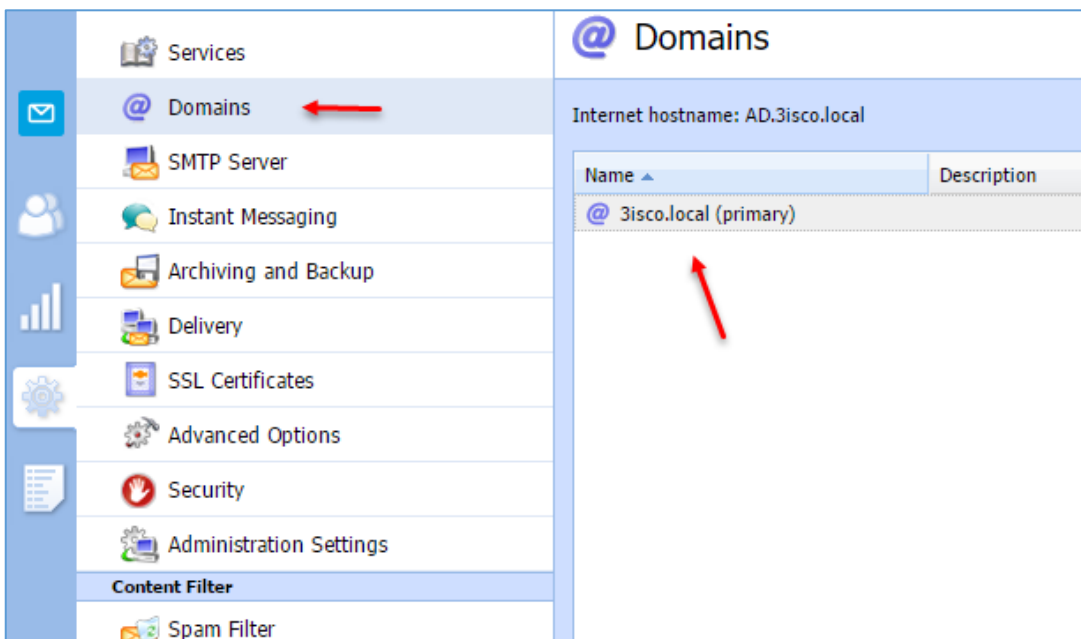


در تب **Quota** می‌توانید حجم مشخصی را برای کاربر تعیین کنید که در شکل روبرو با انتخاب گزینه‌ی **Limit disk space** و دادن **1024** مگابایت **space** این کار انجام شده است، گزینه‌ی **Limit item count** برای تعیین تعداد ایمیل است که می‌توانید تعداد ایمیل یک کاربر را مشخص کنید.

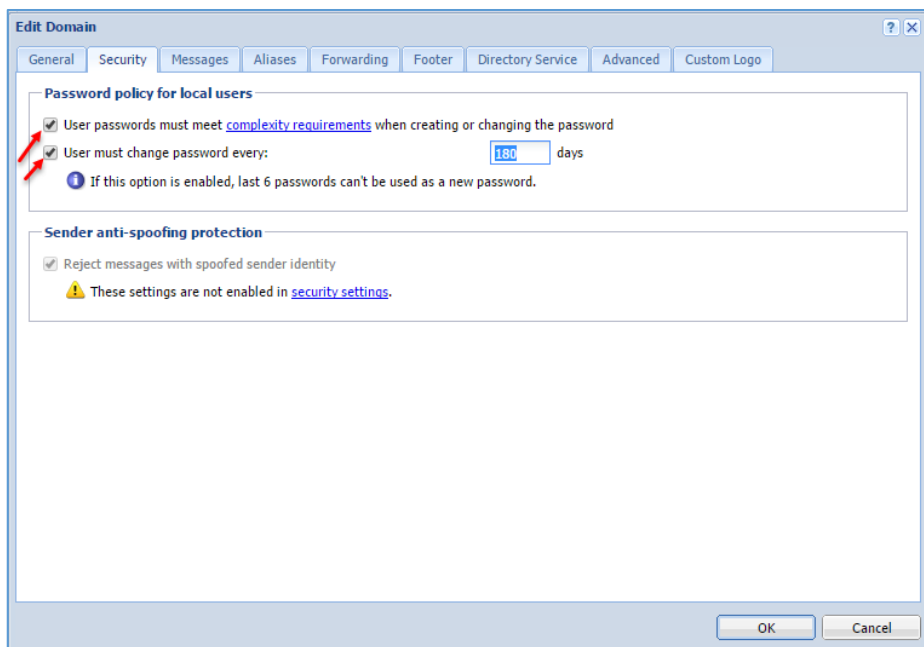


در قسمت Messages نیز می‌توانید قابلیت Instance Messages را که برای چت آنلاین کاربرد دارد برای کاربر فعال کنید؛ در این قسمت می‌توانید مقدار حجم و مدت‌زمان ماندگاری پیام‌ها را مشخص کنید. در آخر بر روی ok کلیک کنید تا کاربر مورد نظر ایجاد شود.

زمانی که بخواهید یک کاربر ایجاد کنید، حتماً باید رمز عبور آن را به صورت پیچیده در Kerio Connect وارد کنید، البته منظور از این کاربر، کاربری است که به صورت Local در Kerio Connect وارد می‌کنید، برای اینکه بتوانید قابلیت پیچیدگی را غیرفعال کنید باید به صورت زیر عمل کنید:



وارد قسمت Domains شوید و بر روی نام دومین خود دو بار کلیک کنید تا شکل بعد ظاهر شود.



در این صفحه وارد تب Security

شوید، در این قسمت و در قسمت

PasswordPolicy for local

users دو گزینه وجود دارد که

گزینه‌ی اول مربوط به وارد کردن رمز عبور کاربر به صورت پیچیده

است که برای اینکه این قابلیت را

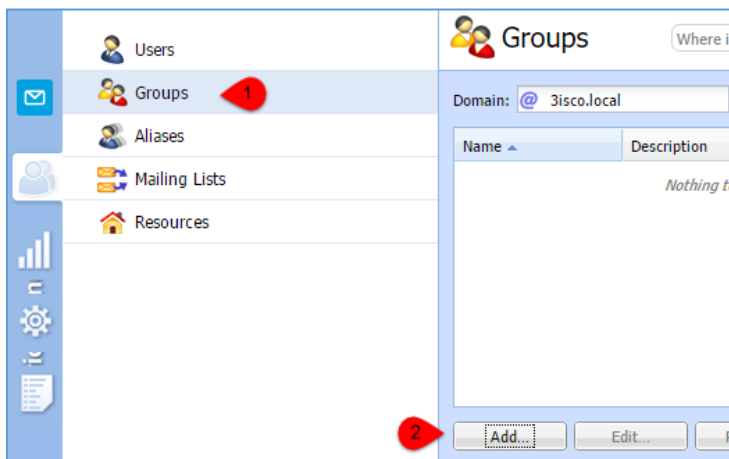
غیر فعال کنید می‌توانید تیک این

گزینه را بردارید، گزینه بعدی

مربوط به این است که با فعال کردن

آن کاربران باید طبق روزی که در شکل مشاهده می‌کنید، رمز عبور خود را تغییر دهید که در اینجا به صورت پیش‌فرض ۱۸۰ روز در نظر گرفته شده است.

ایجاد گروه در Kerio Connect:



برای ایجاد گروه به مانند شکل روبرو وارد قسمت

Accounts شوید و بر روی گزینه‌ی یک،

Groups کلیک کنید و در صفحه‌ی باز شده بر روی

Add کلیک کنید.

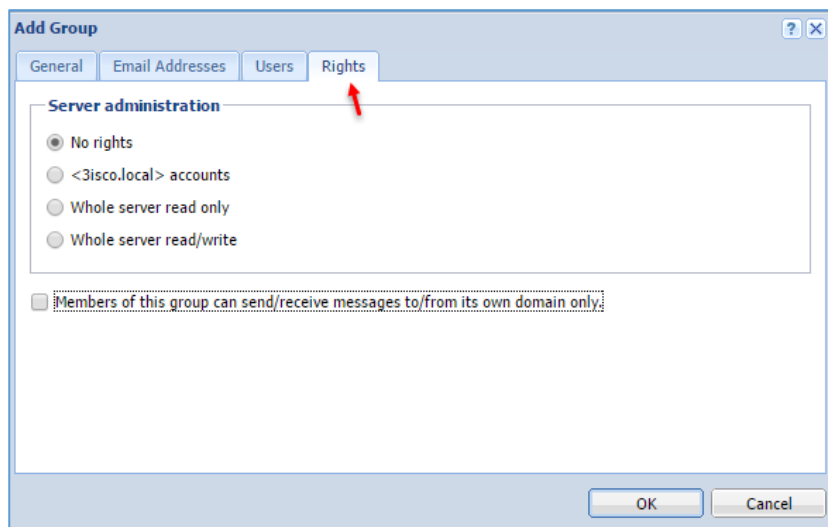
در تب **General** و در قسمت **Name**، نام گروه خود را وارد کنید و اگر تیک گزینه **publish in Global** را انتخاب کنید، این گروه در آدرس لیست قرار می‌گیرد و کاربر می‌تواند نام آن را در لیست خود پیدا کند.

در قسمت **Email Addresses** می‌توانید با کلیک بر روی دکمه **Add**، یک آدرس ایمیل برای این گروه ایجاد کنید که در شکل روبرو این موضوع را مشاهده می‌کنید.

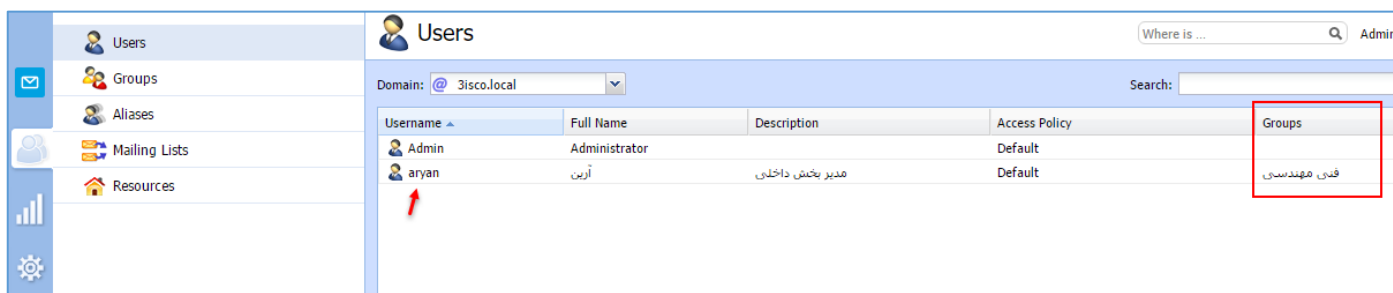
با وارد کردن این آدرس، کاربران دیگر می‌توانند ایمیل‌های خود را به این گروه ارسال کنند تا همه‌ی کاربران عضو این گروه، آن ایمیل را دریافت کنند.

Name	Full Name	Description
aryan	آرین	مدیر بخش داخلی

در قسمت **User** می‌توانید کاربران مربوط به این گروه را با کلیک بر روی **Add** به لیست اضافه کنید.

