Kaspersky Administration Kit 8.0

GETTING STARTED

APPLICATION VERSION: 8.0 CRITICAL FIX 2

KASPERSKY

ترجمه : مهندس مصطفی شمیزی

منبع: kasp8.0_adminkitgsen محصول شرکت کاسپراسکای

کاربر گرامی!

انتشار مجدد این متن و یا هرگونه ترجمه، با ذکر Kaspersky Lab ZAO مجاز می باشد.

این متن و تصاویر مندرج در آن می توانند برای موارد آموزشی بکار گرفته شوند، ولی استفاده تجاری و شخصی از آنها مجاز نمی باشد.

این متن ممکن است برخی نکات موجود در ورژنهای جدید را شامل نباشد. جهت دسترسی به آخرین متن منتشر شده، میتوانید به آدرس http://www/kaspersky.com/docs مراجعه نمایید.

Document revision date: 10/14/2010

فهرست:

درباره این راهنما:

این راهنما توضیحات و مراحل اساسی که می بایست مدیر امنیتی و آنتی ویروس یک شبکه در مورد Administration KIT کاسپرسکای بداند، در اختیار می گذارد، و نیز چگونگی نصب آنتی ویروس از طریق شبکه بر روی کلاینتها را توضیح می دهد.

این متن جزییات مراحل نصب را شرح می دهد، در شرایطی که می توان بر روی چندین کامپیوتر در شبکه که سیستم عامل مایکروسافت ویندوز بر روی آنها نصب می باشد بدون رعایت سلسه مراتب مدیریتی سرورها آنتی ویروس را نصب کرد.

سناریوی نحوه نصب آنتی ویروس از طریق شبکه برروی کلاینتها در یک شبکه کامپیوتری با سایز متوسط در شرایط زیر شرح داده می شود:

- کامپیوترهایی که سیستم عامل متناسب با سخت افزار برروی آنها نصب گردیده اند.
- برخی از کامپیوتر ها جزو Domain می باشند و برخی در Work Group ها
- شبکه دارای DC می باشد.
- DNS مبتنی بر NetBIOS موجود می باشد.

این راهنما همچنین نحوه ارتقا از ورژن 6.0 به 8.0 را شرح می دهد.

محتویات متن

فصلهای زیر در این متن گنجانده شده اند:

- سایر منابع اطلاعاتی.

این فصل درباره اینکه چطور اطلاعاتی درباره قسمتهایی از نرم افزار که توسط مستندات هر بخش در اختیار گذاشته می شود را بدست آوریم در اختیار می گذارد.

- Administration KIT.

این فصل درباره Administration KIT و اجزا و بخشهای مختلف آن توضیح خواهد داد.

- رابط نرم افزاری

این فصل در خصوص چگونگی کار با Administration KIT و نکات لازم در خصوص آن را شرح می دهد.

- اجرا و توقف نرم افزار

این فصل در خصوص اجرا و شروع Administration KIT شرح می دهد.

- راه اندازی

این فصل در مورد نحوه اجرای آنتی ویروس و راه اندازی کامل Administration KIT در شبکه راه توضیح خواهد داد.

- ارتقا از ورژن 6 به ورژن 8

این فصل نحوه این ارتقا و بروز آوری را شرح می دهد.

- نتیجه گیری

این فصل کلیه مطالب این متن را جمع بندی نموده و ارایه می دهد.

نکات قراردادی در این متن

نکات قراردادی زیر جهت بکار گیری راحت تر این متن بیان می گردد.

متن نمونه	توضیحات
لطفا دقت نمایید که	هشدارها به رنگ قرمز و داخل کادر در متن آورده شده اند. هشدارها شامل نکات و اطلاعات مهمی می باشند، بعنوان مثال، در مورد خطاهای حاد کامپیوترها
توصیه می شود که	نکاتی که در داخل کادر آمده اند. این نکات شامل منابع و اطلاعات اضفی در خصوص یک مطلب می باشند.
مثال :.....	مثال های هر فصل با پس زمینه زرد رنگ و با تیتر "مثال" ارائه گردیده اند.
بروز رسانی بمعنی....	اصطلاحات جدید با خطوط مورب نمایش داده می شوند.
ALT + F4	نام کلیدهای صفحه کلید که با حروف بزرگ و پررنگ نمایش داده شده اند. و ترکیب آنها جهت یک عملکرد بکار گرفته می شوند.
فعال سازی	عناوین عناصر رابط کابری، بعنوان مثال، فیلدهای ورود، منو فرامین، کلیدها، وماننند آنها با حروف پررنگ نمای داده شده اند.
1. برای تنظیم زمان عملکردهای اتوماتیک	ابتدا و شورع عبارتها با حروب مورب نشان داده شده اند.
راهنمایی	متن سطر فرمان یا متن های پیام با قلم خاصی نمایش داده خواهند شد.
<آدرس IP کامپیوتر شما>	متغییرها داخل علامت <...> قرار میگیرند. در مقابل متغیرهای با مقادیر صحیح و مشخص فاقد علامتهای فوق خواهد بود.

سایر منابع اطلاعاتی

اگر سوالاتی در مورد نحوه خرید، نحوه نصب یا کاربری Administration KIT دارید پاسخها به ارحتی در دسترس میباشند.

تولیدکنندگان نرم افزار کاسپرسکای منابع اطلاعاتی مختلفی در اختیار کاربران قرار داده اند. شما می توانید مفید ترین آنها را نسبت به اهمیت و ضرورت سوالی که دارید برای خود انتخاب نمایید.

محتویات این فصل

منابع اطلاعاتی برای پیشبرد فعالیتهای تحقیقاتی

تالار گفتگو در وب سایت کاسپرسکای

بخش ارتباط با مشتریان

منابع اطلاعاتی برای پیشبرد فعالیتهای تحقیقاتی

شما می توانید به منابع اطلاعاتی در مورد نرم افزار دسترسی داشته باشید:

- صفحه نرم افزار در وب سایت کاسپرسکای
- صفحه دانش پایه ای نرم افزار در بخش سرویس پشتیبانی فنی وب سایت کاسپرسکای
- سیستم پشتیبانی آنلاین
- مستندات

صفحه نرم افزار در وب سایت کاسپرسکای

http://www.kaspersky.com/administration_kit

این صفحه جهت ارایه اطلاعات عمومی در مورد نرم افزار و نکات مهم به کاربران طراحی گردیده است.

صفحه دانش پایه ای نرم افزار در بخش سرویس پشتیبانی فنی وب سایت کاسپرسکای

http://support.kaspersky.com/remote_adm

این صفحه حاوی مقالات منتشر شده توسط سرویس پشتیبانی فنی نرم افزار می باشد.

این مقالات شامل اطلاعات مفید، توصیه ها، سوالات متداول مطرح شده، نحوه خرید، نص و استفاده از Administration KIT می باشند. مقالات بر حسب موضوع آنها مرتب گردیده اند، بعنوان مثال " کار با فایلهای کلیدی" ، " بروزرسانی بانک اطلاعاتی" و "ایرادیابی". مقالات نه تنها پاسخهایی در مورد Administration KIT بلکه در مورد سایر محصولات کاسپر نیز در اختیار قرار می دهند. و ممکن است اخباری در مورد سرویس پشتیبانی فنی نرم افزار نیز داشته باشند.

