# نصب و مدیریت Kaspersky Security Center

**تهیه کنندگان:** حسین ظفری مرجان امیری

خرداد ماه 96



## نصب سرور کسپرسکی (Kaspersky Security Center):

جهت نصب کنسول مرکزی آنتی ویروس، وارد DVD دریافتی شده و مانند تصاویر زیر از درون پوشه Endpoint Security for Business پوشه Security Center 10.4.343 را باز کرده و فایل اجرایی موجود در این





با اجرای این فایل، ویزاردی برای شما باز خواهد شد که با اجرای Install Kaspersky Security Center10 فایل های موجود بر روی بسته از حالت فشرده خارج و بلافاصله فایل نصب اجرا خواهد گردید. مراحل نصب را بر اساس تصاویر ذیل ادامه دهید.

KA	PERSKY	KASPERSKY	SECURITY	CENT	ER 10 - ×
		<u>Install Kaspersky</u> <u>Center 10</u>	sy Security		Install only Kaspersky Security Center 10 Administration Console
	••				Install only Kaspersky Security Center 10 Network Agent
∞	<u>Install Kaspersk</u> <u>SHV</u>	y Security Center		⇔ ⊡	stall management plugins
[]	Install iOS MDM	<u>Server</u>		Ê Ex	tract installation packages
	Install Exchange Mobile Device Se	e ActiveSync_ erver			

در این مرحله نصب اصلی کنسول آغاز می شود:





Kaspersky Security Center Administration Server
License Agreement
Please read the following License Agreement carefully:
KASPERSKY LAB END USER LICENSE AGREEMENT
IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.
BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOUL IF YOU
✓ I accept the terms of the License Agreement.
© 2011 Kaspersky Lab ZAO. All Rights Reserved.
< Back Next > Cancel

### عملیات نصب را به صورت Custom ادامه دهید.

stallation Type					
Select the installation ty	pe that best suits your needs.				
Select the installation t Administration Server	type that is most suitable for your with mobile device support or mod	company. You lify its configur	i can ir ation li	nstall ater.	
Select the installation t Administration Server	type that is most suitable for your with mobile device support or moc	company. You lify its configur	i can ir ation l	nstall ater.	
Select the installation t Administration Server ( Standard Custom	type that is most suitable for your with mobile device support or moc	company. You lify its configur	ı can ir ation l	nstall ater.	
Select the installation t Administration Server	type that is most suitable for your with mobile device support or moc	company. You	ı can ir ation l	nstall ater.	

در این قسمت شما Component های مورد نیازبرای نصب Security Center را انتخاب می نمایید. در صورتیکه این سیستم سروراصلی آنتی ویروس شما می باشد، نصب را به همین صورت انجام دهید.در زیر توضیح کوتاهی از Component های موجود خواهید دید.



- Security Center نصب Component که اصلی ترین Component نصب Security Center می باشد، سرویسی است که مسئولیت مدیریت نرم افزارهای نصب شده کسپرسکی در شبکه را به عهده دارد.این سرویس درهنگام نصب احتیاج به یک پایگاه داده برای ذخیره اطلاعات دارد.
   همزمان با نصب این Component نرم افزار Network Agent نیز بر روی این سرور نصب می شود که وظیفه برقراری ارتباط بین کلاینت ها و سرور آنتی ویروس را بر عهده دارد، علاوه بر این پس از نصب این نرم افزار بر روی کلاینت ها وظیفه ی انتقال فایل ها و اطلاعات بر عهده آن خواهد بود.
- Mobile devices support با انتخاب این قسمت، شما اجازه مدیریت آنتی ویروس نصب شده بر روی دستگاه های Mobile را نیز از طریق کنسول Security center خواهید داشت.

Kaspersky Security Center 10 Administration Server	—		$\times$
Custom Setup			
Select the components to install.			
Administration Server			
Administration Server manages Kaspersky Lab applications.			
This component requires 150.2 MB free space on the hard disk.			
Location:	E	rowse	
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\			
– © 2017 AO Kaspersky Lab. All Rights Reserved.	_		_
< Back Next >		Cancel	



در این مرحله بزرگی شبکه خود را مشخص کنید. برای این منظور از تعداد لایسنس خود استفاده کنید.

Kaspersky Security Center 10 Administration Server	-		×
Network Size			
Specify network size.			
Select the approximate number of devices that you intend to manage. T	This		
information will be used to configure Kaspersky Security Center 10 prop be able to modify these settings later.	erly.	You will	
Fewer than 100 networked devices			
C From 100 to 1,000 networked devices			
C From 1,000 to 5,000 networked devices			
C More than 5,000 networked devices			
© 2017 AO Karawala Lab. All Diable Deserved			
- C 2017 AO Kaspersky Lab, All Rights Reserved,		6	1
< Back Next >	_	Cancel	



در قسمت بعدی شما باید یک Account برای نصب سرویس انتخاب نمایید. در این قسمت تنظیمی انجام ندهید و به مرحله بعد بروید.