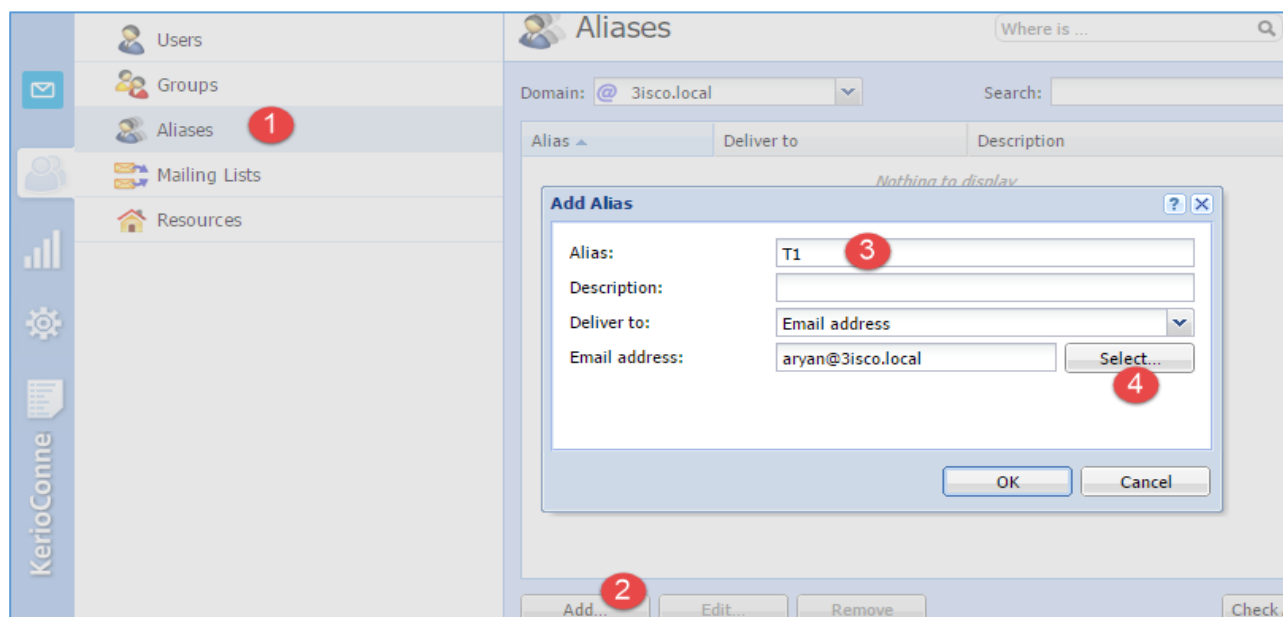


در این صفحه می‌توانید به گروه مورد نظر دسترسی دهید تا کاربران این گروه بتوانند به قسمت مدیریتی دسترسی داشته باشند که به صورت پیش‌فرض، این دسترسی غیرفعال است، در قسمت آخر نیز با انتخاب تیک مورد نظر قابلیت چت را به کاربران گروه خواهید داد.



اگر وارد قسمت Users شوید، جلوی کاربر مورد نظر و در ستون Groups، نام گروهی که کاربر در آن عضو شده است را مشاهده می‌کنید.

ایجاد نام Aliases برای ایمیل کاربران:



گزینه‌ای با نام **Aliaes** وجود دارد که این امکان را به شما می‌دهد که برای یک ایمیل، یک یا چند نام دیگر نیز در نظر بگیرید. در شکل صفحه قبل وارد قسمت **Aliases** شوید و بر روی **Add** کلیک کنید و در پنجره‌ی باز شده در قسمت شماره‌ی سه، نام جدید خود را وارد کنید و در قسمت شماره‌ی چهار، آدرس ایمیل کاربر مورد نظر را انتخاب کنید تا این نام بر روی ایمیل آن ست شود.

بعد از ایجاد **Alias** با نام **T1** می‌توانید به جای استفاده از آدرس aryan@3isco.local از آدرس T1@3isco.local استفاده کنید.

ارتباط نرم‌افزار Outlook با Kerio Connect:

نرم افزار Outlook را که در مجموعه‌ی آفیس موجود است، نصب و اجرا کنید.

با اجرا کردن برنامه‌ی Outlook، گزینه‌ی **Add Account** به صورت پیش فرض اجرا می‌شود که این در صورتی است که هیچ اکانتی را به Outlook معرفی نکرده باشید؛

در شکل روبرو برای معرفی اکانت جدید، گزینه‌ی **Manual setup....** را انتخاب و بر روی **Next** کلیک کنید.

Add Account

Choose Service

Microsoft Exchange Server or compatible service
Connect to an Exchange account to access email, calendars, contacts, tasks, and voice mail

Outlook.com or Exchange ActiveSync compatible service
Connect to a service such as Outlook.com to access email, calendars, contacts, and tasks

POP or IMAP
Connect to a POP or IMAP email account

< Back **Next >** Cancel

در این صفحه، گزینه‌ی POP or IMAP را انتخاب و بر روی Next کلیک کنید.

Add Account

POP and IMAP Account Settings
Enter the mail server settings for your account.

User Information
Your Name:
Email Address:

Server Information
Account Type:
Incoming mail server:
Outgoing mail server (SMTP):

Logon Information
User Name:
Password:
 Remember password
 Require logon using Secure Password Authentication (SPA)

Test Account Settings
We recommend that you test your account to ensure that the entries are correct.

 Automatically test account settings when Next is clicked

Deliver new messages to:
 New Outlook Data File
 Existing Outlook Data File

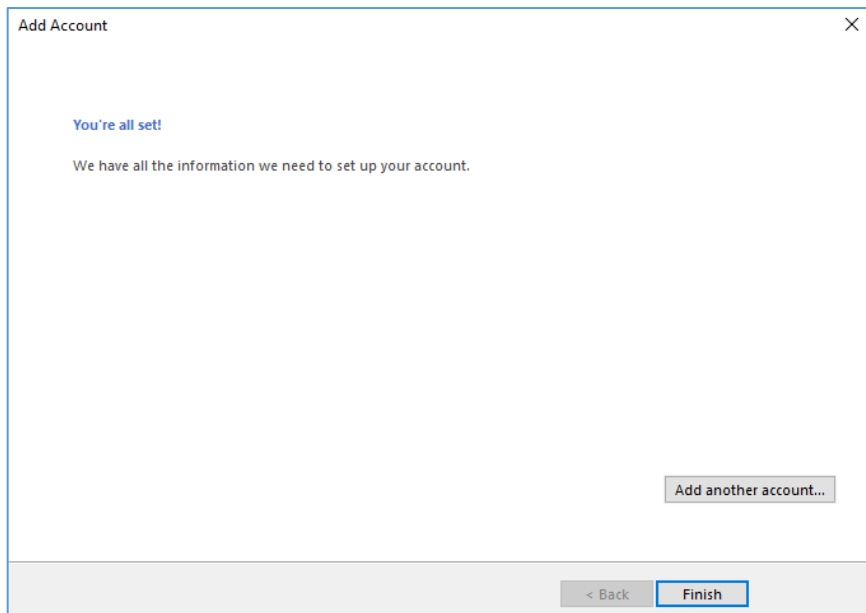
< Back **Next >** Cancel

در این صفحه باید اطلاعات مربوط به ایمیل کاربر و سرور مربوط به آن را وارد کنید؛ در قسمت شماره‌ی یک، نام فرد مورد نظر را وارد کنید، در قسمت Email Address، آدرس ایمیل فرد مورد نظر را وارد کنید، در قسمت Account Type، گزینه‌ی POP3 را انتخاب کنید و در هر دو قسمت Incoming و Outgoing، آدرس سرور ایمیل را وارد کنید و

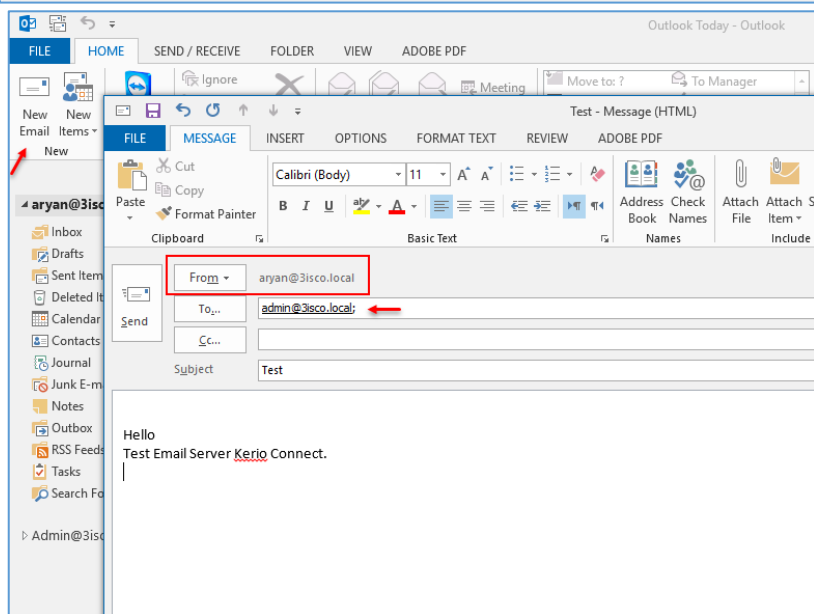
در قسمت Username، نام کاربری یا همان آدرس ایمیل را وارد و در قسمت Password، رمز عبور آن را وارد کنید و در پایان بر روی Next کلیک کنید.

بعد از کلیک بر روی **Next**، ایمیل تست خواهد شد و صفحه‌ی پایانی ظاهر خواهد شد.

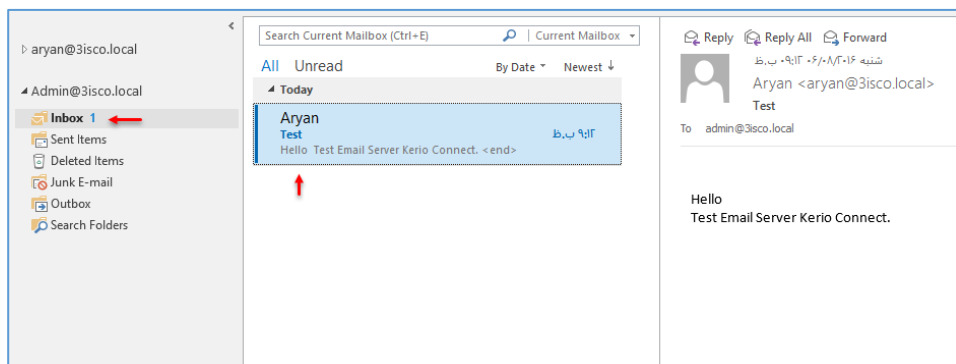
بر روی **Finish** کلیک کنید تا وارد نرم‌افزار **Outlook** شوید.



بعد از وارد شدن به نرم‌افزار **Outlook** بر روی **New Email** کلیک کنید و به مانند شکل از طریق ایمیل **Aryan@3isco.local** که آن را **Add** کردید به ایمیل دیگر نامه‌ای را ارسال کنید.



همانطور که مشاهده می‌کنید، ایمیل با موفقیت به کاربر **Admin** ارسال شده است.