سیستم پشتیبانی آنلاین

بسته نرم افزاری فایل های راهنمای کاملی را شامل می شود، که توضیحات دقیقی از قابلیتهای نرم افزار را شرح می دهد.

برای باز کردن این فایلها، از داخل کنسول برنامه و قسمت Help گزینه Kaspersky Administrator Kit help system را انتخاب نمایید.

اگر سوالی در مورد اختصاصی سازی پنجره نرم افزار داشته باشید، می توانید از این راهنما استفاده نمایید.

مستندات

مستند سازی با هدف در اختیار گذاشتن کلیه اطلاعات مربوط به نرم افزار که مورد نیاز کاربران می باشد، انجام گرفته است.

- **راهنمای مسئول شبکه** اطلاعات پایه ای، قابلیتها و شمای عمومی استفاده از نرم افزار Administration KIT را در اختیار می دهد.
- **راهنمای تکمیلی** حاوی توضیحاتی در خصوص پروسه نصب اجزای مورد نیاز برای Administration KIT جهت نصب ریموت نرم افزار از طریق شبکه و با انجام تنظیمات ساده و آسان می باشد.
- **شروع** مراحل قدم به قدم آموزش به مدیران امنیتی شبکه جهت کاربری سریع و آسان از نرم افزار Administration KIT و نحوه نصب آنتی ویروس برروی کلاینتهای موجود در شبکه را توضیح می دهد.
- **راهنمای مرجع** حاوی توضیحات تکمیلی از نرم افزار و نیز راهنمایی های جزیی لازم در خصوص قابلیتهای آن می باشد.

این راهنمایی ها با فرمت PDF در بسته نصب نرم افزار موجود می باشند.

همچنین از طریق وب سایت Kaspersky و صفحه مربوط به نرم افزارها قابل دسترس می باشند.

اطلاعات در خصوص رابط نرم افزاری (API) مربوط به Administration KIT با فرمت فایلهای CHM در دسترس می باشند. این فایلها نیز درداخل پوشه مربوط به نصب نرم افزار موجود می باشند.

KASPERSKY ADMINSTRATION KIT

این نرم افزار بصورت رایگان در آدرس وب سایت http://www.kaspersky.com جهت داونلود موجود است.

KASPERSKY ADMINSTRATION KIT کنسول مدیریتی جامعی برای سیستم امنیت ضد ویروس شبکه می باشد و با استفاده از پروتکل TCP/IP تمامی تنظیمات تحت شبکه ای را انجام می دهد.

این نرم افزار ابزاری است در دست مدیران و مسئولین امنیت شبکه های کامپیوتری.

با استفاده از این کنسول مدیر شبکه می تواند:

- گروههای مدیریت شده ای را ایجاد نماید و از طریق آن یک کامپیوتر محلی را مدیریت نماید.
- از طریق ریموت، نرم افزار ضد ویروس را بر روی کلاینتها نصب یا حذف نماید.
- از روی یک کامپیوتر به طور متمرکز کلیه کامپیوترهایی که آنتی ویوس بر روی آنها نصب گردیده را مدیریت نماید.
- بسته های بروز رسانی را دریافت و از طریق آن برروی کلیه کلاینتها نصب نمود.
- پیامهای خطای ایجاد شده توسط نرم افزار ضد ویروس در کلاینتها را دریافت و بررسی نماید.
- اطلاعات و گزراشات مربوط به نرم افزار ضد ویروس را دریافت و تحلیل نماید.
- مجوز نرم افزار را برروی تمامی کلاینتها مدیریت نماید.
- به طور متمرکز موارد بلوک شده و فایلهای پشتیبان گرفته شده توسط آنتی ویروس، و نیز مواردی که جهت پاکسازی و حذف ویروسهای موجود نگهداری شده اند را مدیریت کند.
- و بطور متمرکز هر نرم افزار ثالثی که از طریق شبکه نصب گردیده را مدیریت کند.

Administration Kit متشکل از سه عنصر (جز) اصلی می باشد:

- Administration Server : متمرکز سازی ذخیره اطلاعات مربوط به نرم افزار کاسپراسکای نصب شده در شبکه و نحوه مدیریت آنها را عهده دار است.
- Network Agent : یکسان سازی و ایجاد تعامل بین Administration server و نرم افزارهای کاسپراسکای نصب شده برروی سایر کامپیوتر ها (اعم از سرور یا کلاینت ها) را عهده دار می باشد.
- Administration Console : یک رابط کاربری برای سرویس های مدیریتی Administration Server و Network Agent را فراهم می نماید. کنسول مدیریتی مشابه ساختار کنسول مدیریتی مایکروسافت (MMC) طراحی گردیده است.

رابط گرافیکی نرم افزار:

مشاهده، ایجاد، تغییر و تنظیمات مربوط به گروههای مدیریتی به طور متمرکز و از طریق یک کامپیوتر به آسانی امکان پذیر خواهد بود.رابط کاربری مدیریتی توسط جزء کنسول مدیریتی امکان پذیر می باشد. و آن نیز شکل خیلی اختصاصی یافته از کنسول مدیریتی مایکروسافت (MMC) می باشد، بنابر این Administration Kit ساختار استانداردی از رابط گرافیکی MMC می باشد.

پنجره اصلی نرم افزار حاوی منو، نوار ابزار، پنل مرورگر و یک ناحیه مشاهده اطلاعات می باشد.

منوی این پنجره کلیدهای کنترلی برای مدیریت پنجره و نیز راهنما را در اختیار می گذارد. زیر منوی Action حاوی فرامینی برای مدیریت اجزاء درختی کنسول در دسترس قرار میدهد.

تنظیم نوار ابزار این اجازه را به شما خواهد داد که براحتی به تعدادی از آیتم های نوار منو دسترسی داشته باشید. آیتم های موجود در نوار ابزار بسته به اینکه بر روی کدام کلید یا پوشه ای از درخت کنسول کلیک کرده باشید فعال خواهند شد.

پنل انجام عملیات حاوی یک یا چند بخش می باشد که هر یک شامل چند کلید اجرایی برای دسترسی آسان و سریع به دستورات پایه برای آیتم انتخاب شده از درخت کنسولی می باشند.

پنل مشاهده نتایج دستورات درحال اجرا، لیستی از آیتمهایی که مربوط به جز انتخاب شده از درخت کنسول می باشند را نمایش می دهد. مثلا لیستی از کامپیوترهای یک گروه، لیستی از گزراشات و یا کامپیوترهای انتخاب شده را خواهید دید.

اجرا و یا توقف عملکرد نرم افزار

Administration Kit بطور اتوماتیک با راه اندازی Administration Server اجرا خواهد شد.

Administration Kit را می توانید از مسیر Start و سپس Programs و از داخل پوشه مربوط به نرم افزار کاسپراسکای اجرا نمایید.