Select the user account fr	or the Administration Server	service.	
Assign a logon account to administrator permissions	Administration Server servi to edit Administration Serve	ce. The account m r database.	ust obtain
KL-AK-8A79AB8D88BD	)A4		
C User account			
Accounts			Select
Processing and			
Password:			
Password: Confirm password:			-

tabase server				
Select database serve	er type.			
Select the type of dat Server, A database w	tabase server to which you want to cor vill be created for the selected DBMS at	nnect Administra	ation If the	
Select the type of dat Server. A database w application installation	tabase server to which you want to cor vill be created for the selected DBMS at n.	nnect Administra : further steps o	ation f the	
Select the type of dat Server. A database w application installation Microsoft SQL Ser	tabase server to which you want to cor vill be created for the selected DBMS at 1. ver	nnect Administra : further steps o	ation f the	
Select the type of dat Server. A database w application installation Microsoft SQL Ser MySQL	tabase server to which you want to cor vill be created for the selected DBMS at n. ver	nnect Administra i further steps o	ation f the	
Select the type of dat Server. A database w application installation Microsoft SQL Ser MySQL © 2017 AO Kasper	tabase server to which you want to cor vill be created for the selected DBMS at n. ver	nnect Administra further steps o	ation f the	

در این مرحله شما باید نوع پایگاه داده مورد نظربرای استفاده Security Center را مشخص کنید.پیشنهاد کسپرسکی استفاده از Microsoft SQL Server می باشد.



در این مرحله بگذارید خود کسپرسکی یک سرور SQL نسخه Express Edition برای شما نصب کند که این کار را به صورت اتوماتیک انجام میدهد،به مرحله بعد بروید.

onnection settings					
Specify Microsoft SQL Serv	ver parameters.				
Select the device with SQL	Server installed and specify the	e name of the	SQL S	Server	
ualabase.					
Install Microsoft SOL S	erver 201 <mark>4</mark> Express SP1 (Recom	mended)			
~					
Change attinting					
Choose existing					
Choose existing     SQL Server name:			1	Browse	
Choose existing SQL Server name:	[			Browse	
Choose existing SQL Server name: Database name:	KAV			Browse	
Choose existing SQL Server name: Database name:	KAV			Browse	
<ul> <li>Choose existing</li> <li>SQL Server name:</li> <li>Database name:</li> <li>(© 2017 AO Kaspersky I</li> </ul>	KAV			Browse	

در این قسمت نحوه ی اتصال به SQL Server را مشخص کنید. اجازه دهید گزینه ی Windows Authentication در این قسمت نحوه ماند.

Kaspersky Security Center 10 Admi	inistration Server		-		×
SQL Authentication Mode					
Choose Authentication Mode.					
Choose the authentication mode you select SQL Server Authentic	e you want to use to conne cation, enter the account a	ct to Micro nd confirm	soft SQL the pass	Server. If word.	F
Microsoft Windows Authentic	cation Mode				
O SQL Server Authentication M	1ode				
Account:					
Password;					
Confirm password:					
— © 2017 AO Kaspersky Lab. A	ll Rights Reserved,				
Check connection	< Back N	lext >		Cancel	



کنسول کسپرسکی برای ذخیره ی فایل های به روز رسانی وبسته های نصب و ...از یک پوشه ی به اشتراک گذاشته شده استفاده می کند.این پوشه به صورت پیش فرض در مسیر نصب کنسول قرار می گیرد. این پوشه KLshare نام دارد. در این قسمت هم تغییری ندهید و به مرحله بعدی بروید.

Kaspersky Security Center 10 Administration Server —		×
Shared folder		
Create a new shared folder or select an existing one.		
Shared folders store installation packages and updates for Kaspersky Lab applications. Create a new shared folder or select an existing one.	,	
Create a shared folder		
Folder:		
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center'	Browse	
Shared folder name: KLSHARE		
C Select existing shared folder		
	Browse,,	.,
— © 2017 AO Kaspersky Lab. All Rights Reserved. ——————		
< Back Next >	Cancel	

برای ارتباط بین کلاینت و سرور، Network Agent از دو در گاه **13000 و 14000**استفاده می کند. در گاه پیش فرض برای اتصال 13000می باشد که یک در گاه امن(SSL) است.

pecify settings to connect to	Administration Server.		
Enter the Administration Se to 65535.	erver ports. Port numbers must	be within th	e range of 1
Port number:	14000		
Port number: SSL port number:	13000		
Port number:	14000 13000		



درمرحله بعد، شما باید نحوه ی ارتباط Network Agent نصب شده بر روی کلاینت ها با سرور را مشخص کنید.

برای ارتباط با سرور،Network Agent می تواند از سه روش زیر استفاده کند:

- **IP Address:** بهترین حالت، استفاده از این گزینه می باشد. توجه داشته باشید و توجه داشته باشید که حتما IP را در این قسمت انتخاب کنید.
- DNS Name: زمانی که کنسول در شبکه ی Domain راه اندازی می شود ، بهترین حالت استفاده از DNS می PNS name
   باشد. زیرا اگر IP سرور تغییر کند و یا حتی Range شبکه عوض شود، می توان با تغییر کوچکی در سرور DNS ارتباط کلاینت ها با سرور را مجدّداً برقرار کرد.
  - Net Bios Name: در این قسمت نام خود سرور را انتخاب میکنیم.

```
کسپرسکی به صورت پیش فرض از IP Address جهت برقراری ارتباط استفاده می کند.
```

spersky Security Center 10 Administration Server —	×
Administration Server address	
Specify Administration Server address.	
Set the Administration Server address to one of the following options:	
<ul> <li>DNS name. Used if a DNS server is present and devices can get the Administration Server address from it.</li> </ul>	
b. NetBIOS name. Used if devices can get the Administration Server address through NetBIOS, or if a WINS server is present in the network.	
<ul> <li>c. IP address. Used only if the Administration Server has a static IP address which will not be changed in the future.</li> <li>Administration Server address:</li> </ul>	
Marjan-203.IEDCO.LOCAL	
© 2017 AO Kaspersky Lab. All Rights Reserved,	
< Back Next > Cancel	