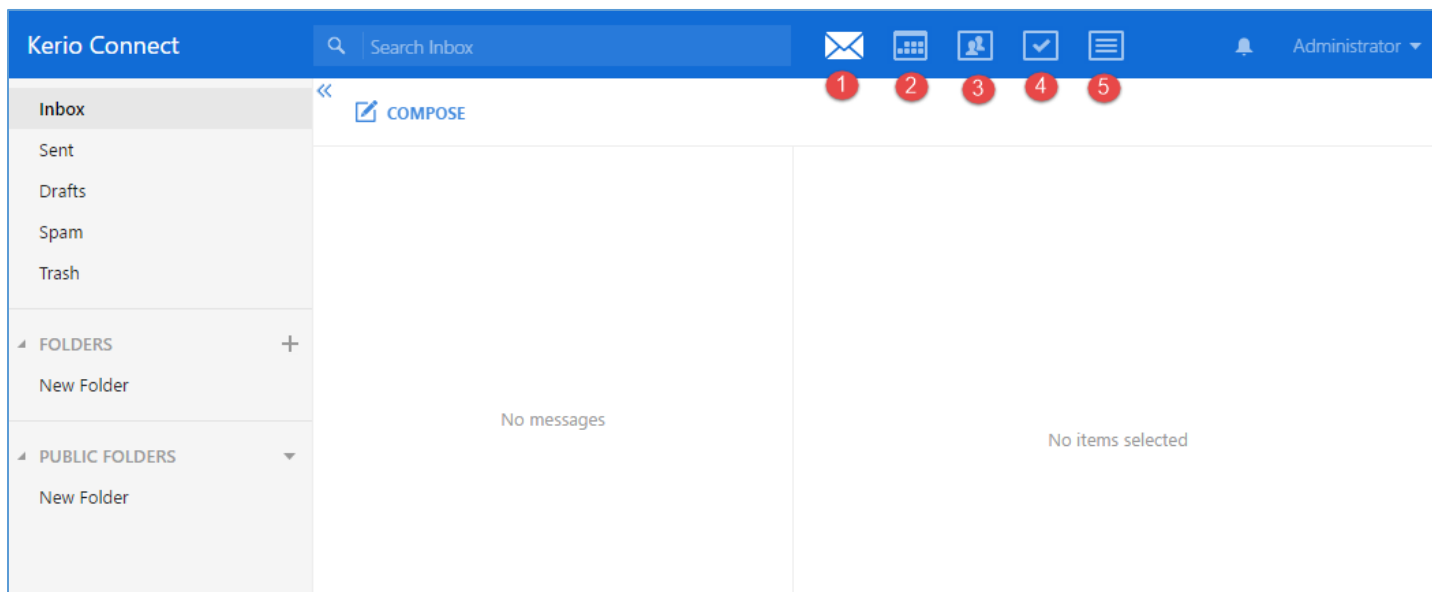
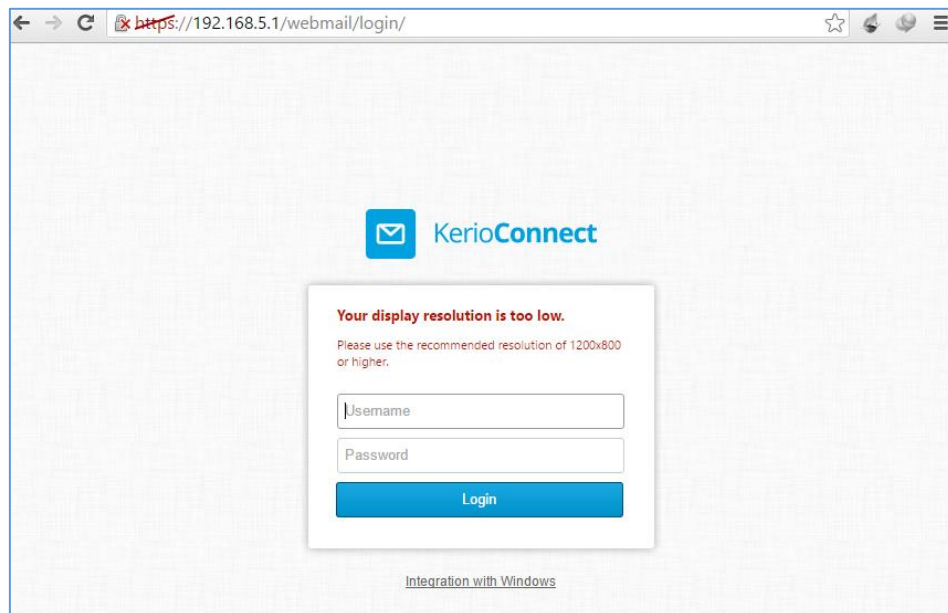
بررسی ایمیل تحت وب: در Kerio Connect، این قابلیت وجود دارد که بتوانید ایمیل‌ها را تحت وب باز

کنید، برای باز کردن ایمیل تحت وب باید آدرس سرور کریو را به صورت زیر وارد کنید:

<https://192.168.5.1/webmail/>

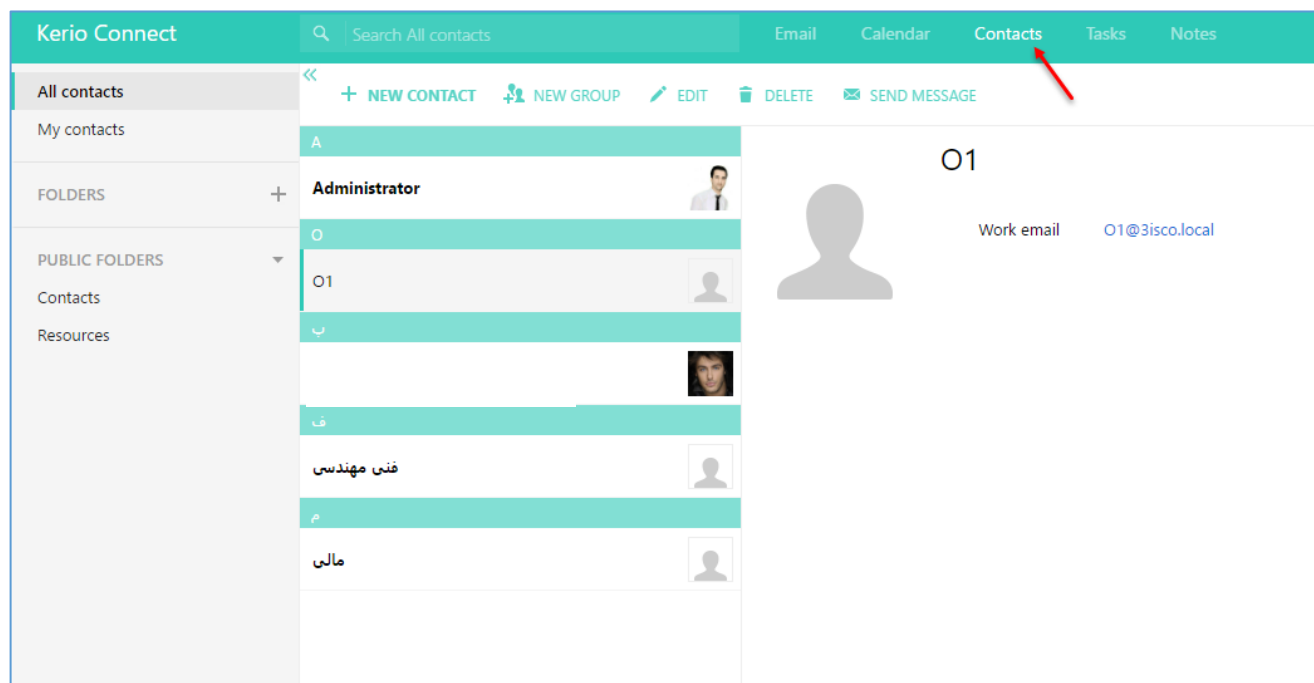
در آدرس مورد نظر شما باید به جای 192.168.5.1، آدرس سرور کریو خود را وارد کنید.

همانطور که مشاهده می‌کنید، صفحه‌ی تحت وب، باز شده است که با وارد کردن نام کاربری و رمز عبور کاربر وارد ایمیل تحت وب خواهید شد.



همانطور که در شکل بالا مشاهده می‌کنید، ایمیل تحت وب برای کاربر Administrator باز شده است.

قسمت شماره‌ی یک، مربوط به ایمیل شما است؛ قسمت شماره‌ی دو، مربوط به تقویم است؛ قسمت شماره‌ی سه، مربوط به تمام اطلاعات کاربران در شبکه است و قسمت شماره‌ی چهار، مربوط به تعریف کار و انجام آلازم در تاریخ و زمان مشخص است؛ قسمت شماره‌ی پنج نیز مربوط به یادداشت است که می‌توانید یادداشت‌های روزانه و کارهای مختلف خود را در آن وارد کنید.



برای مدیریت کاربران در ایمیل تحت وب، با کاربر Admin وارد شوید و بعد وارد قسمت Contacts شوید، همانطور که در شکل بالا مشاهده می‌کنید، صفحه‌ی Contacts باز شده است و لیست کاربران را مشاهده می‌کنید که برای ویرایش هر یک از آن‌ها می‌توانید بر روی آن‌ها دو بار کلیک کنید تا صفحه‌ی زیر باز شود.

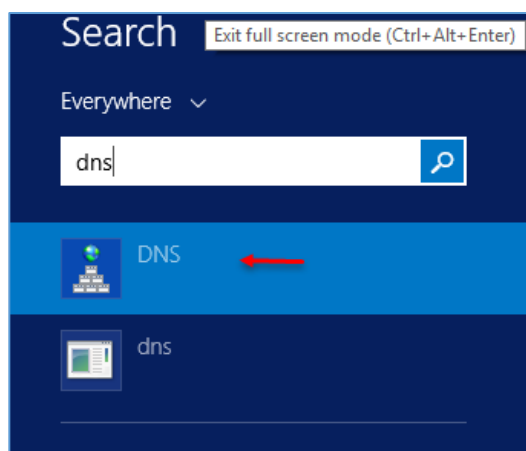
در شکل روبرو اطلاعات کاربر را مشاهده می‌کنید که می‌توانید اطلاعات آن را ویرایش کنید و بر روی Save کلیک کنید تا اطلاعات جدید آپدیت شود.

راه‌اندازی سرویس چت instant Messaging در Kerio Connect:

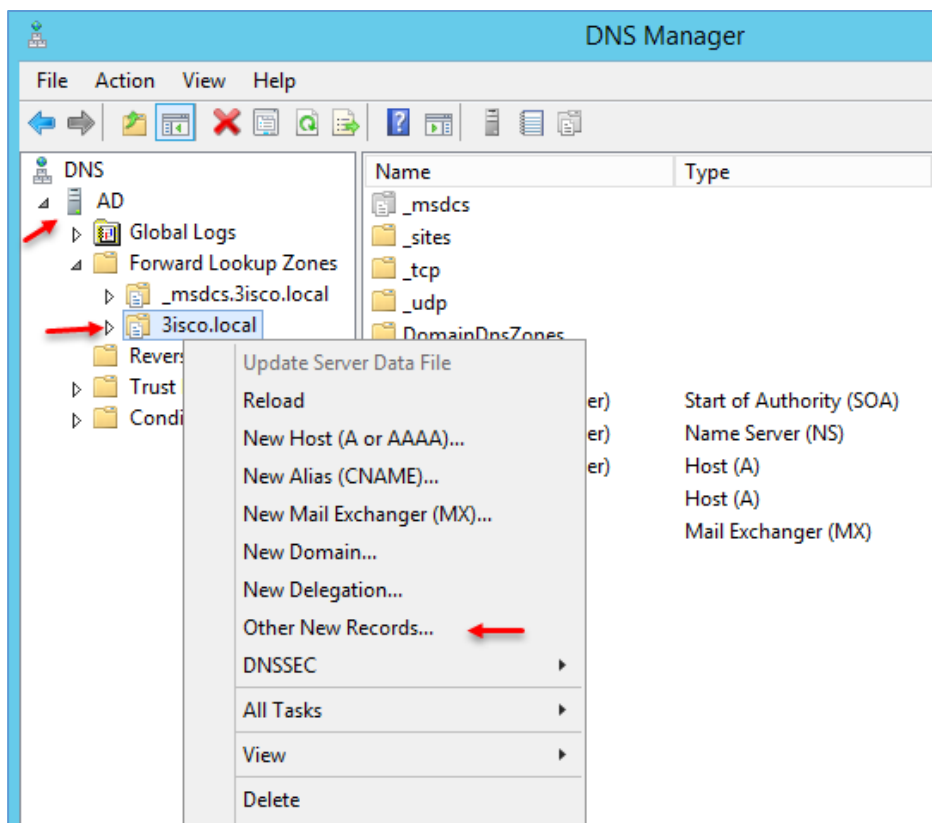
یکی از قابلیت‌های جالب Kerio Connect می‌تواند سرویس چت instant Messaging باشد که قابلیت