شروع کار

برای دستیابی به مفهوم واقعی جلوگیری از نفوذ ویروسها در شبکه کامپیوتری می بایست :

بسته مربوط به آنتی ویروس را بر روی تمامی کامپیوترهای موجود در شبکه نصب نمایید.(بخش ایجاد بسته ضد ویروس)

ایجاد یک سری دستورات اتوماتیک روزمره (بخش دستورات روزمره) که توسط آنها می توانید از وضعیت موجود امنیت ضد ویروسی شبکه را تحت کنترل داده باشید.

ایجاد یکسری دستورات اتوماتیک زمانبندی شده (بخش دستورات اتوماتیک زمانبندی شده)، برای انجام بروز رسانی بانک اطلاعاتی و هر عمل دیگری که می خواهیم در زمان مشخصی اعمال گردد از این قابلیت استفاده می نماییم.

عناوین اصلی این فصل به شرح زیر می باشد:

- نصب آنتی ویروس
- دستورات اتوماتیک روزمره
- دستورات اتوماتیک زمانبندی شده

نصب آنتی ویروس

2. جهت نصب آنتی ویروس از طریق شبکه:

1- Administration Server و Administration Console را نصب نمایید. (بخش نصب اجزاء Administration Kit)

2- تنظیمات پیش فرض را تغییر داده و ویزارد آسان نصب آنتی ویروس را شروع نمایید. (بخش تنظیمات اولیه آنتی ویروس)

3- یک گروه در زیر مجموعه کامپیوترهای مدیریت شده ایجاد نمایید. (بخش ایجاد گروه در مجموعه کامپیوترهای مدیریت شده) و کامپیوتر کلاینتها را به آن گروه اضافه نمایید. گروه مدیریت شده این قابلیت را دارد که تمامی کامپیوترهای اضافه شده در آن را توسط دستورات اتوماتیک و Policyها به صورت واحد و یکپارچه مدیریت نماید.

4- بطور ریموت آنتی ویروس را برروی کامپیوتر ها انتخاب شده نصب نمایید. (بخش نصب ریموت آنتی ویروس). در این مرحله باید از صحت نصب آنتی ویروس بر روی کامپیوتر کلاینتها، اطمینان حاصل نمایید.

5- مطمئن شوید آنتی ویروس بطور کامل و صحیح بروزرسانی شده است. (بخش تشخیص بروز رسانی شدن بانک اطلاعاتی).

6- تنظیمات مربوط به اتفاقات صورت پذیرفته در مورد آنتی ویروس کاسپراسکای بر روی کامپیوتر کلاینتها را انجام دهید. (بخش تنظیمات مربوط به یادآورها)

7- بطور دستی دستور اسکن آنتی ویروس را اجار کنید و از عملکرد صحیح ثبت اتفاقات و یادآورها بر روی کامپیوتر کلاینتها مطمئن شوید. (بخش تشخیص عملکرد صحیح ثبت وقایع و یادآورها در هنگام اجرای دستور اسکن آنتی ویروس)

8- گزارشات و تنظیمات مربوط به ارسال گزارشات ضروری از طریق ایمیل را انجام دهید. (بخش دریافت گزارشات)

9- تنظیمات مربوط به نصب اتوماتیک آنتی ویروس بر روی کامپیوترهای تازه اضافه شده به شبکه کامپیوتری را انجام دهید.(بخش تنظیمات مربوط به نصب اتوماتیک نرم افزار)

هنگامیکه این عملیات را به اتمام رساندید، میتوانید نصب آنتی ویروس بر روی کامپیوترهای موجود در شبکه را آغار نمایید.

در این بخش:

- نصب اجزاء مربوط به Administration Kit
- تنظیمات اولیه مربوط به آنتی ویروس
- ایجاد گروه در مجموعه کامپیوترهای مدیریت شده
- نصب ریموت آنتی ویروس
- تشخیص بروز رسانی شدن بانک اطلاعاتی
- تنظیمات مربوط به یادآورها
- تشخیص عملکرد صحیح ثبت وقایع و یادآورها در هنگام اجرای دستور اسکن آنتی ویروس
- دریافت گزارشات
- تنظیمات مربوط به نصب اتوماتیک نرم افزار

نصب اجزاء مربوط به Administration Kit

3. جهت نصب Administration Server و Administration Console بروش زیرعمل نمایید:

1- یک کامپیوتری را جهت نصب اجزاء مربوط به نرم افزار را انتخاب نمایید. توصیه میشود این کامپیوتر Join شده بر روی Domain شما باشد.

می توانید Administration Server و Administration Console ورژن 8.0 را نیز برروی کامپیوتری که همان اجزاء فوق با ورژن 6.0 نصب شده اند بطور همزمان نصب و در اختیار داشته باشید.

توصیه می کنم با استفاده از یک نام کاربری که بعوان Admin شبکه دسترسی دارد این نرم افزار را نصب نمایید. این کار باعث میشود گروههای کاربری KLAdmins و KLOprators بطور اتوماتیک ایجاد شوند، و دسترسی های اولیه لازم برای کاربر Admin اعمال می شود.

2- با اجرای فایل Setup.exe وارد ویزارد نصب برنامه خواهید شد.

3- حالت نرمال و استاندارد نصب را انتخاب نمایید.

با انتخاب حالت نصب ویژه وارد مراحلی خواهید شد که توضیحات دقیق و جزیی مربوط به آنها در راهنمای تکمیلی Administration Kit آورده شده است.

نرم افزار نیاز به نصب برنامه هایی دارد که اگر برروی سیستم شما نصب نگردیده باشد، قبل شروع نصب اصلی ابتدا آنها را بر روی سیستم نصب خواهد نمود، و این برنامه ها عبارتند از:

- Microsoft Windows Installer 3.1

- Microsoft Data Access Components (MDAC) 2.8
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2005 Express Edition

این نرم افزار های جانبی نیازی به نگهداری و مدیریت خاصی نخواهند داشت.

در مرحله بعدی از ویزارد نصب نرم افزار، فایلهای نرم افزار بر روی کامپیوتر شما کپی خواهند شد و بانک اطلاعاتی مربوطه به آنتی ویروس و امنیت کامپیوترهای تحت شبکه نیز بر روی کامپیوتری که بعنوان سرور انتخاب کرده اید ایجاد و ذخیره خواهد شد.

پس از اتمام ویزار نصب می توانید کنسول مدیریتی نرم افزار را اجرا نمایید و تنظیمات اولیه مربوطه را انجام دهید (بخش تنظیمات اولیه مربوط به آنتی ویروس)

همچنین میتوانید کنسول مدیریتی را بر روی یک کامپیوتر دیگر نصب نمایید و سرور مدیریتی خود را از طریق شبکه کنترل کنید. جهت انجام این کار گزینه نصب ویژه را انتخاب نموده و در پنجره انتخاب اجزاء نصب، فقط گزینه Administration Console را انتخاب نمایید.

پس از نصب کنسول مدیریتی، می بایست با اجرا آن به سرور مدیریتی متصل شوید. در این پنجره باز شده از نرم افزار، می بایست نام کامپیوتری که Administration Server بر روی آن نصب گردیده را وارد نموده و نیز اطلاعات و تنظیمات مربوط به اتصال سرورمکور از قبیل نام کاربری و کلمه عبور را وارد نمایید. پس از اتصال به سرور می تونید مدیریت های لازم مربوط به آنتی ویروس را اعمال نمایید.