در قسمت بعد شما میتوانید Plugin های آنتی ویروس هایی از کسپرسکی را که میخواهید بر روی سیستم هایتان نصب کنید را انتخاب نمایید تا در زمان نصب کنسول آن ها نیز نصب شوند.

Kaspersky Security Center 10 Administration Server —	×
Plug-ins for management of Kaspersky Lab applications	
Scheet plug in sto be installed.	
List of plug-ins:	
Console Plug-in of Kaspersky Security 8.0 for Linux Mail Server     Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 Console Plug-in     Kaspersky Anti-Virus 8.0 MP1/MP2 for Linux File Server Console Plug-in     Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition     Kaspersky Embedded Systems Security     Kaspersky Embedded Systems Security 1.1 MR1     Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Window     Kaspersky Endpoint Security 10 Service Pack 1 for Mac	ws
Kaspersky Endpoint Security 10 Service Pack 1 for Windows Console Plug-in Kaspersky Endpoint Security 10 Service Pack 2 for Windows Administration Plug-i	n ¥
- © 2017 AO Kaspersky Lab. All Rights Reserved.	1

در ادامه بر روی گزینه Install کلیک نمایید تا نصب شروع شود.

Caspersky Security Center 10 Administration Server	3 <del>-</del> 73		×
Ready to install Kaspersky Security Center 10 Admin	nistration	Server.	
Click Install to begin the installation. Click Back to review or installation settings. Click Cancel to exit the wizard.	chang <mark>e</mark> any	of your	
- © 2017 AO Kaspersky Lab. All Rights Reserved. ——			
< Back Insta		Cancel	



در انتهای نصب بر روی گزینه Finish کلیک کنید.





**Quick Start Wizard** 





در این مرحله در صورتیکه سرور برای دسترسی به اینترنت از Proxy استفاده می کند، می بایست گزینه Use Proxy در این مرحله در صورت به بخش بعدی بروید. Server را فعال کنید و سپس IP Address و پورت آن را وارد کنید. در غیر این صورت به بخش بعدی بروید.

Use proxy server	
Address:	
Port number:	3128
Bypass proxy server for local addresses	
Proxy server authorization	
User name:	
Password:	
Confirm password:	

در قسمت بعدی که KSN است به دلیل اینکه سرور های کسپرسکی ادارات امور شعب و شعبه ها اینترنت ندارند شما نمیتوانید از این ابزار استفاده نمایید. بنابراین گزینه I do not accept to participate in kaspersky security network را انتخاب نمایید و به مرحله بعدی بروید.

	×
Administration Server Quick Start Wizard	
Kaspersky Security Network	
Kaspersky Security Network (KSN) is a cloud database with constantly and rapidly updated information about the reputation of files, web resources, and software. Use of Kaspersky Security Network ensures faster responses to new threats, improves the performance of protection components, and reduces the likelihood of false positives.	
Kaspersky Security Network Statement – Kaspersky Security Center 10	
Please read this document thoroughly. It provides important information that you should be acquainted with before continuing to use our services or software. We reserve the right to modify this Statement at any time by making changes to this page.	
AO Kaspersky Lab (further Kaspersky Lab) has created this Statement in order to inform and disclose its data gathering and dissemination practices for Kaspersky Security Center 10 (further Software).	
Kaspersky Lab has a strong commitment to providing superior service to all of our customers and $\checkmark$	
○ I agree to participate in Kaspersky Security Network	
○ I do not agree to participate in Kaspersky Security Network	
Next Can	cel



در صورتیکه تمایل داشته باشید Notification های مربوط به کنسول برای شما ایمیل شود،می توانید آدرس ایمیل دریافت کننده، آدرس SMTP Server و پورت مربوط به SMTP Server را در این پنجره وارد کنید تا از این پس پیغام ها برای شما ارسال شود.

1	1	
/	5	

Administration Server Quick Start Wizard

Configure the method of email notification sending

SMTP servers:	
SMTP server port:	25 🛋
Use ESMTP authorization	
User name:	
Password:	
Confirm password:	
	Send test message

بعد از ساخته شدن Task وPolicy های مورد نیازاز قبیل Virus Scan و Update این قسمت به پایان میرسد.

	×
<ul> <li>Administration Server Quick Start Wizard</li> </ul>	
•	
You have successfully completed the Quick Start Wizard.	
Run Protection Deployment Wizard	
	Finish



## معرفی Tree کنسول:

همان طور که مشاهده می کنید tree کنسول شامل چندین بخش است که همه آنها زیر مجموعه Administration هستند.