چت را برای کاربران فعال می‌کند، برای فعال کردن این سرویس به صورت زیر عمل کنید:

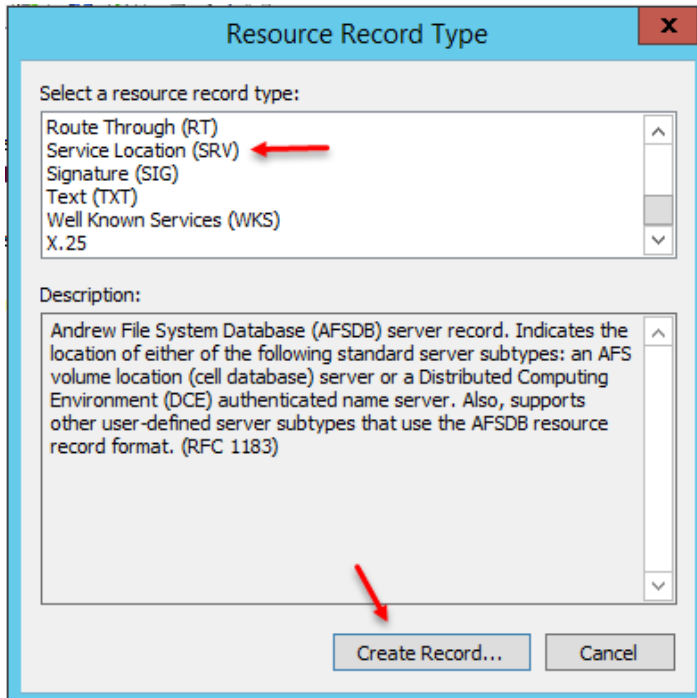
مرحله اول:



برای شروع کار باید دو SRV record در سرویس DNS مربوط به سرور اکتیو دایرکتوری خود ایجاد کنید تا دسترسی لازم به سرویس instant Messaging داده باشید؛ برای شروع وارد سرور اکتیو دایرکتوری شوید و سرویس DNS را اجرا کنید.



به مانند شکل روبرو در سرویس DNS بر روی نام دومین خود کلیک راست و گزینه‌ی Other New Records را انتخاب کنید.



در این لیست، گزینه‌ی Service Location (SRV) را انتخاب کنید و بر روی **Create Record** کلیک کنید تا شکل بعد ظاهر شود.

در این صفحه شما باید در قسمت شماره‌ی یک، نام سرویس را `_xmpp-server` و در قسمت شماره‌ی دو، نام پروتکل را `_tcp` وارد کنید و عدد `۰` و `۵` را در قسمت **Priority** و **Weight** وارد کنید و در قسمت شماره‌ی ۳، شماره‌ی پورت را `۵۲۶۹` وارد کنید و در قسمت شماره‌ی چهار نیز نام سروری که روی آن **Kerio Connect** نصب کردید را وارد و بر روی **ok** کلیک کنید.

New Resource Record

Service Location (SRV)

Domain: 3isco.local

Service: **1** _xmpp-client

Protocol: **2** _tcp

Priority: 0

Weight: 5

Port number: **3** 5222

Host offering this service: **4** ad.3isco.local

Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

در قسمت قبل برای سرویس **_xmpp-client** باید ایجاد کردید، در این قسمت باید برای سرویس **_xmpp-client** فایل SRV را ایجاد کنید که باید به صورت روبرو عمل کنید و اطلاعات را تکمیل کنید.

DNS Manager

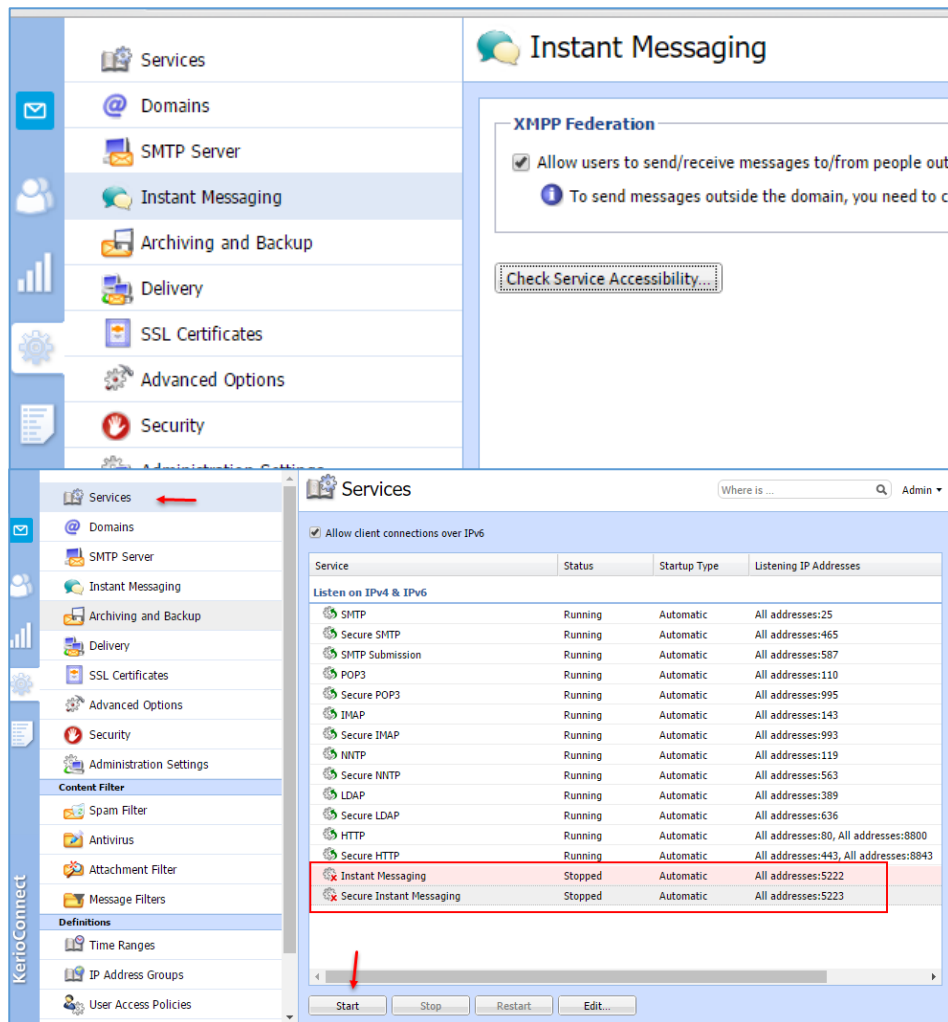
File Action View Help

Name	Type	Data	Timestam
_gc	Service Location (SRV)	[0][100][3268] ad.3isco.loc...	8/18/2016
_kerberos	Service Location (SRV)	[0][100][88] ad.3isco.local.	8/18/2016
_kpasswd	Service Location (SRV)	[0][100][464] ad.3isco.local.	8/18/2016
_ldap	Service Location (SRV)	[0][100][389] ad.3isco.local.	8/18/2016
_xmpp-client	Service Location (SRV)	[0][5][5222] ad.3isco.local.	static
_xmpp-server	Service Location (SRV)	[0][5][5269] ad.3isco.local.	static

همانطورکه در شکل بالا مشاهده می کنید، دو SRV Record برای سرویس **instant Message** ایجاد شده است.

مرحله ی دوم:

در این مرحله باید وارد قسمت مدیریتی Kerio Connect شوید و سرویس InstantMessage را فعال کنید.



به مانند شکل روبرو وارد Instant Messaging شوید و تیک گزینه ی Allow users to send/recive... را انتخاب، بعد بر روی Apply کلیک کنید تا دسترسی لازم به کاربران داده شود.

در ادامه، وارد Services شوید و دو سرویس Instant Messaging و Secure Instant Messaging را انتخاب و بر روی Start کلیک کنید.

بعد از اینکه سرویس instantMessage را به طور کامل فعال کردید باید یک مسنجر روی کلاینت نصب کنید و وارد آن شوید.

مرحله ی سوم:

در این مرحله باید یک مسنجر با نام pidgin دانلود کنید و به سرور متصل شوید.

برای دانلود نرم افزار pidgin می توانید از لینک زیر استفاده کنید:

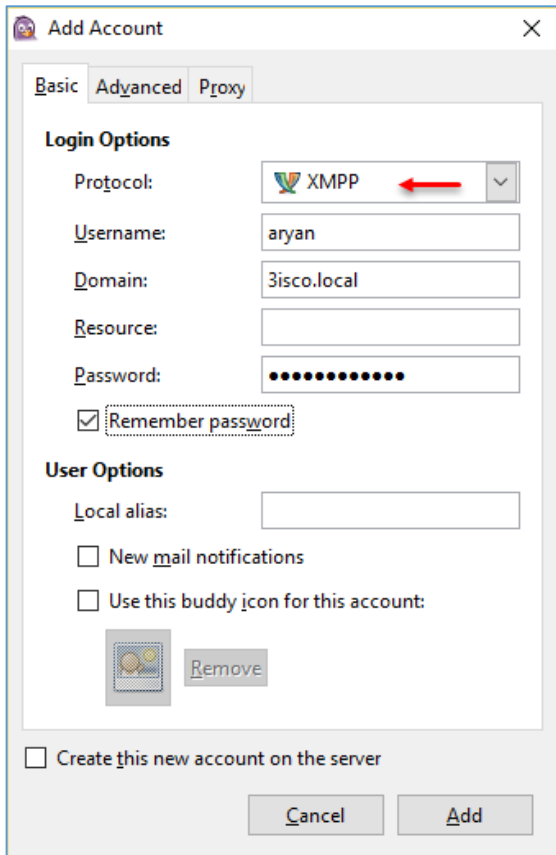
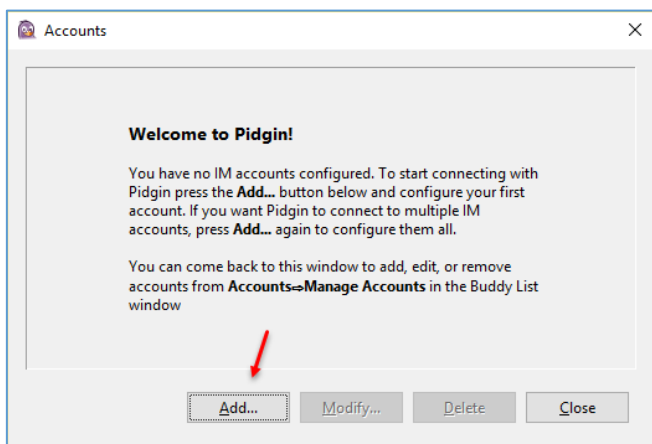
http://download.cnet.com/Pidgin/3000-2150_4-10281799.html

در هنگام نصب، اگر به افزونه ی GTK نیاز داشتید، می توانید از لینک زیر دانلود کنید:

<https://sourceforge.net/projects/gtk-win/>

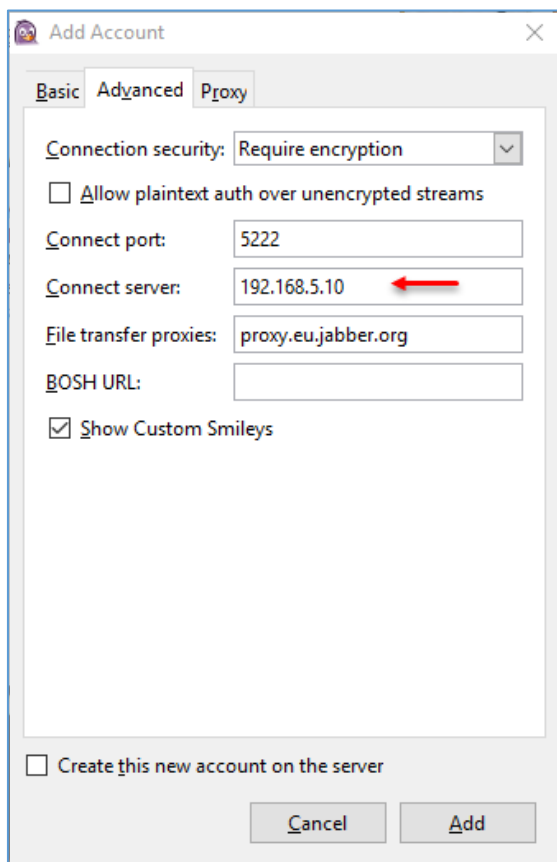
بعد از نصب نرم افزار، آن را اجرا کنید:

بعد از اجرای نرم افزار، شکل روبرو ظاهر می شود که باید بر روی **Add** کلیک کنید تا اکانت و آدرس سرور kerio Connect را وارد کنید.