تنظیمات اولیه مربوط به آنتی ویروس

آماده سازی های اولیه مربوط به آنتی ویروس توسط یک ویزارد و هنگامی که برای اولین بار کنسول مدیریتی را اجرا می نمایید، انجام می پذیرد.

4. برای انجام این تنظیمات شرکت یک ویزارد آسان به روال زیر در اختیارتان قرارداد است:

1. اختصاص کد فعال سازی نرم افزار که توسط Administration Kit دریافت و این کد بطور اتوماتیک برای هر کامپیوتری که بتازگی به گروه کامپیوتر مدیریت شده اضافه میگردد، اختصاص خواهد یافت. می توانید بدون وارد نمودن کد فعال سازی از این مرحله عبور نمایید و در فرصت دیگری این کد را وارد نمایید.

2. تا زمانی Administration Server اطلاعات مربوط به شبکه تان کنترل می نماید و کامپیوترهای موجود در شبکه را به فهرست خود اضافه می نماید منتظر بمانید.

3. تنظیمات مربوط به یادآورهای لازم جهت ارسال آنها از طریق ایمیل را انجام دهید، که اطلاعاتی را در مورد وضعیت موجود و عملکرد آنتی ویروس و کامپیوترهای شبکه را در اخیار قرار میدهد. این تعاریف را نیز بعدا از قسمت تنظیمات Administration Server می توانید انجام دهید.(جهت کسب اطلاعات بیشتر به راهنمای مرجع مراجعه نمایید)

4. در این مرحله نسبت به تتعریف Policyها و دستورات اتوماتیک اقدام نمایید. این تعاریف و دستورات جهت عملکرد صحیح آنتی ویروس و Protectionها در شبکه شما بسیار لازم و ضروری می باشند. Policyهای Administration Kit برای تعاریف عمومی و کلی در مورد نحوه عملکرد نرم افزار، و دستورات (Task) به منظور عملکرد صحیح آن بکار میروند.

اجزا زیر در کنسول ایجاد خواهند گردید:

- Policyهای اصلی نرم افزار (شامل Policyهای مربوط به آنتی ویروس نصب شده بر روی ویندوزهای کلاینتها و ویندوزهای سرور) که حاوی تنظیمات پیش فرض می باشند. می توانید این Policyها را بعدا مشاهده و ویرایش نمایید. به منظور جلوگیری از دستکاری و تغییر این تنظیمات توسط کاربران عادی از علامت در قسمتهای مختلف این Policyها استفاده نمایید.

- دستورات اتوماتیک اصلی برای بروزآوری بانک اطلاعاتی مربوط به آنتی ویروس بر روی کامپیوتر کلاینتها (دستورات اتوماتیک مربوط به آنتی ویروس نصب شده بر روی ویندوزهای کلاینتها و ویندوزهای سرور) که حاوی تنظیمات پیش فرض می باشند. این دستورات بمنظور دریافت (داونلود) بسته های بروز رسانی از Administration Server و نصب بر روی کلاینتها تنظیم می شوند.

برای کسب اطلاعات بیشتر در مورد سایر روش های بروزرسانی، به آدرس وب سایت کاسپراسکای مراجعه نمایید.

(http://www.kaspersky.com/avupdates)

- دستورات مربوط به اسکن کامپیوترها با تنظیمات پیش فرض (دستورات اتوماتیک مربوط به آنتی ویروس نصب شده بر روی ویندوزهای کلاینتها و ویندوزهای سرور).

- یک دستور اتوماتیک برای داونلود بسته بروز رسانی Administration Server از اینترنت با تنظیمات پیش فرض.

این دستور بسته های لازم برای بروزرسانی بانک اطلاعاتی نرم افزار و ماجول های نرم افزاری را از سرور سایت کاسپراسکای داونلود کرده و در داخل پوشه های به اشتراک گذارده شده که در هنگام نصب کاسپراسکای معین شده اند، بارگذاری می شوند. کامپیوترهای کلاینتها می توانند این بسته ها را ا داخل پوشه های به اشتارک گذارده شده در Administration Server دریافت و بانک اطلاعاتی آنتی ویروس را بروز رسانی نمایند. در ادامه مطالب شما با نحوه تنظیمات دقیق تر پروسه بروزرسانی آنتی ویروس برای سرورهای زیر مجموعه سرور اصلی و استفاده از رابط بروزرسانی آشنا خواهید شد.

- دستور اتوماتیک تهیه فایل پشتیبان از بانک اطلاعاتی Administration Server با تنظیمات پیش فرض. این دستور یک نسخه از اطلاعات موجود در سرور را بعنوان پشتیبان گیری ذخیره می نماید، که شامل بانک اطلاعاتی، ساختار گروای مدیریت شده، بسته های قابل نصب دردسترس و مستندات و مجوزهای مربوط به سرور اصلی می باشد.

- دستور اتوماتیک گزارشات مستمر سرور اصلی. بصورت پیش فرض، سرور اصلی گزارش روزانه ای را در مورد سطح امنیتی آنتی ویروس از طریق ارسال ایمیلی که دز هنگام اجرای ویزارد ابتدایی تعیین کرده اید ارسال می نماید.

پس از ایجاد این Policyها و دستورات اتوماتیک، سرور اصلی شروع به دانلود بسته های بروز رسانی و ذخیره آنها خواهد نمود. در این حالت می توانید بدون اینکه منتظر باتمام رسیدن بروزرسانی باشید به مرحله بعدی ویزارد بروید.

اطلاعات مربوط به بسته های بروزرسانی و محل ذخیره آنها در پوشه های باشتراک گذارده شده در شاخه اصلی کنسول و در قسمت Updates از بخش Repositories قابل مشاهده می باشند.

5. در نهایت پنجره ای ظاهر خواهد گردید مبنی بر اینکه آیا مایل به ایجاد بسته قابل نصب آنتی ویروس برای کلاینتها می باشید یا نه؟ (بخش نصب ریموت آنتی ویروس)

ایجاد یک گروه مدیریت شده

برای اضافه نمودن یک گروه جدید به روش زیر عمل نمایید:

1- در درخت کنسول، گروهی را که می خواهید در آن گروه جدیدی را ایجاد نمایید انتخاب کنید.

2- در پنل عملیاتی از بخش Groups بر روی قسمت Create a subgroup کلیک نمایید.

3- در پنجره باز شده، نام گروه را وارد نموده و کلید OK را کلیک نمایید.

پس از آن، کنسول مدیریتی پوشه را در داخل گروه انتخاب شده ایجاد می کند.

4- کامپیوترهای مورد نظر را از داخل پوشه Unassigned computers به داخل پوشه گروه مدیریت شده ای که ایجاد نموده اید انتقال دهید. برای این کار از پنل عملیاتی بر روی لینک Add computers to the group کلیک نموده و ویزارد باز شده را دنبال کنید.

کامپیوترهای اضافه گردیده، در پنل نتایج پوشه Client computers قابل مشاهده خواهند بود.