K Kaspersky Security Center 10		-	- 0	×
File Action View Help				
🗢 🔿 🙍 📰 👔 🖬				
<ul> <li>Kaspersky Security Center 10</li> <li>Administration Server MARJAN-</li> <li>Managed devices</li> <li>Device selections</li> <li>Unassigned devices</li> </ul>	Administration Server MARJAN-203 > Advanced Advanced			
<ul> <li>✓ Policies</li> <li>Tasks</li> <li>✓ ■ Advanced</li> <li>▲ User accounts</li> <li>&gt; □ Application managemer</li> <li>&gt; 모 Remote installation</li> <li>&gt; Q Network poll</li> </ul>	<ul> <li>Unassigned devices</li> <li>List of unassigned devices and detection statistics.</li> <li><u>Bo to Unassigned devices folder</u></li> </ul>	<u>Move to Adva</u>	nced fold	<u>er</u>
> 🗄 Repositories	<ul> <li>User accounts</li> <li>This list displays information about user accounts in the network. To populate the list, Administration Server collects data from different so domain controllers, etc.).</li> <li><u>B</u> Go to User accounts folder</li> </ul>	Move from Advar	tory,	er
	<ul> <li>Application management</li> <li>Inventory, startup management, applications updating, and vulnerability scan on networked devices.</li> <li><u>Go to Application Management folder</u></li> </ul>	Move from Adva	nced fold	<u>er</u>
	Remote installation Remote installation of applications.	Move from Adva	nced fold	er V
< >>		Help 🔻 🖡	(A)PER	SKX₽

#### Managed devices:

گروه اصلی و یا به اصطلاح Parent کنسول کسپرسکی می باشد، به صورت پیش فرض کلیه ی سیستم های شبکه پس از نصب Network Agent در این گروه قرار می گیرند و در صورت ایجاد گروه بندی های جدیدی همه گروه ها نیز در زیر مجموعه ی این گروه قرار می گیرند.

این قسمت خود شامل چهار تب است:

#### **Devices:**

در این قسمت کامپیوتر های موجود در گروه Managed devices نمایش داده می شوند. برای اضافه کردن کامپوتر جدید می توانید Add Devices را انتخاب کنید یا از داخل قسمت Unassigned Devices سیستم های مورد نظر را با موس به گروه مورد نظر منتقل کنید.



**Policies:** 

جهت تنظيم policy براى Server ها و client ها از اين تب استفاده مى كنيم.

#### Tasks:

شامل Task های Update و Virus Scan و Find vulnerabilities است و جهت ایجاد Task برای Security Center های مربوط به Security Center نیز قرار می گیرند که به occurity هااز این تب استفاده می کنیم. در این قسمت Task های مربوط به Security Center نیز قرار می گیرند که به صورت معمول شامل Task های Task های vorus Security جهت دریافت فایل های به روز رسانی از سایت کسپرسکی و Task های Task می نسخه ی پشتیبان از تمامی تنظیمات Security کسپرسکی و Center می باشد. همچنین تسک های نصب ریموت که فقط مخصوص شبکه های دامین میباشد نیز در این بخش تنظیم میشوند.

در این قسمت باید در داخل تسک Download updates to the repository در بخش Settings و سپس در بخش Update Source سورس آپدیت سرور کسپرسکی شعب و سرپرستی را بر روی گزینه Master Server قرار دهید.

#### **Computer Selection:**

در این بخش میتوانید از کلاینت هایی که یک ارور خاص را دارند را کلی مشاهده نمایید.

Kaspersky Security Center 10 <u>File</u> Action View Help										– 0 ×
Kaspersky Security Center 10  Managed computers Computer selections Guassigned devices Zi Policies Tasks Advanced	Administration Server Computer selections to Use computer selections to Computers in this sel	DESKTOP-JBB ections sort out compute	PADS > ers with s	Computer sele	ections and run actions on <u>" status</u> <b>* *</b>	them, such as cre	ate a task for the	computers.		
	Selection properties	Perform action	n 💌	Advanced 🔻	Add/Remove colu	umns				Refresh
	Name	Type of operati Microsoft	Dom WOR	Agent installed ✓ Yes	Agent running ✓ Yes	Real-time file s No	Connecting to 1 minute ago	Last update 6 minutes ago	Status Critical/Las	Status description Kaspersky Anti-Virus is not ir
	<									>
									Help	▼ KA\$PER\$KY <sup>®</sup>



به طور مثال میتوانید سیستم هایی که آپدیت نشده اند را با کلیک بر روی گزینه Database are out of date در سراسر شبکه مشاهده نمایید. به تصویر زیر نگاه نمایید.