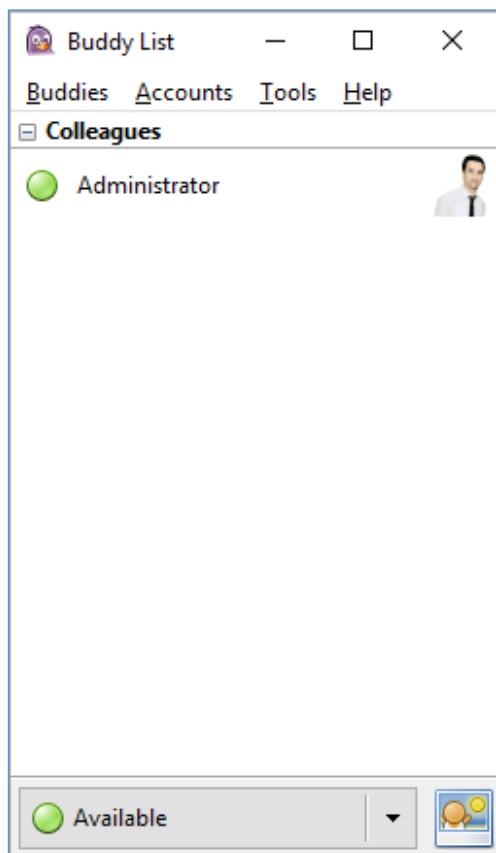


در این صفحه در قسمت Protocol، گزینه ی XMPP را انتخاب و Username کاربر مورد نظر را وارد کنید و بعد در قسمت Domain، نام دومین شبکه ی خود را وارد کنید و رمز عبور را در قسمت Password وارد کنید.

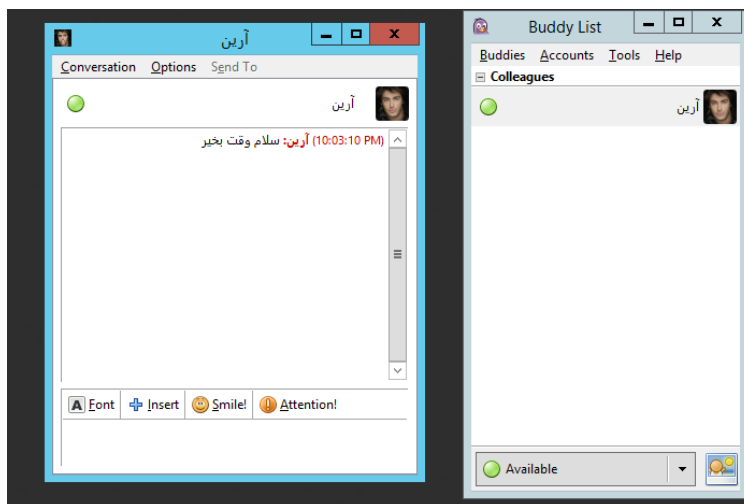
در ادامه، تیک گزینه ی Remember password را انتخاب کنید تا اطلاعات ذخیره شود، بعد از این کار وارد تب Advanced شوید.



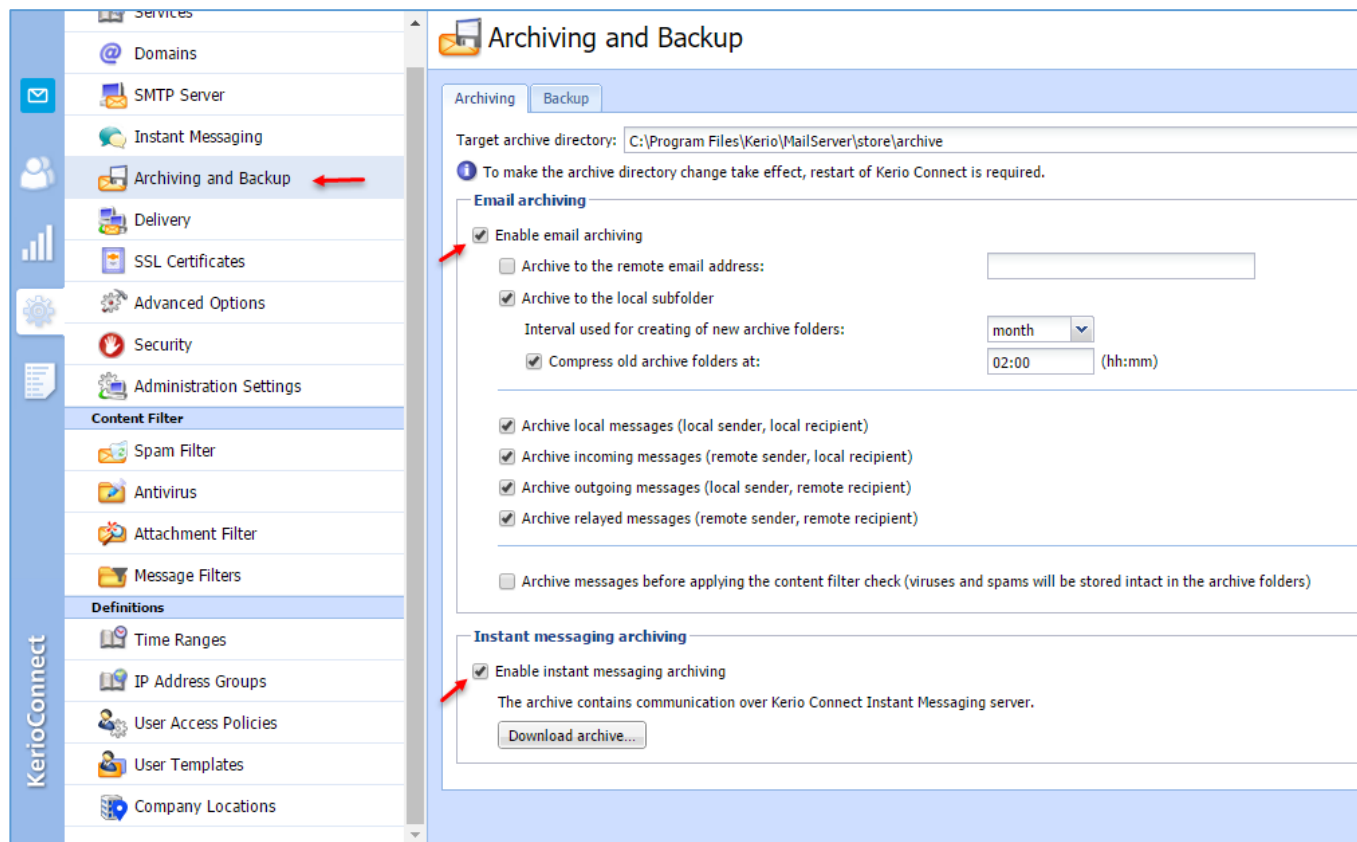
در تب **Advanced** و در قسمت **Connect Server** آدرس سروری که **Kerio Connect** روی آن نصب کردید را وارد و بر روی **ok** کلیک کنید.



همانطور که مشاهده می کنید، کاربر مورد نظر به سیستم مسنجر متصل شده است و کاربر **Administrator** که آنلاین است را مشاهده می کنید.



فعال کردن Backup و Archiving در Kerio Connect



به مانند شکل بالا وارد Archiving and Backup شوید، در این صفحه دو قسمت وجود دارد که یکی برای Email Archiving و دیگری برای Instant messaging archiving کاربرد دارد که می‌توانید تیک هر کدام از گزینه‌ها را که نیاز دارید، فعال کنید.

در بالای صفحه، گزینه‌ی Target archivedirectory وجود دارد که می‌توانید مسیر ذخیره‌سازی فایل‌های آرشیو را مشخص کنید.

اگر بخواهید یک نسخه از آرشیو اطلاعات ایمیل و مسنجر کاربران را تهیه کنید، می‌توانید بر روی Archiving کلیک کنید، بعد از این کار اطلاعات دانلود خواهد شد.

برای ایجاد Backup از اطلاعات کاربران باید به صورت زیر عمل کنید:

The screenshot shows the 'Archiving and Backup' configuration interface. At the top, there are tabs for 'Archiving' and 'Backup'. A search bar and 'Admin' dropdown are in the top right. The main content area has a checkbox labeled 'Enable message store and configuration recovery backup' (marked with a red circle 1). Below it is the 'Backup scheduling' section, which includes a table of backup jobs:

Type	Day	Time	Description
<input checked="" type="checkbox"/> Differential	Thursday	01:00	Differential backup
<input checked="" type="checkbox"/> Differential	Friday	01:00	Differential backup
<input checked="" type="checkbox"/> Differential	Saturday	01:00	Differential backup
<input checked="" type="checkbox"/> Full	Sunday	01:00	Full backup

Buttons for 'Add...', 'Edit...', 'Remove', and 'Advanced...' are located below the table. The 'Target backup directory' section shows a text input field with the path 'C:\Program Files\Kerio\MailServer\store\backup' (marked with a red circle 3) and buttons for 'Select Folder...' and 'Specify...'. The 'Notification' section has a text input field for an email address. The 'Current status' section has a 'Start Now' button (marked with a red circle 4). At the bottom right, there are 'Apply' and 'Reset' buttons.

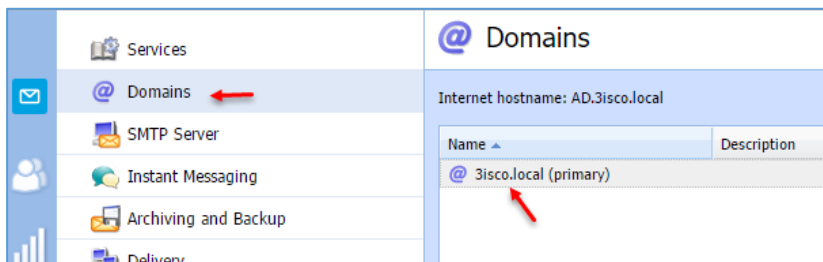
وارد تب Backup شوید و برای فعال کردن سرویس، تیک گزینه‌ی Enable Message Store... را انتخاب کنید، در قسمت شماره‌ی دو، یک‌سری زمان-بندی‌ها برای گرفتن Backup به صورت پیش‌فرض وجود دارد که فقط در روز یکشنبه، یک Backup کامل یا همان Full از کل داده‌ها انجام می‌شود و در روزهای دیگر، Backup به صورت Differential انجام می‌شود، اگر بخواهید خودتان یک زمان‌بندی مشخص ایجاد کنید، می‌توانید بر روی Add کلیک کنید.