برای اعمال تنظیمات مربوط به کامپیوترهای انتقال داده شده به گروه مدیریت شده، (با هر گونه تنظیمات ایجاد شده برای آن گروه) از منو پوشه Unassigned computers را باز نموده و گزینه Search را انتخاب نمایید. وقتی که کامپیوتر مورد نظر را پیدا کردید، با کلیک راست نمودن گزینه Move to Group را انتخاب نمایید. برای کسب اطلاعات بیشتر، راهنمای پیشرفته Administration Kit را مطالعه نمایید.

نصب Remote نرم افزار ضد ویروس

این بخش نحوه نصب آنتی ویروس بر روی کلاینتها را از طریق Remote شرح می دهد. این روش مشابه روش نصب سایر نرم افزارهای ضد ویروس مجموعه کاسپراسکای می باشد.

برخی از نرم افزارهای مجموعه کاسپراسکای می توانند از طریق Administration Kit مدیریت شوند، اما فقط می توانند به شکل لوکال بر روی سیستم ها نصب شوند. (برای کسب اطلاعات اضافی، لطفا به راهنمای نرم افزارهای مشابه مراجعه نمایید.)

5. برای نصب آنتی ویروس بروش Remote به ترتیب زیر عمل نمایید:

1- در درخت کنسولی، نود Administration Server را انتخاب نمایید.

2- در بخش Deployment پنل عملیاتی، بر روی لینک Install Kaspersky Anti-virus کلیک نموده تا ویزارد نصب آنتی ویروس اجرا گردد.

3- در ویزارد باز شده، پکیج مربوط به نصب آنتی ویروس کاسپر اسکای برای کامپیوتر کلاینت ها را انتخاب نمایید. این پکیج به هنگام نصب Administration Serve ایجاد گردیده است، و حاوی تنظیمات پیش فرض مربوط به نرم افزار می باشد. Network Agent در هر حال همراه نرم افزار نصب می شود.

4- کامپیوترها و یا گروه مدیریت شده ای را که می خواهید نرم افزار بر روی آنها نصب شوند انتخاب نمایید.

5- نحوه اینکه چگونه پکیج مربوطه بر روی کامپیوتر هدف دانلود گردد را انتخاب کنید.

6- چنانچه هنگام ایجاد پکیج کلید (اعتبار) نرم افزار وارد ننموده اید مسیر فایل رجیستری (کلید) را مشخص نمایید.

7- مشخص کنید که آیا کامپیوتر بعد از نصب آنتی ویروس ری استارت خواهد شد یا نه.

8- اگر مجموعه ای از کامپیوترها را برای نصب آنتی ویروس انتخاب کرده باشید، مشخص نمایید که آیا مایل هستید آنها به داخل یک گروه مدییت شده انتقال یابند یا نه.

9- نصب Remote نرم افزار را آغاز نمایید.

هنگامی که دستور نصب Remote آنتی ویروس به اتمام رسید، آنتی ویروس کاسپراسکای به همراه Network Agent بر روی کامپیوتر مشخص شده نصب خواهد گردید.

نصب Remote می تواند بر روی کامپیوترهایی که آنتی ویروس کاسپراسکای 5.x و یا 6.x برروی آنها نصب می باشد صورت گیرد. در این حالت، آنتی ویروسهای کاسپراسکای 5.x و یا 6.x از سیستم حذف و بجای آن نسخه آنتی ویروس 6.0 MP4 نصب خواهد شد.

برای اطمینان از اینکه نصب انتی ویروس موفقیت آمیز بوده، یا پوشه Client computers مربوط به گروه مدیریت شده را انتخاب نمایید و یا از پوشه Unassigned computers بر روی محل که کامپیوتر مورد نظر در آن قرار داشت در پنل عملیاتی کلیک نمایید تا اطلاعات مربوط به را در ستون Agent/Anti-virus مشاهده نمایید. اگر این ستون حاوی دو علامت (+) باشد، هر دو نرم افزار بر روی سیستم نصب گردیده است. ستون Status نیز می بایست مقدار Running را نشان دهد.

تشخیص بروز بودن بانک اطلاعاتی

سیستم امنیت آنتی ویروس فقط هنگامی ملکرد صحیح خواهد داشت که آخرین ورژنهای مربوط به بروزرسانی ها نصب شده باشند. بنابر این، ضروریست که Task مربوط به دانلود بسته های بروزرسانی (downloading updates to the repositories) را کنترل نموده (پوشه باشتراک گذارده شده) و task مربوط به بروز رسانی کامپیوتر کلاینتها را نیز بررسی نمایید تا مطمئن شوید هر دوی آنها بدرستی عمل مینمایند.

برای تست بروز بودن بانک اطلاعاتی:

1- در کنسول مدیریتی، پوشه Kaspersky Administration Kit tasks را باز نموده، و Task مربوط به دانلود بسته های بروز رسانی را انتخاب نمایید.

2- بروی آن کلیک راست نموده و آیتم Propertiesرا کلیک نمایید.

3- بخش Updates verification را انتخاب نمایید.

4- گزینه Test updates before distributingرا فعال نمایید.

5- در فیلد Updates verification task ، یکی از Task های موجود را با استفاه از کلید Select انتخاب نمایید. می توانید یک دستورتشخیص بروزبودن جدید را نیز ایجاد نمایید. برای انجام این کار، بر روی کلید Create a task کلیک نموده و ویزارد باز شده را ادامه دهید. در طول ایجاد Updates verification task جدید، Administration server یک Policies آزمایشی ، و یک گروه بروزرسانی و اسکن زمانبندی شده ایجاد خواهد نمود.

توصیه می شود دستور تشخیص بروز بودن آنتی ویروس را در شبکه اجرا نمایید. این قابلیت باعث افزایش کیفیت اسکن، حداقل رسیدن ریسک ناشی از خطای فردی و احتمال یافتن ویروس در هنگام اسکن می شود. اگر ویروسی بر روی کامپیوترهای شاهد (کامپیوترهایی از شبکه که بطور تصادفی انتخاب شده و دستور فوق بر روی آنها اجرا میگردد) یافت شود معلوم می شود که بروزرسانی صورت نگرفته و مشکلی در این زمینه وجود دارد.

پس از اینکه تنظیمات مربوطه تنظیم گردید، دستور تشخیص بروز بودن قبل از اینکه بانک اطلاعاتی در شبکه و بر روی کلاینتها توزیع شود اجرا خواهد شد. Administration server بسته های بروز رسانی را دانلود کرده و در یک محل موقت ذخیره می کند، و سپس دستور تشخیص بروز بودن را اجرا می نماید. اگر این دستور با موفقیت اجرا شود، بسته های بروز رسانی موجود در محل نگهداری موقت به داخل پوشه باشتراک گذاری بر روی Administration server کپی می شوند و از این طریق بر روی کلیه کامپیوترهایی که Administration Server بعنوان منبع بروزرسانی آنها تعریف شده توزیع و نصب می شوند.

اگر در نتیجه دستور تشخیص بروز بودن بانک اطلاعاتی مشاهده شود که محل ذخیره موقت بسته های بروزرسانی صحیح نمی باشد و یا این دستور همراه با خطا به پایان برسد؛ مثلا بست های بروز رسانی به داخل پوشه باشتراک گذاشته شده کپی نگردید، Administration Server آخرین بروزرسانی که صحیح انجام شده را نگهداری میکند. در این حالت دستورهای اتوماتیکی که در بخش زمان بندی اجرایی آنها طوری تنظیم شده اند که وقتی اجرا شوند که بسته های بروزرسانی جدید دانلود شوند.