K Kaspersky Security Center 10					- 0	×
<u>File Action View H</u> elp						
🗢 🔿 📶 🍳 🖬						
<ul> <li>Kaspersky Security Center 10</li> <li>Managed computers</li> <li>Computer selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Mavanced</li> </ul>	Administration Server DES	ixtop-JBBPADS       > Computer selections         Preset selections       New computers found         Computers with the "Critical" status       Computers with the "Critical" status         Unassigned computers with Network Agent       Update agents         Lost connection to client computer       Protection is off         Kaspersky Anti-Virus is not installed       There are unprocessed objects         Many viruses detected       Virus Scan has not been performed for a long time         Databases are out of date       Not connected for a long time         Data encryption errors       Computers with "Warning" and "Critical" statuses due to vulnerabilities	rpdate utes ago	Status Critical/Las	Status descriptio Kaspersky Anti-V	Refresh n firus is not ir
				Help		₹
Commuter 1						
Computers: 1						

نحوه ایجاد گزارش در کنسول Kaspersky :

رای اینکار بر روی Administration Server کلیک نمایید ودر تب Report گزینه Administration Server گزینه template



K Kaspersky Security Center 10					- C	×
File Action View Help						
🗢 🔿 🙍 📅 🗙 🗐 🛛 🖬						
Kaspersky Security Center 10     Administration Server MARJAN     Managed devices     Device selections     Unassigned devices     Policies     Tasks	Administration Server Monitoring Sta	MARJAN-203 (IEDCO atistics Reports	(marjan.am) Events delivery		Server	<u>settings</u> <u>Refresh</u>
> advanced	Add/Remove columns					
	Name	Туре	Description	Creat ^		
	Database usage report	Database usage report Errors report	Kaspersky Lab anti-virus database usage re Report on main errors in Kaspersky Lab ap	6/7/ 6/7/	Database usage report	×
	Hardware report	Hardware report Incompatible applicatio	Report contains information about equipm Report on incompatible security applicatio	6/7/ 6/7/	Type: Database usage Description: Kaspersky Lab a	report nti-virus
	Kaspersky Lab softwa Key usage report Protection deployme	Kaspersky Lab software Key usage report Protection deployment	Report on Kaspersky Lab software versions Report on status of keys on devices Report on network deployment of Kaspers	6/7/ 6/7/ 6/7/	Created: 6/7/2017 3:28:	report 54 PM
	<ul> <li>Protection status report</li> <li>Report about errors in</li> </ul>	Protection status report Report about errors in e	This report contains information about the Report about errors in encryption of files a	6/7/ 6/7/	Actions Show report	
	Report on blockage o Report on blocked runs	Report on blockage of a Report on blocked runs	Report on blockage of access to encrypted This report contains information about blo	6/7/ 6/7/	Save     Deliver reports	
	Report on device users Report on effective us	Report on device users Report on effective user	This report displays the accounts of users Rights of the user specified in the report pr	6/7/ 6/7/	Properties     Delete	
	Report on encryption Report on file operati	Report on encryption st Report on file operation	This report displays the encryption statuses File operations on removable drives	6/7/ 6/7/		
	Report on installed ap	Report on installed appl Report on key usage by	Report on all installed applications Report on statistics of the use of keys by vir	6/7/ 6/7/		
	Report on most heavi	Report on most heavily	Top 10 most heavily infected devices	6/7/		
< >						R∫KYᡱ
Reports: 27						

		×
~	New report template wizard	
	Defining report template name	
	Name:	
	New report	
	Next Cance	I







در این مرحله می توانید یک محدوده ی زمانی برای گرقتن گزارش تهیه نمایید، به عنوان مثال 30 روز گذشته.

	×
New report template wizard	
Selecting reporting period	
○ From starting date to ending date:	
Starting date:	1/ 1/2017
Ending date:	6/11/2017
$\bigcirc$ From starting date to the report creation date:	
Starting date:	1/ 1/2017
Specified number of days before the report creation d	ate:
Number of days:	30
	Next Cancel



در این پنجره می توانید این گزارش را برای گروه خاصی از سیستم ها ایجاد کنید.

		×
←	New report template wizard	
	Select report type	
	You can generate a report for an arbitrary set of devices, for a selection of devices, or for all devices in any administration group.	
	Report type:	
	I want to create a report for a group	
	○ I want to create a report for specific devices	
	○ I want to create a report for a selection of devices	
	Next Cance	el



		×
←	New report template wizard	
	Select group	
	Target group for report:	
	Managed devices	Browse
	N	ext Cancel



		$\times$
~	New report template wizard	
	Creating a report template on the Administration Server	
	Click the Finish button to create "New report" and complete the Wizard.	
	Finish Cancel	



همان طور که مشاهده می کنید گزارش ساخته شده در لیست Report ها اضافه شده است.





#### Advanced:

این بخش شامل چندین قسمت است. مانند، ساختن category، مشاهد ه برنامه های نصب شده، فایل های اجرایی داخل شبکه و لایسنس ها و آپدیت سیستم عامل ها است.

#### **Application categories:**

در این بخش شما می توانید دسته بندی های مختلفی بر روی application های نصب شده روی سیستم های داخل شبکه انجام دهید، این قابلیت ها شامل دسترسی یا عدم دسترسی تعدادی از application به کاربران می باشد. در قسمت Policy در بخش Start of application control می توانید از این Category ها استفاده کنید. به صورت پیش فرض در این قسمت هیچ Category از قبل تعریف نشده است. جهت تعریف یک Category مطابق مراحل زیر عمل کنید:

Kaspersky Security Center 10 <u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp ← → 20				-	- 0	×
Kaspersky Security Center 10	Administration Server DESKTOP-JBB Application categories Categorizing applications allows you to enhan	<u>BPADS</u> > <u>Advanced</u> > <u>Application management</u> > Application categotice applications start management.	ories			
Tasks     Tasks     User accounts     Application management     Application categories     Applications registry     Executable files     Software vulnerabilities     Software updates     Kaspersky Lab licenses     S 모 Remote installation     Outputs Mentione	Create a category Import				<u>Refre</u>	<u>sh</u> nd
> Q, Network poll > ☐ Repositories	Add/Remove columns	Description	Search by text colu	Updated	C	2
Application categories: 0				<u>Help</u> ▼	KASPERSKY	

ابتدا بر روی گزینه Create a category کلیک کنید.