در قسمت شماره‌ی سه، مسیر ذخیره‌سازی Backup مشخص شده است که شما می‌توانید با کلیک بر روی Select Folder، این مسیر را تغییر دهید.

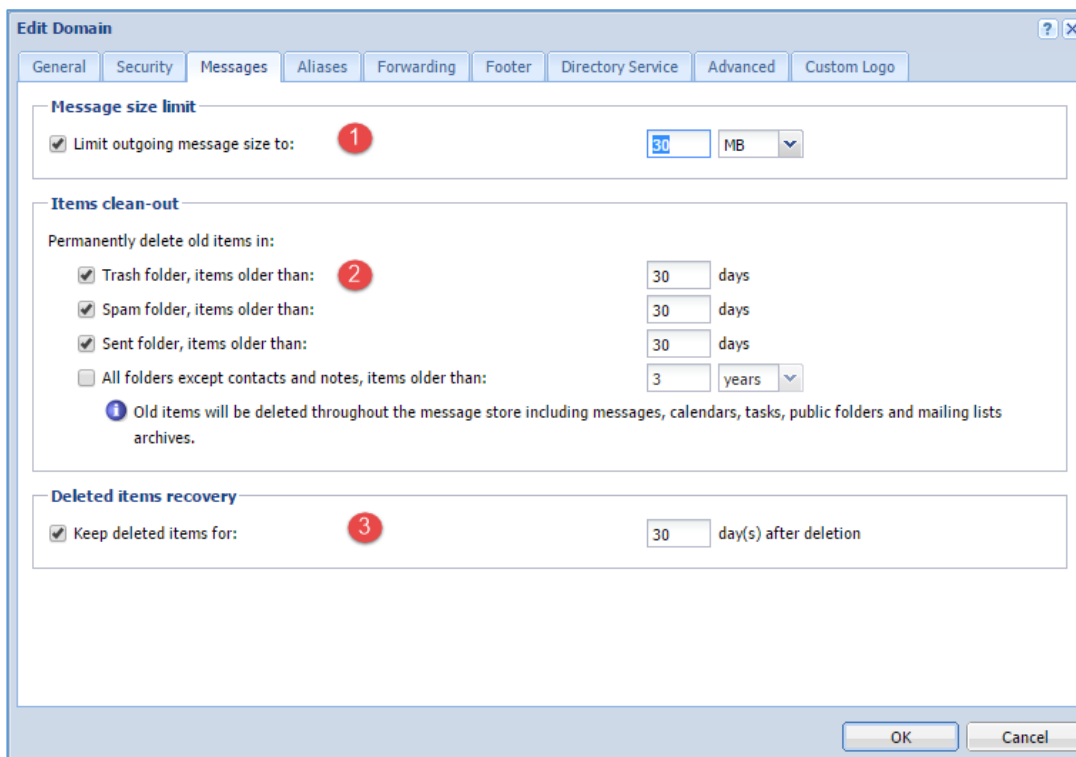
در قسمت شماره‌ی چهار برای شروع به کار، سرویس را بر روی Start Now کلیک کنید تا کار backup آغاز شود.

پاک کردن ایمیل‌های کاربران به صورت اتوماتیک:

برای اینکه بتوانید ایمیل‌های کاربران را در فواصل زمانی مشخص پاک کنید می‌توانید به صورت زیر عمل کنید:



وارد صفحه‌ی Domain شوید و بر روی نام دومین خود، دو بار کلیک کنید.

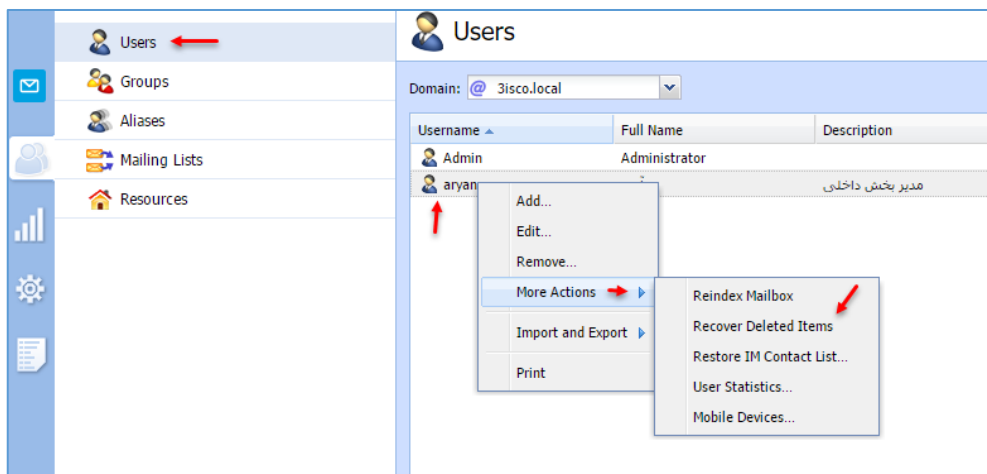


در صفحه‌ی روبرو وارد تب Messages شوید، در این صفحه سه قسمت وجود دارد؛ در قسمت شماره‌ی یک اگر بخواهید حداکثر حجم ایمیل کاربران را برای ارسال مشخص کنید می‌توانید تیک گزینه‌ی

مورد نظر را انتخاب کنید که در این تصویر، هر کاربر می‌تواند حداکثر تا ۳۰ مگابایت ایمیل به دیگران بفرستد.

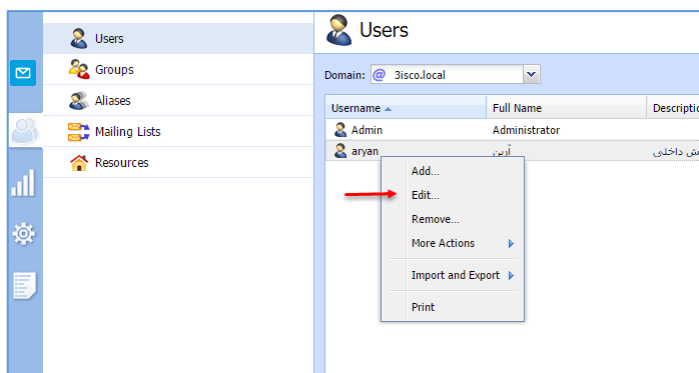
در قسمت شماره‌ی ۲، می‌توانید مقدار ماندگاری پیام‌ها را در سه پوشه‌ی Send, Spam, Trash مشخص کنید که به صورت پیش‌فرض، ۳۰ روز در نظر گرفته شده است که شما می‌توانید بنا به نیاز خود آن را تغییر دهید.

در قسمت شماره‌ی سه، می‌توانید مشخص کنید زمانی که اطلاعات کاربران حذف می‌شود تا چه مدت قابلیت برگشت داشته باشد که در اینجا ۳۰ روز در نظر گرفته شده است، یعنی اگر اطلاعاتی از ایمیل کاربران حذف شود شما می‌توانید حداکثر تا یک ماه، این اطلاعات را به‌روشی که در زیر بیان می‌کنیم برگردانید.

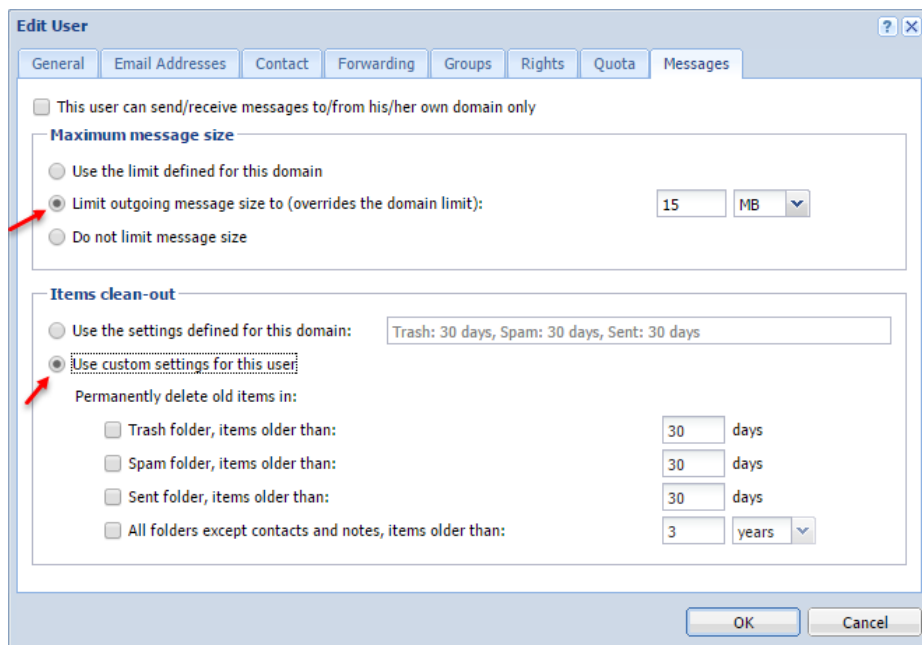


برای اینکه اطلاعات کاربران را ریکاوری کنید باید به صورت روبرو وارد Users شوید و بر روی کاربر مورد نظر کلیک راست کنید و از قسمت **More Actions** گزینه **Recover Deleted Items** را انتخاب کنید.

این مرحله‌ای که انجام دادید برای کل کاربران و در دومین انجام شد، اما اگر بخواهید برای یک یا چند کاربر خاص انجام دهید باید به صورت زیر عمل کنید:

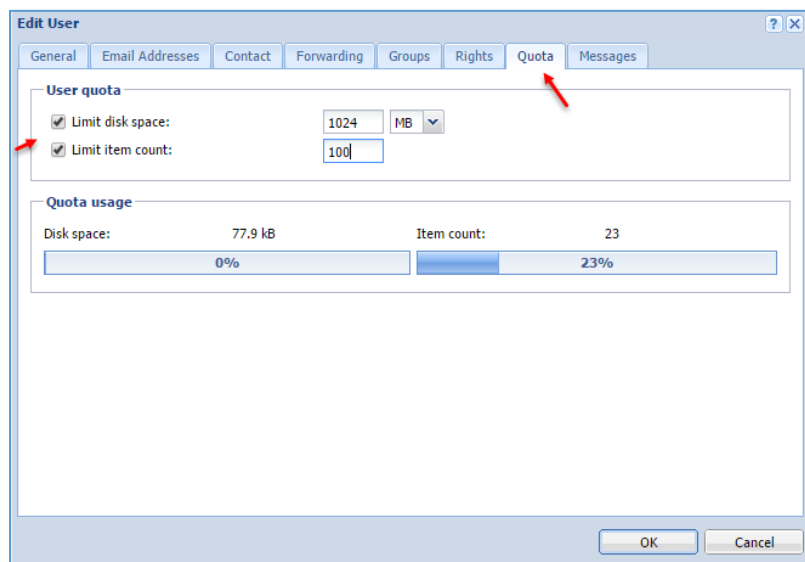


در قسمت **users** بر روی کاربر مورد نظر کلیک راست کنید و گزینه **Edit** را انتخاب کنید و یا بر روی کاربر دو بار کلیک کنید.



در تب **Messages**، همان گزینه‌ها که در قسمت دومین وجود داشت را در این قسمت مشاهده می‌کنید که برای محدود کردن حجم پیام ارسالی برای این کاربر می‌توانید تیک گزینه **Limit outgoing message** را انتخاب و مقدار حجم ارسالی را مشخص کنید.

در قسمت **Items clean-out** می‌توانید تعداد روزهای نگهداری از ایمیل‌ها در جاهای مشخص را وارد کنید.