پیکربندی یادآورها (پیام های هشدار)

- برای پیکربندی یادآورهای اتفاقات رخ داده در عملکرد سیستم ضد ویروس

1- یک Policy برای نرم افزار ضد ویروس در زیرپوشه Policy در گروه مدیریتی (به عنوان مثال، آنتی ویروس برای ایستگاههای کاری ویندوز) را انتخاب کنید.

2- در پنجره سمت نتایج در بخش Action، روی لینک configure notifications برای رفتن به پیکربندی یادآورها در مورد رویدادها کلیک کنید.

3- برنامه های مورد نیاز و آگاه شدن از طریق روش های تحویل برای آنها مشخص است. برای این کار ، از کلیک بر روی دکمه خواص و بررسی جعبه در کنار روش های اطلاع رسانی مورد نیاز، در بخش اطلاع رسانی رویداد روشهای متفاوتی برای ارسال یاد آورها وجود دارد که عبارتند از :

ارسال یاد آور از طریق ایمیل

ارسال یاد آور از طریق شبکه و دستور (Net Send)

یادآوری با استفاده از فایل های قابل اجرا یا اسکریپت

ارسال یادآوری از طریق SNMP

برای بررسی نحوه توزیع یادآورها، کافی است به مجموعه اطلاع رسانی برای موارد آلوده شناسایی شده مراجعه شود (رجوع کنید به بخش " بررسی توزیع یادآورها و دستورات اسکن درخواست شده"

4- تنظیمات مربوط به یادآورها را تغییر دهید. برای انجام اینکار در قسمت Event Notification بر روی لینک Setting برای انجام تنظیمات لازم کلیک نمایید. بطور پیش فرض تنظیمات مربوط به سرور تنظیم شده است.

با استفاده از کلید Test می توانید یک پیام آزمایش را ارسال کنید. به هنگام کلیک بر روی این کلید، یک پنجره ارسال یادآور آزمایش باز می شود. در هنگام وقوع خطا، جزییات مربوط به آن نمایش داده می شود.

به محض انجام تنظیمات مربوط یادآورها و ذخیره سازی آنها در Policy بر روی کامپیوتر کلاینتهای موجود در گروه اعمال می شود.

بررسی نحوه توزیع یادآورها (پیام های هشدار) و دستورات درخواست شده اسکن کردن

- برای بررسی اینکه آیا یادآورهای مربوط به رخ دادها صحیح اعمال شده است یا نه، و اینکه آیا دستورات مربوط به اسکن به درستی و کامل اعمال میشوند:

1- سعی کنید یک فایل تست Eicar را بر روی کامپیوتری که آنتی ویروس بر روی آن نصب شده کپی نمایید. (تعریف: فایل تست Eicar فایلی است که عملکردی مشابه ویروس دارد ولی در اصل ویروس نیست). اگر آنتی ویروس به درستی عمل کند اجازه

کپی فایل را به شما نخواهد داد. هشداری مبنی بر تشخیص ویروس مشاهده خواهید نمود، و گزارشی مربوط به آن را در پوشه Events از درخت کنسول مدیریتی مشاهده خواهید نمود.

2- System real-time protection بر روری کامپیوتر کلاینت غیر فعال کنید و سپس فایل Eicar را بر روی کامپیوتر کپی نمایید. پس از آن دوباره System real-time protection فعال کنید.

3- دستور اسکن کامپیوتر کلاینت را اجرا نمایید. درهنگام اجرای دستور اسکن فایل مذکور شناسایی خواهد شد. پیامی نیز مبنی بر یافت شدن ویروس برای شما ارسال (ظاهر) می گردد و گزارشی مربوط به آن را در پوشه Events از درخت کنسول مدیریتی واقع در پوشه Event and computer selections --> Events --> Recent events مشاهده خواهید نمود.

فایل تستی ویروس **یک ویروس نیست** و حاوی کد مخربی که باعث آسیب به سیستم شود نمی باشد. البته بسیاری از شرکت های ارائه کننده آنتی ویروس این فایل را بعنوان ویروس شناسایی می کنند. این فایل تست ویروس را می توانید از سایت رسمی سازمان EICAR دانلود نمایید.

گزارشات دریافتی

بر اساس اطلاعات ذخیره شده درلوگ های Administration Kit از سرور مدیریتی، در پوشه Reports and notifications از درخت کنسولی، میتوانید گزارشات خلاصه شده ای از وضعیت آنتی ویروس را مشاهده نمایید. در قسمت Statistics اطلاعاتی در چندین صفحه نمایش داده می شود: Protection status, Deployment, Update, Anti-virus statistics و General information. هر صفحه شامل یک سری اطلاعات نموداری، گرافها یا متن های توضیحی می باشند. با استفاده از کلید می توانید تنظیمات مربوط به نحوه نمایش اطلاعات را تغییر دهید.

همچنین می توانید با استفاده از گزارش ساز می توانید گزراشاتی با جزییات بیشتری را ایجاد نمایید. برای انجام این کار در پوشه Reports and notifications به قسمت قالب گزارشات مورد نیاز بروید و یا از بخش Reports در نوار وظیفه ، با کلیک کردن بر روی نام گزارش مورد نیاز خروجی دلخواه را انتخاب نمایید.

چندین قالب استاندارد برای تهیه انواع گزارشات مد نظر در ارتباط با وضعیت عملکرد آنتی ویروس وجود دارد که عبارتند از:

- **Kaspersky Lab software version report**.
- **Viruses report**.
- **Most infected computers report**.
- **Incompatible applications report**.
- **Users of infected computers report**.
- **Protection coverage report**.
- **Report on application registry**.
- **Protection status report**.
- **License usage report**.
- **Anti-virus database usage report**.
- **Errors report**.

برای مثال : اگر گزارش در سطح فعالیت ویروس را ایجاد می کنید، اطلاعات مربوط به تمام ویروس های شناسایی شده توسط Administration Kit را مشاهده خواهید نمود.

تنظیمات مربوط به نصب اتوماتیک نرم افزار ها

- برای نصب اتوماتیک نرم افزارها بر روی کامپیوترهای جدیدی که به یک گروه مدیریتی اضافه می شوند به ترتیب زیر عمل نمایید:

1- پنجره مربوط به تنظیمات (Properties) مربوط به گروه مدیریتی مد نظر را انتخاب نمایید.

2- وارد قسمت Automatic installation شوید.

3- هر کدام از نرم افزارهایی را که مایل به نصب آن می باشد با علامت دار کردن باکس مربوط انتخاب نمایید و سپس گزینه OK را کلیک نمایید.

با این کار دستور گروهی برای اجرا در گروه مورد نظر ایجاد خواهد گردید و بلافاصله در کلیه کلاینتهایی که به گروه اضافه گردند اعمال خواهد شد.