Create User Category Wizard			×
Conditions			
	Condition Value		×
•	m	4	
	<u>A</u> dd ▼	Properties	]
		Next	Cancel

جهت اضافه کردن Add مورد نظر بر روی دکمه Add کلیک نمایید، لیست باز شونده کنار دکمه ی Add این امکان را به شما می دهد تا شیوه ی اضافه کردن application ها در category مورد نظر را انتخاب کنید.در این مثال بر روی لیست باز شونده کلیک می کنیم و روشانتخاب را بر اساس From the executable files list تنظیم می کنیم و در پنجره ای که باز می شود executable file مورد نظر خود را انتخاب می کنیم.





پس از انتخاب این گزینه لیستی از فایل های اجرایی موجود بر روی سیستم های داخل شبکه نمایش می یابد. برای مثال در این پنجره فایل اجرایی فیلتر شکن U1008.exe را انتخاب می کنیم.

File name	File version	Application name
🖃 sctasks.exe	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
SearchFilterHost.exe	7.00.7601.17610 (win7sp	Windows® Search
SearchIndexer.exe	7.00.7601.17610 (win7sp	Windows® Search
SearchProtocolHost.exe	7.00.7601.17610 (win7sp	Windows® Search
services.exe	6.1.7600.16385 (win7_rt	Microsoft® Windows® Opera
SHELL32.DLL	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
🖃 smss.exe	6.1.7600.16385 (win7_rt	Microsoft® Windows® Opera
🖃 spoolsv.exe	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
SQLBROWSER.EXE	2007.0100.2531.00 ((Kat	Microsoft SQL Server
SQLSERVR.EXE	2005.090.5000.00	Microsoft SQL Server
SQLSERVR.EXE	2007.0100.2531.00 ((Kat	Microsoft SQL Server
SQLWRITER.EXE	2007.0100.1600.022 ((S	Microsoft SQL Server
🖃 svchost.exe	6.1.7600.16385 (win7_rt	Microsoft® Windows® Opera
🖃 taskeng.exe	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
🖃 taskhost.exe	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
TeamViewer.exe	6.0.11656.0	TeamViewer
TrustedInstaller.exe	6.1.7601.17514 (win7sp1	Microsoft® Windows® Opera
🖅 U 1008.exe		
💷 updater.EXE	9.0.2786.0	Kaspersky Security Center
🖅 vmnat.exe	7.0.0 build-203739	VMware Workstation
🖅 vmnetdhcp.exe	7.0.0 build-203739	VMware Workstation
4	7.0.0 L. H 202720	URA
		F

Create User Category Wizar	d
Conditions	
Condition criterion	Condition value
MD5 hash	U1008.exe () : B2D30ED05E7A230B1D6254666
•	4
	100 Properous
	Next Cancel



با کلیک بر روی دکمه Add می توانید Application مورد نظر خود را از این لیست مستثنی کنید.

	Create User Category Wiza	rd	×
Ex	clusions		
	Condition criterion	Condition value	×
	•	m	•
		Add 💌	Properties
			Next Cancel

Create User Category Wizard	×
Creating user category	
Click the Finish button to create "client category" and complete the Wizard.	
Finish Cance	<u>.</u>



#### Application registry:

در این قسمت (به شرط وجود Network Agent بر روی سیستم های موجود در شبکه ) می توانید کلیه ی Application

های نصب شده بر روی سیستم های شبکه را مشاهده نمایید.





#### **Executable Files:**

در این قسمت از کنسول فایل های اجرایی که بر روی سیستم های داخل شبکه وجود دارد نمایش داده می شود.

K Kaspersky Security Center 10						- 0 ×
<u>File Action View Help</u>						
Kaspersky Security Center 10     Administration Server DESKTOP-JBBPADS     Managed computers     Computer selections     Linassigned devices     Z' Policies     Tasks	Administration Server DESKTOP-JBB	PADS > Advanced > Adva	Application management > Executabl	e files		
Advanced     Application management     Application categories     Application registry     Executable files     Software vupdates     Kaspersky Lab licenses     Aemote installation     Q Network poll     Bepositories	Report on blocked application runs • No filter specified, records total: 0 AddRemove columns	L		suru protocol to radiume o Search	by text columns	0 Q
	File name	File version	Application name	Application version	Manufacturer	Trust level
	<				Help 💌	
Executable files: 0					Lieip +	

#### Software vulnerabilities:

این قسمت از کنسول آسیب پذیری های شناسایی شده درنرم افزارهای نصب شده بر روی سیستم های داخل شبکه را