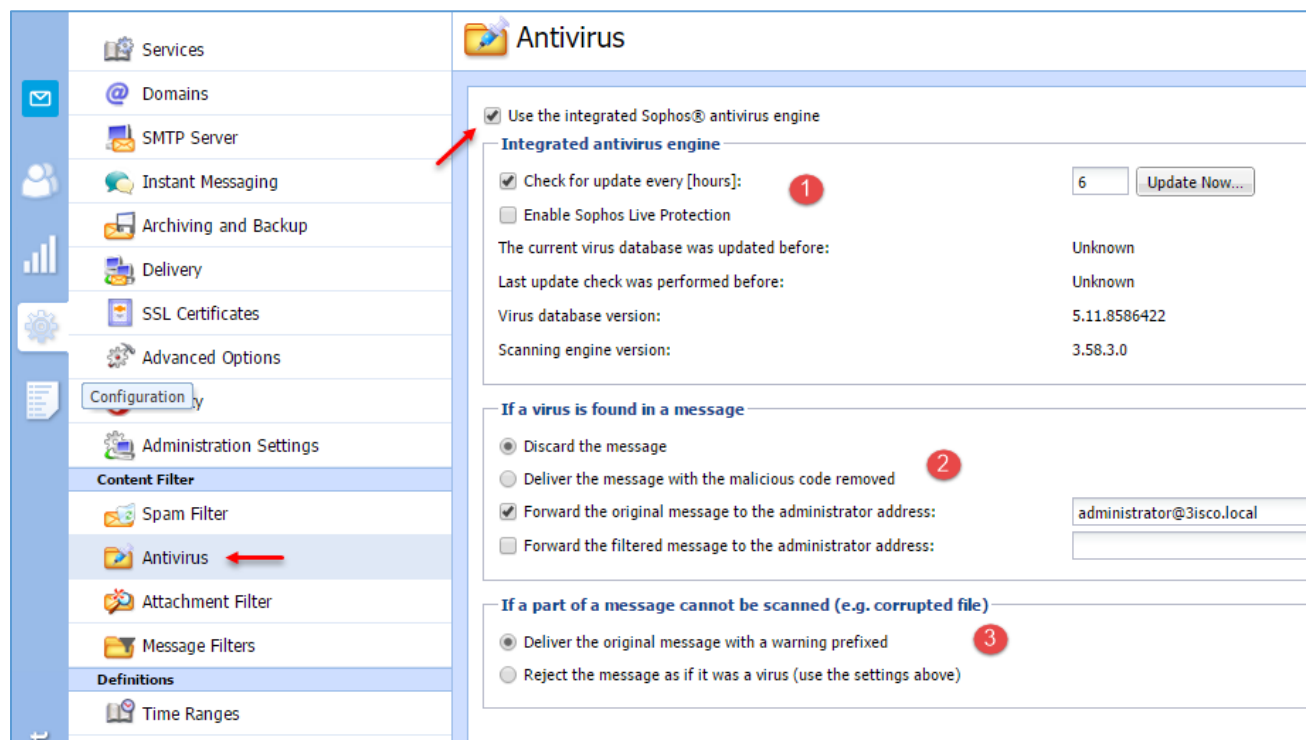


برای اینکه فضای ایمیل کاربران را محدود کنید باید به صورت زیر عمل کنید:

وارد تب **Quota** شوید و در قسمت **User quota** می‌توانید در قسمت اول، فضای ذخیره‌سازی را برای کاربر مورد نظر مشخص کنید و در قسمت **Limit item count** می‌توانید تعداد ایمیل‌های کاربران را مشخص کنید.

فعال کردن Antivirus در Kerio Connect:

برای اینکه **Kerio connect** بتواند ایمیل‌ها را از نظر سالم بودن بررسی کند باید سرویس آنتی ویروس آن را فعال کنید.



برای فعال کردن سرویس آنتی ویروس به مانند شکل صفحه‌ی قبل، وارد **Antivirus** شوید و تیک گزینه‌ی **Use the integrated...** را انتخاب کنید، بعد از انتخاب بر روی **Apply** کلیک کنید تا اطلاعات ذخیره شود.

در قسمت شماره‌ی یک، اگر تیک گزینه‌ی **Check for update every ...** را انتخاب کنید، در صورت متصل بودن به اینترنت، هر ۶ ساعت یک بار، دیتابیس آن آپدیت می‌شود و اگر تیک گزینه‌ی **EnableSophos...** را انتخاب کنید، سرویس **Sophos** نیز که مربوط به سایت آنلاین است، فعال می‌شود.

در قسمت شماره‌ی دو، اگر پیام ویروسی پیدا شد، پیام مورد نظر **Discard** یا از بین می‌رود و اگر بخواهید این پیام برای ایمیل خاصی فرستاده شود و یا گزارش آن فرستاده شود

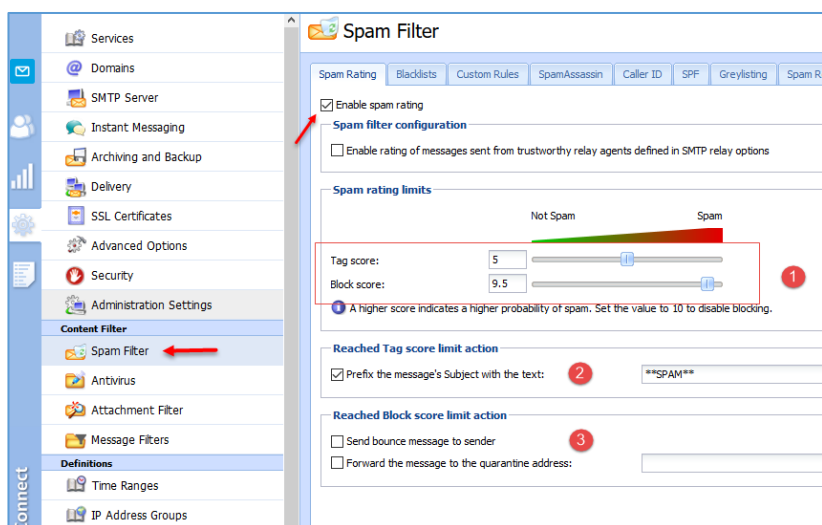
می‌توانید تیک دو گزینه‌ی آخر را انتخاب و آدرس ایمیل خاصی را وارد کنید.

در قسمت شماره‌ی ۳، اگر ایمیلی را نتواند اسکن کند چه کاری بر روی آن ایمیل انجام دهد؟، گزینه‌ی اول، ارسال اصل ایمیل به قرنطینه است که می‌توانید بعداً ایمیل را بررسی کنید و یا رد کردن یا **reject** کردن پیام.

پیگر بندی Spam یا هرزنامه در Kerio control:

در این سرویس، ابزارهایی برای از بین بردن هرزنامه‌ها اجرا می‌شود که در نسخه‌ی جدید آن می‌توان به موارد زیر اشاره کرد:

- ۱- فیلتر کردن پیام‌های هرز توسط اسکن آنلاین سرویس Bitdefender.
- ۲- ایجاد لیست سیاه و سفید که می‌توانید با ایجاد لیستی از آدرس‌های سرور به آن‌ها، اجازه‌ی عبور را بدهید و یا ندهید.
- ۳- SpamAssassin که یک روش تست چندگانه برای فیلتر کردن هرزنامه‌ها است.
- ۴- Greylisting، روشی برای ارسال پیام از فرستنده‌ی شناخته‌شده است.
- ۵- ایجاد یک پیام با سرویس SMTP برای جلوگیری از هرزنامه‌هایی است که از سرورهای دیگر به صورت اتوماتیک ارسال می‌شوند.



برای فعال‌سازی سرویس هرزنامه به مانند شکل روبرو وارد Spam Filter شوید و در تب Spam Rating، تیک گزینه‌ی enable Spam rating را انتخاب کنید، با این کار، سرویس Rating فعال می‌شود، فعالیت این سرویس به این صورت است که در قسمت شماره‌ی یک، دو قسمت وجود دارد که قسمت Tag Score، مربوط به این

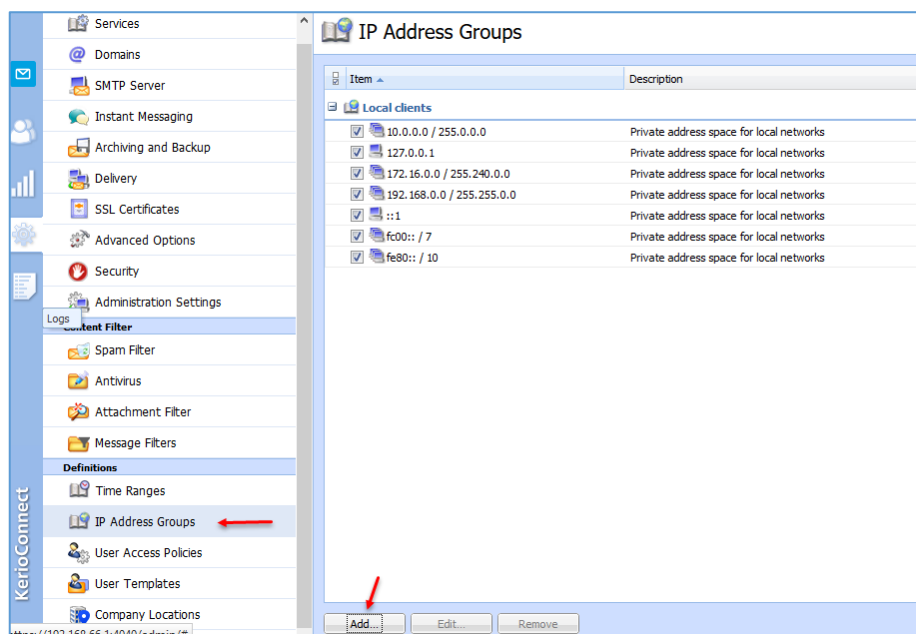
موضوع است که هر پیام هرزنامه از طریق برچسب‌گذاری، شماره‌ای را دریافت می‌کند که اگر این شماره به مانند شکل از ۵ بیشتر باشد، آن پیام به عنوان هرزنامه برچسب‌گذاری می‌شود و در قسمت Block Score، اگر مقدار این شماره، مثلاً از ۹,۵ بیشتر شد، آن پیام مسدود می‌شود.

در قسمت شماره‌ی دو می‌توانید نام برچسب‌گذاری را مشخص کنید و در قسمت شماره‌ی سه، اگر پیام مورد نظر مسدود شد می‌توانید با انتخاب تیک گزینه‌ی Forward و وارد کردن یک ایمیل، پیام مسدودشده را به آدرس دیگر ارسال کنید.

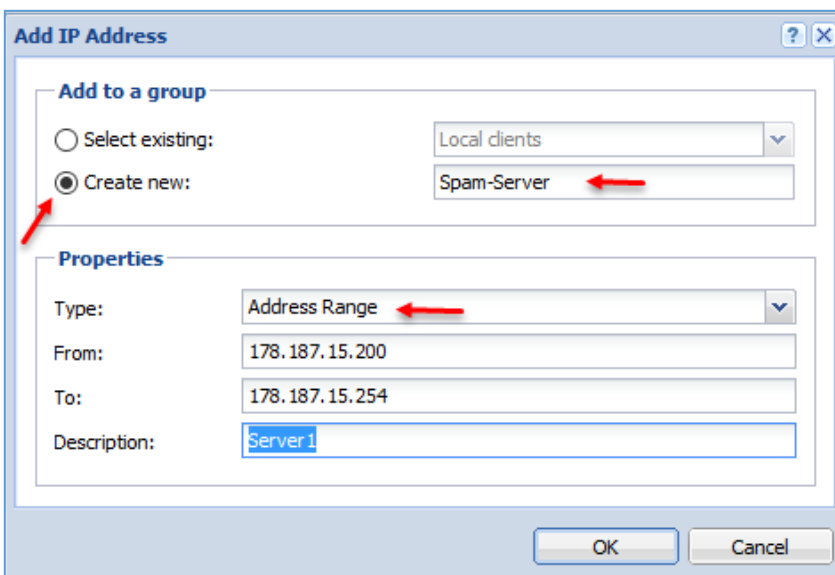
فیلتر کردن پیام‌ها از آدرس‌های خاص:

در Kerio Connect، این قابلیت وجود دارد تا بتوانید با ایجاد گروه‌های خاص از آدرس سرورهایی که باعث ارسال هرزنامه می‌شوند از ارسال پیام‌های آن‌ها به سرور جلوگیری کنید.