دستورات روزانه

برای پیگیری از وضعیت آنتی ویروس، توصیه می شود نظارت بر داده های زیر را به صورت روزانه انجام دهید:

- وضعیت موجود از آنتی ویروس در شبکه کامپیوتری (مراجعه شود به بخش "مشاهده وضعیت موجود آنتی ویروس")
- گزارشات مربوط به ویروسهای پیدا شده در شبکه (مراجعه شود به بخش "مشاهده گزارشات مربوط به ویروسهای پیدا شده")
- اطلاعات مربوط به اتفاقات مهم در نحوه عملکرد آنتی ویروس (مراجعه شود به بخش "مشاهده اطلاعات مربوط به رخدادهای مهم")

در این بخش

مشاهده وضعیت موجود آنتی ویروس

می توان برای مشاهده وضعیت کلی آنتی ویروس از قسمت پنل وضعیتی Administration Server استفاده نمود. پنل های اطلاعاتی در این قسمت، اطلاعات عمومی و کلی درباره وضعیت انواع نرم افزارهایی که در بخشهای مختلف عملکرد دارند به نمایش می گذارند:

- گستره امنیت در کامپیوترهای تحت شبکه
- ساختار ایجاد شده برای گروههای مدیریتی که حاوی کامپیوترهای مدیریت شده می باشند.
- ساختارهای امنیتی اعمال شده بر روی کلاینتها
- اسکن کامپیوترهای کلاینتها
- بروزرسانی بانکهای اطلاعاتی نرم افزارها و ماجولهای آنها
- مونیتورینگ و عملکرد پیامها و یادآورها

با استفاده از آیکون های موجود در پنل های اطلاعاتی بآسانی می توانید وضعیت موجود آنتی ویروس را بررسی نمایید. اگر آیکون برنگ سبز باشد، تمام دستورات و عملکردهای مربوطه در این ناحیه عملیاتی باتمام رسیده اند. اگر آیکون برنگ زرد یا قرمز باشد، این ناحیه از منطقه عملیاتی نیاز به بررسی و دقت دارد و ممکن است نیاز به انجام عملیات خاص داشته باشد.

می توانید بر روی هر Task کلیک کرده و در مجموع وضعیت رنگهای مشاهده شده خود بیانگر خلاصه ای از وضعیت موجود یا مشکل بوجود آمده باشد.

برای مشاهده جزییات بیشتر در خصوص وضعیت موجود آنتی ویروس و مشکلات پدید آمده، لطفا به پوشه Reports and notifications مراجعه نمایید.

مشاهده گزارشات مربوط به ویروسهای یافت شده

- برای مشاهده خلاصه ای از لیست ویروس های یافت شده به ترتیب زیر عمل کنید،

به قسمت پوشه Reports and notifications رفته و از بخش Statistics پنجره مشاهده نتایج صفحه Anti-virus statistics را انتخاب نمایید.

خلاصه ای از فعالیتهای صورت گرفته در 24 ساعت گذشته در پنل مشاهده اطلاعات صفحه باز شده رویت خواهید نمودکه به شکل پیش فرض شامل:

- تاریخچه فعالیت ویروس
- بیشترین تعداد ویروسهایی که یافت شده اند
- کامپیوترهایی که بیشترین تعداد آلودگی را داشته اند
- کاربرانی که بر روی کامپیوترهایی که بیشترین تعداد ویروسهای یافت شده در آنها کار کرده اند

- برای مشاهده جزییات بیشتر در مورد ویروسهای یافت شده در شبکه،

بخش Report را انتخاب نمده و در قسمت Basic reports بر روی یکی از لینکهای گزارش مورد نظر کلیک نمایید:

- گزارش ویروسهای یافت شده
- گزارش کامپیوترها با بیشترین آلودگی
- گزارش کاربرانی که با کامپیوترهای آلوده کار کرده اند

هنگامی که گزارش مورد نظر را انتخاب نمودید، در پنجره نمایش نتایج، شاهد اطلاعات مربوط به ویروسهای یافت شده از زمان نصب سرور آنتی ویروس خواهید بود.

می توانید با تنظیم زمان مورد نظر خود در یک بازه زمانی خاص به تحلیل داده ها بپردازید.

مشاهده اتفاقات رخ داده مهم

- برای مشاهده اتفاقات رخ داده مهم در نرم افزار به ترتیب زیر عمل نمایید:

1. در درخت کنسولی، پوشه Event and computer section و سپس پوشه Events را انتخاب نمایید.

2. در لیست باز شده بر روی اتفاق مود نظر خود کلیک نمایید.

برای مشاهده آخرین رویدادها، Recent events را انتخاب نمایید. در جدول پدیدار شده شاهد اطلاعات جزیی در مورد هر رویداد خواهید بود. بطور پیش فرض تمامی اتفاقات رخ داده در طول هفت روز اخیر را مشاهده خواهید نمود.

می توانید رویداد مهم را با استفاده از بخش های Critical Events, Functional Events و Warnings Selections مشاهده نمایید.

همچنین می توانید رویدادهای خاص مورد نظر خودتان را ایجاد و مشاده نمایید. (برای اطلاعات بیشتر در این خصوص از راهنمای پیشرفت مدیریتی نرم افزار استفاده نمایید.

تنظیم نکات امنیتی مربوط به نرم افزار

- برای تنظیم یک Policy برای نرم افزار آنتی ویروس که برای کامپیوترهای زیر مجموعه یک گروه مدیریت شده ایجاد شده است، می بایست مراحل زیر را انجام داد:

1- یکی از Policy های مربوط به آنتی ویروس را از زیر پوشه Policies در گروه مدیریتی انتخاب نمایید.

2- در پنجره باز شده بر روی Edit Policy کلیک نمایید تا به قسمت مربوط به تنظیمات آن وارد شوید.

3- در این پنجره تنظیمات مربوطه را انجام دهید.

وقتی که تنظیمات ذخیره گردید، آن Policy بلافاصله بر روی تمامی کامپیوترهای زیر مجموعه گروه مدیریت شده اعمال می گردد.

تنظیم مربوط به آنتی ویروس:

تنظیمات عمومی نرم افزار برای تمامی کامپیوترهای زیر مجموعه گروه مدیریتی با استفاده از تنظیم Policies انجام می گیرد (تنظیم نکات امنیتی مربوط به نرم افزار). همچنین می توانید بر روی یک کامپیوتر خاص تغییرات لازم را اعمال نمایید.

برای انجام تغییرات مربوط به تنظیمات آنتی ویروس بر روی یک کامپیوتر خاص مراحل زیر را انجام دهید:

1- در گروه مدیریتی مورد نظر بر روی قسمت Client Computers کلیک نمایید و پنچره مربوط به تنظیمات (Properties) را باز کنید.

2- قسمت Applications را انتخاب نمایید.

3- یک نرم افزار انتخاب کرده و بر روی Properties کلیک نمایید.

4- تنظیمات مرود نیاز را تغییر دهید.

5- اگز تنظیمات غیر قابل ویرایش می باشد به این معنی است که در قسمت Policy قفل ( ) شده است.

بعد از اینکه تنظیمات را ذخیره نمودید بلافاصله بر روی کامپیوتر مورد نظر اعمال خواهد شد

چاپ و ذخیره سازی گزارشات

در کنسول مدیریتی نرم افزار کاسپراسکای می توان بخشی از گزارش را چاپ کرد و یا تمامی گزارش را با فرمت HTML و فایل اکسل و یا PDF ذخیره نمود.