<ul> <li>              Assersty Security Center 10          </li> <li>             Elie Action View Help         </li> <li>             Elie Action View Help         </li> <li>             Administration Server DESKTOP-JBBRADS             Application management             Sintware uphatesin             Servere uphates</li></ul>
prime       prime <t< td=""></t<>
Kaspersky Security Center 10 Kaspersky Security Center 10 Managed computers Computer selections Computer selections Folicies Foli
Administration Server DESKTOP-JBBPADS Administration Server DESKTOP-JBBPADS Computer selections Computer sel
↓ Unassigned devices   ↓ Dicise   ↓ Dicise   ↓ Dication management   · Application management   · Application categories   · Application registry   · Software vulnerabilities   · Repositories
In Tasks       Configure vulnerability scan       Vulnerabilities report       Refer         ▲ Application management       - Application sregistry       - Executable files       - Software vulnerabilities
<ul> <li>Application management         <ul> <li>Application anagement</li> <li>Application categories</li> <li>Application categories</li> <li>Application categories</li> <li>Software vulnerabilities:</li> <li>Secret by text columns</li> </ul> </li> <li>AddRemove columns</li> </ul>
> Q Network poll         > B Repositories         Name       Severity level       Show       Source       Web address       Manufacturer       Application family       Application
Name         Severity Yevel         Show         Source         Web address         Manufacturer         Application family         Application
Help - KASPERSKY



#### Kaspersky Lab licenses:

در این قسمت میتوانید لایسنس های کسپرسکی خود را اضافه نمایید تا بعد از نصب آنتی ویروس ها بر روی سیستم های دیگر، لایسنس به صورت اتوماتیک بر روی آن ها قرار گیرد.



برای اضافه کردن لایسنس ها ابتدا بر روی گزینه Add key کلیک نماییدو پس از باز شدن صفحه زیر، بر روی گزینه Activate application with key file کلیک نمایید.





سپس در مرحله بعد فایل لایسنس خود را Browse کنید و تیک گزینه Automatically deploy key را نیز بزنید. این کار را برای هر دو فایل لایسنس انجام دهید.

			×
←	Add Key Wizard		
	Selecting a key		
	Specify key file:		
	I	Select	
	Automatically deploy key to managed computers		
		<u>N</u> ext C	ancel

			$\times$
←	Add Key Wizard		
	Selecting a key		
	Constitution flat		
	specity key nie:		
	C:\Users\test\Desktop\53EF221B.key	Select	
	Automatically deploy key to managed computers		
	[	<u>N</u> ext Cance	el



#### **Remote installation:**

 Installation packages: برای نصب هر گونه نرم افزاری (چه نرم افزار های کسپرسکی و چه نرم افزار های غیر از آن) ابتدا باید Package مربوط به آن نرم افزار در این قسمت ساخته شود، البته Package های مربوط به نصب نرم افزارهای کسپرسکی با نصب کنسول Security center به صورت پیش فرض ساخته می شود و نیازی به ساختن دوباره آن ها نمی باشد.

برای نصب بروی کلاینت ها ابتدا باید از پکیج آنتی ویروس موجود در این قسمت یک پکیج نصب به نام Stand-alone بسازید. ابتدا مطابق تصویر زیر بر روی پکیج Kaspersky Endpoint Security راست کلیک کنید و بر روی گزینه Create stand-alone installation package کلیک نمایید.

Kaspersky Security Center 10 Eile Action View Help ← ➡   20 000 100 00 100 100 100 100				- 0 ×	
<ul> <li>Kaspersky Security Center 10</li> <li>Administration Server DESKTOP-JBBPADS</li> <li>Managed computers</li> <li>Computer selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Advanced</li> <li>User accounts</li> <li>Application management</li> </ul>	Administration Server DESKTOP-JBBPADS > Advar Installation packages Installation packages are used for remote deployment. Create installation package View the list of stand-are Add/Remove columns	nced > Remote installation > Instal lone packages Additional actions	llation packages	<u>Properties</u> Refresh	
<ul> <li>Application categories</li> <li>Applications registry</li> <li>Executable files</li> <li>Software updates</li> <li>Kaspersky Lab licenses</li> <li>✓ IRemote installation</li> <li>Installation packages</li> <li>Q Network poll</li> <li>E Repositories</li> </ul>	Name Kaspersky Endpoint Security 10 for Windows (10.3.0.6294) Kaspersky Security Center Network Agent (10.4.343)	Application Install application Create stand-alone installation packa Show the list of stand-alone package Group by column Delete Export list Properties	Version number Language en s >>	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	
Installation packages: 2					



سپس در صفحه جدید پکیج Network Agent را انتخاب نمایید و به مرحله بعد بروید.

		$\times$
←	Stand-alone Installation Package Creation Wizard	
	Selecting Network Agent installation package for combined installation	
	Install Network Agent along with this application	
	Name	
	Kaspersky Security Center Network Agent (10.4.343)	
	N <u>e</u> w	
	<u>N</u> ext Can	cel

در مرحله بعدی تغییری ندهید و به مرحله بعد بروید.