برای شروع کار باید یک گروه از آدرس‌هایی را که در نظر دارید را ایجاد کنید که برای این کار باید به صورت زیر عمل کنید:



به‌مانند شکل روبرو وارد IP Address Groups شوید و در صفحه‌ی باز شده بر روی Add کلیک کنید.

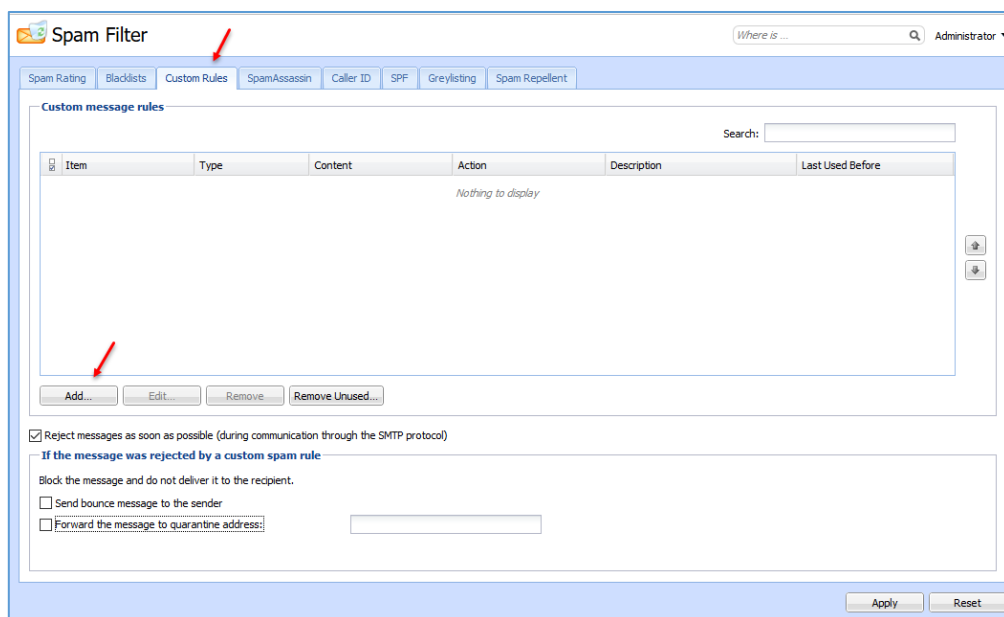


در این صفحه، گزینه‌ی Create new را انتخاب کنید و نام گروه خود را به دلخواه وارد کنید؛ بعد از این کار در قسمت Type، نوع آدرس خود را انتخاب کنید که در این قسمت، Range آدرس انتخاب شده است و باید رنجی از آدرس‌ها که به آن‌ها مشکوک هستید را در قسمت روبرو وارد کنید و بر روی ok کلیک کنید تا گروه مورد نظر ایجاد شود.

بعد از ایجاد گروه در مرحله‌ی قبل باید آن را به سرویس Spam معرفی کنید؛ بدین منظور به‌مانند شکل بالا وارد Spam Filter شوید و بعد وارد تب Black List شوید. در این صفحه، سه قسمت وجود دارد.

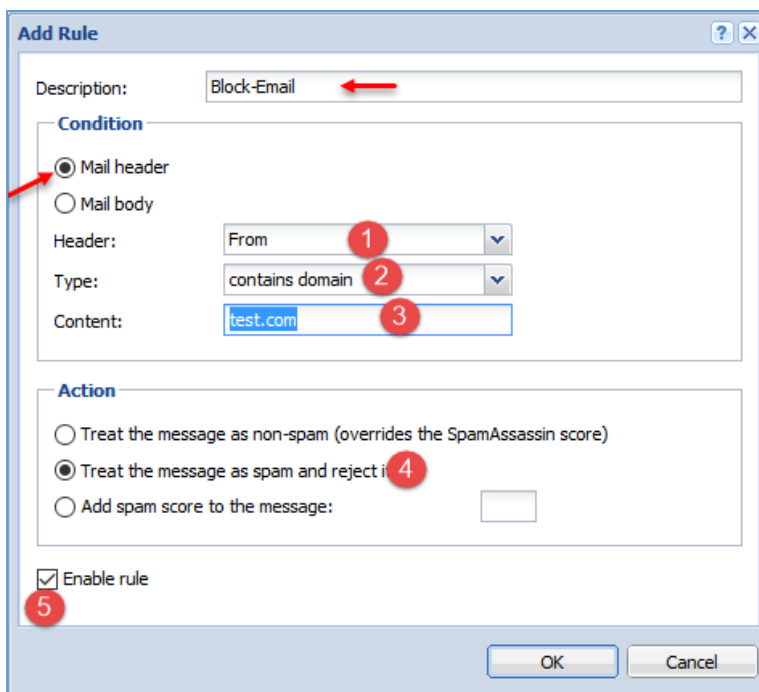
در قسمت Custom whitelist of ip addresses می‌توانید گروه‌هایی از آدرس‌ها را معرفی کنید که در لیست سفید قرار بگیرند و هیچ‌وقت پیام‌های آن‌ها فیلتر نشود، مانند آدرس شبکه‌ی داخلی.

در قسمت Custom Blacklist of spammer IP address می‌توانید همان گروهی را که در قسمت قبل ایجاد کردید را در این قسمت و در لیست کشویی روبرو انتخاب کنید که در شکل بالا این اقدام را مشاهده می‌کنید، برای فعال کردن باید گزینه‌ی Use IP address group را انتخاب و در لیست کشویی روبرو، گروه مورد نظر خود را انتخاب کنید؛ بعد از انتخاب، دو گزینه را در زیر آن مشاهده می‌کنید که اگر گزینه‌ی Block the message را انتخاب کنید، تمام ایمیل‌هایی که از این آدرس‌ها به سرور شما ارسال می‌شود، مسدود خواهند شد و یا اگر گزینه‌ی دوم، یعنی Add spam score to the message را انتخاب کنید، می‌توانید به سرور اعلام کنید که اگر شماره‌ی Spam پیام مورد نظر که در درس‌های قبل خواندیم از این عدد بیشتر شود، آن پیام فیلتر شود، در قسمت پایان نیز می‌توانید یک‌سری سرورهای را مشاهده کنید که آدرس‌های فیلتر در آن قرار دارد.



در تب Custom Rules می‌توانید یک‌سری قوانین ایجاد کنید، مثلاً اگر فرستنده-ی ایمیل، X بود، این ایمیل فیلتر شود.

برای انجام این کار به‌مانند شکل روبرو بر روی Add کلیک کنید.



در این صفحه، یک نام برای این Rule خود وارد کنید، بعد دو گزینه وجود دارد، یکی برای عنوان ایمیل (Mail header) و دیگری برای متن ایمیل (Mail body) است که در این قسمت باید گزینه‌ی اول را انتخاب کنید و در قسمت شماره‌ی یک، From را انتخاب کنید و در قسمت شماره‌ی دو برای اینکه بتوانید ایمیل‌های ارسالی از یک دومین خاص را فیلتر کنید باید گزینه‌ی contains domain را انتخاب و در قسمت شماره‌ی سه آدرس دومین را وارد کنید.

در قسمت شماره‌ی چهار با انتخاب گزینه‌ی مورد نظر، پیام مورد نظر Spam و Reject خواهد شد و در آخر، یعنی شماره‌ی ۵ با انتخاب این گزینه، این Rule فعال خواهد شد و تمام پیام‌هایی که از دومین test.com ارسال می‌شود، فیلتر خواهد شد؛ شما می‌توانید گزینه‌های دیگری را نیز برای فیلترکردن پیام، انتخاب و استفاده کنید.

محدود کردن فایل‌های پیوستی ایمیل:

The screenshot shows the 'Attachment Filter' configuration page in Kerio Control 2016. The left sidebar has 'Attachment Filter' selected. The main panel shows the following configuration:

- Enable attachment filter
- Filter options**
 - Send the sender a warning informing that the attachment was not delivered
 - Forward the original message to: administrator@3isco.local
 - Forward the filtered message to: administrator@3isco.local
 - Discard zip archive containing files with dangerous extensions (e.g. executable files).
 - The blocked attachment will be removed and the message will be delivered to the recipient.
- Filter rules**

Type	Content	Action	Description
<input type="checkbox"/>	File name *.exe	Block	Executable File
<input checked="" type="checkbox"/>	File name *.com	Block	DOS Executable
<input checked="" type="checkbox"/>	File name *.scr	Block	Microsoft Windows Screen Saver
<input checked="" type="checkbox"/>	File name *.bat	Block	Batch Processing
<input checked="" type="checkbox"/>	File name *.vbs	Block	Visual Basic scripts
<input checked="" type="checkbox"/>	File name *.{**}	Block	CLSID extension vulnerability

برای اینکه بتوانید نوع فایل‌های پیوستی را در ایمیل‌های ارسالی مدیریت کنید، می‌توانید به‌مانند شکل بالا وارد سرویس **Attachment Filter** شوید و تیک گزینه **Enable attachment filter** را انتخاب کنید؛ با این کار، تمام ایمیل‌ها از نظر نوع فایل پیوستی بررسی خواهد شد، اگر به‌مانند شکل بالا در قسمت **Filter Rules**، یکی از پسوندها به‌عنوان پیوست انتخاب شود، کاربر مورد نظر با خطا مواجه خواهد شد.

The screenshot shows the 'Add Filter Rule' dialog box. The configuration is as follows:

- Description:** Allow
- Condition:** If a message contains an attachment where: File name is *.bin
- Action:**
 - Block the attachment
 - Accept the attachment
 - Enable filter rule

برای اینکه به پسوند فایل، دسترسی لازم را بدهید یا ندهید، می‌توانید به‌مانند شکل روبرو بر روی **Add** کلیک کنید و در قسمت **Condition**، نوع فایل پیوستی را انتخاب کنید و در قسمت **Action** می‌توانید به فایل مورد نظر اجازه دهید یا ندهید.

تماس با ما:

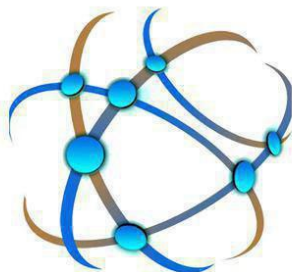
Farshid_babajani@live.com

Farshid_babajani@yahoo.com

<http://3isco.ir>

کانال آموزشی شبکه

3isco.ir



دریافت آخرین خبرها
و آموزش‌های شبکه

آدرس کانال :

<https://telegram.me/ciscopress>

آدرس گروه آموزش شبکه :

https://t.me/joinchat/BkXe4z8z-z2iSC8H_J-UUQ

زندگی پایان رویاها نیست، حتی پایان غم‌ها هم نیست، زندگی در تب و تاب و در برگریز ثانیه‌هایی گرفتار است که قدرش را ندانیم و من در امتداد تمام بودن‌های ناپایدار دانستم که پژواک پرواز قاصدک‌های عشق هنوز هم پابرجاست (آزاده تیشه برسر).

به پایان آمدیم دفتر، حکایت همچنان باقیست...