برای پرینت بخشی از گزارش به روند زیرعمل نمایید:

1- در درخت کنسولی قسمت مربوط به Reports and notifications را انتخاب نمایید.

2- در پنجره باز شده بر روی Statistics صفحه مورد نظر را انتخاب نمایید.

3- بر روی آیکون  کلیک نمایید.

برای ذخیره کل گزارش:

1- در درخت کنسولی، بر روی پوشه Reports and notifications بر روی گزارش مورد نظر کلیک نمایید.

2- بروی آن کلیک راست نموده و گزینه Save را انتخاب کنید و مراحل را مطابق جادوگر برنامه ادامه دهید.

بعد از ذخیره سازی گزارش از این طریق، میتوانید گزارش را بعدا به کمک نرم افزارهای لازم باز کرده و مشاهده نمایید و یا چاپ کنید.

پشتیبان گیری از بانک اطلاعاتی سرور مدیریتی

آسانترین راه برای تهیه نسخه پشتیبان از بانک اطلاعاتی سرر مدیریتی آنتی ویروس کاسپراسکای استفاده از جادوگر برای ایجاد دستور اتوماتیک پشتیبان گیری است (روجوع کنید به بخش : **تنظیمات اولیه مربوط به آنتی ویروس**). به صورت پیش فرض هر روز یک کپی از اطلاعات سرور که کنسول مدیریتی را روی آن نصب کرده اید تهیه می شود. مسیر این فایل در پوشه Backup از پوشه اصلی نصب شده کنسول مدیریتی می باشد.

برای تهیه نسخه پشتیبان به صورت دستی، در شاخه **Kaspersky Administration Kit tasks** پوشه دستورات را انتخاب و دستور Run the task را اجرا کنید.

ارتقاء کنسول مدیریتی کاسپراسکای از نسخه 6.0 به 8.0
این بخش به ما یاد می دهد چگونه کنسول مدیریتی کاسپراسکای را از نسخه 6.0 به 8.0 ارتقاء دهیم. بخشی از توضیحات لازم در خصوص بروزرسانی نرم افزار در قسمتهای قبلی توضیح داده شده است. این بخش شامل توضیحات تکمیلی دراین زمینه می باشد.
روش معمول ارتقاء بروال زیر است:
1- یک نسخه پشتبان از بانک اطلاعاتی ورژن قبلی کاسپراسکای با استفاده از ابزار پشتیبان گیری تهیه کنید و در یک مسیر مشخص ذخیره نمایید. این ابزار پشتیبان گیری همراه با مجموعه نصب کاسپراسکای نصب می شود و پس از نصب سرور در شاخه اصلی مسیر نصب کاسپراسکای قابل دسترسی می باشد.
2- سرور و کنسول کاسپراسکای ورژن 8.0 را می توانید بروی همان سرور قبلی و یا یک سرور جدید نصب نمایید.
سرور کاسپر میتواند بروی کامپیوتری که نسخه قبلی بروری آن نصب می باشد و درحال اجرا نصب گردد. هنگام ارتقاء به نسخه 8.0 همه اطلاعات و تنظیمات مربوط به سرور قبلی و کنسول مدریتی مربوطه از نسخه قبلی برروی نسخه جدید اعمال می شود.
اگر سرور آنتی ویروس کاسپراسکای نسخه 8.0 برروی یک کامپیوتر جدید نصب شود اطلاعات و تنظیمات مربوط به نسخه قبلی را می توان با بازیابی از نسخه پشتیبان بکمک ابزار پشتیبان گیری بازیافت نمود.
3- اگر تنظیمات از نسخه قبلی به نسخه جدید انتقال نیابد، تنظیمات اولیه آنتی ویروس قابل اعمال خواهد بود.
4- ساختار گروه مدیریتی ایجاد خواهد شد.
5- کامپیوترهایی که نسخه قبلی را دارا می باشد در نسخه جدید قابل مشاهده و در دسترس و آماده انجام عملیات ارتقاء خواهند بود.
6- یک دستور نصب از راه دور برای نصب نسخه 6.0 آنتی ویروس برای کامپیوترهای در دسترس در کنسول ایجاد خواهد شد.این دستور در هنگام نصب نسخه جدید به شکل اتوماتیک ایجاد می شود.
7- دستورارتقاء اجرا خواهد شد و کاسپراسکای نسخه 6.0 برروی کامپیوترهای انتخاب شده نصب می شود. در طی این عملیات نسخه قبلی به شکل اتوماتیک حذف و نسخه جدید نصب خواهد شد.

8- تمامی کامپیوترهایی که نسخه 6.0 برروی آنها نصب شده اند به شکل اوماتیک در داخل ساختار گروه مدیریتی ورژن 8.0 قرار خواهند گرفت.
کلیه تنظیمات مربوط به آنتی ویروس نسخه قبلی در قالب تنظیمات نسخه جدید بروی تمامی کامپیوترهایی که نسخه جدید در آنها نصب شده باشد اعمال خواهد می شود.

با استفاده از جادوگر برنامه می توانید کلیه دستورات و تنظیمات خاص را که در ورژن قبلی ایجاد کرده بودید به ورژن جدیدتر تبدیل کنید. برای اطلاعات بیشتر به راهنمای جامع کاسپر با زبان اصلی مراجعه نمایید.

نتیجه گیری

قابلیتهای کنسول مدیریتی کاسپراسکای بسیار بیشتر از مطالبی است که در این مبحث به آن اشاره گردیده است. مطالب حاض یک سناریوی ساده را شرح می دهد و دتورات که به خواننده اجازه می دهد کار با سیتم مدیریتی کاسپراسکای را شروع کند و یک تنظیمات اولیه برای کامپیوترهای شبکه خود ایجاد نماید. این سناریو عملیاتی می باشد اما شرح کامل و توضیحات دقیتر برای اعمال تنظیمات مربوط به شبکه نیازمند:

- اعمال تنظیمات مربوط به مدیر امنیتی سیستم و توسعه آن
- توسعه متمرکز سیساست امنیتی آنتی ویورس بر روی کامپیوترهای کاربران از طریق شبکه کامپیوتر
- تعریف سیاستهای امنیتی قابل اعمال توسط آنتی ویروس
- تشخیص و تعریف عملیات مربوط به دستورات بروز رسانی بانک اطلاعاتی و کامپیوترهای کاربران
- تعریف دستورات عملیات امنیتی
- تعریف و اعمال دستورات مربوط به اسکن کامپیوترهای کاربران
- دریافت پیامهای مربوط به وضعیتهای بحرانی از وضعیت آنت ویروس شبکه
- مشاهده وضعیت جاری آنتی ویروس و دریافت گزارشات
- تهیه نسخه پشتیبان از اطلاعات سرور

توضیح: مطلب ترجمه شده مربوط به نسخه های قبلی آنتی ویروس کاسپراسکای می باشد. با توجه به اینکه کلیات و ساختار ورژنهای جدید تغییرات مختصری نسبت به قبل داشته اند بدیهی است مترجم تغییرات اساسی در نسخه های جدیدتر ترجمه و در اختیار همکاران قرار خواهد داد.