		$\times$
~	Stand-alone Installation Package Creation Wizard	
	Moving to the list of managed computers	
	Select the group to which computers will be moved after installation:	
	O Do not move computers	
	Move unassigned computers to the group:	
	Managed computers Select	
		_
	<u>N</u> ext Cancel	



## سپس اجازه دهید تا پکیج فوق ساخته شود. پس از ساخت این پکیج در share سرور کسپرسکی در مسیر زیر قرار میگیرد.

\\Kaspersky server IP\KLshare\pkginst\





#### **Network Poll:**

در این قسمت شما میتوانید مطابق تصویر زیر در سه بخش مختلف Domain و Active Directory و IP Subnet سمت معامی داخل شبکه را شناسایی کنید و آن ها را به داخل Managed devices انتقال دهید.



این قسمت خود شامل چندین زیر شاخه است :

- Kaspersky Lab updates and patches : شامل نمایشی از پایگاه داده و ماژول های آپدیت و آخرین تاریخ به روز رسانی این اجزا (تاریخ Createشدن و receive شدن فایل های به روز رسانی) می باشد
- Quarantine: در صورتیکه آنتی ویروس برنامه ای را مشکوک به ویروس ببیندآن را قرنطینه می کند و اطلاعات آن فایل قرنطینه شده را به Security Center ارسال می کند.
- Backup: زمانی که آنتی ویروس ها بر روی سیستم ها فایلی را ویروسی شناسایی کنند در ابتدا سعی می کنند آلودگی را از روی فایل برطرف کنند (Disinfect) ، در صورتی که موفق به رفع آلودگی نشوند، فایل مذکور به صورت کامل پاک خواهد شد. در هر صورت، قبل از اینکه آنتی ویروس عملیاتی بر روی فایل های آلوده انجام دهد یک نسخه ی پشتیبان از آن فایل تهیه می شود تا در صورت لزوم بتوان آن فایل را Restore نمود.اطلاعات نسخه های پشتیبان تهیه شده از فایل ها در این محل ذخیره می شود.
- Unprocessed files: در این بخش فایل های ویروسی شناسایی شده توسط آنتی ویروس سیستم ها که هنوز پردازشی روی آنها صورت نگرفته نمایش داده می شود.



# Policy های مربوط به سرور و کلاینت

Policyها به طور عموم در جهت تنظیمات کاربردی و حفاظتی بروی سیستم های شما استفاده می شود

در شاخه ی Managed computer یک Policy برای Server ها و Workstation ها جهت تنظیمات و تغییرات اجزای آنتی ویروس بر روی سیستم ها یا فعال و غیرفعال کردن قسمت هایی بر روی آنتی ویروس و همچنین اعمال محدودیت تغییر بر روی آنتی ویروس توسط کار بران وجود دارد.

تنها مکان برای تعریف Policy داخل گروه های موجود می باشد، به ازای هر گروه یک Policy در قسمت Policies مربوط به آن گروه تعریف می شود.

وارد Policies در قسمت Managed computer شوید.

جهت تغییر تنظیمات Policy بر روی سیستم ها، وارد تب Policies در Managed computer شوید، سپس بر روی Protection policy راست کلیک نمایید و گزینه یProperties را انتخاب کنید .در این قسمت تمامی تنظیمات مربوط به آنتی ویروس قرار دارد که بر اساس نیاز می توانید آنها را تغییر دهید.

همان طور که در این قسمت مشاهده می کنید لیست تمام Component های محافظت مربوط به نوع نرم افزار برای شما نمایش داده خواهد شد شما می توانید با فعال یا غیر فعال کردن هر Component ، آنComponent را بر روی آنتی ویروس سیسستم ها فعال یا غیر فعال کنید، همچنین در کنار هر قسمت یک قفل موجود می باشد با یکبار کلیک کردن بر روی قفل حالت قفل تغییر خواهد کرد، این قفل دسترسی کاربران را مشخص می کند هر قسمتی که قفل باز داشته باشد توسط کاربر قابل تغییر می باشد.در ادامه چند نمونه از این Component ها را توضیح خواهیم داد.



#### **Application startup control**

این Component راه اندازی Application های داخل شبکه را کنترل می کند. شما در این قسمت می توانید مشخص کنید چه Application هایی توسط چه اشخاصی اجازه ی اجرا شدن داشته باشند و یا چه اشخاصی نتوانند آن را اجرا کنند. برای اجرای این قابلیت شما در ابتدا باید در Applications and vulnerabilities یک Category ایجاد کنید که در قسمت های قبلی توضیح به طور کامل داده شده است .سپس برای استفاده ازین قابلیت شما با زدن دکمه Add، Category ماخته شده را برای کاربران تعیین نمایید .

📧 Properties: Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows 🛛 – 🛛 🛛 🗙							
Sections	Applicatio	n Startup Contro	l i				
General ^ Application Startup Control							
Event notification	This component	nt monitors users' attemp	ts to start ap	plications and control	s the startup	ofapplicatio	ons by
Endpoint control using rules.							
Application Startup Control	A To send a	pplication startup informa	ition to Admin	istration Server, sele	ct the About	started	
Application Privilege Control	Administra	applications check box in the policy properties in the Reports and Storages section under Inform Administration Server.					
Vulnerability Monitor	Application	Startup Control Settings -					
Device Control	Application	Startup Control rules:			🔎 Eve	rywhere	•
Web Control	- h		O Chattar	iant nanturin			
Anti-Virus protection	- Auu Status					Plackad	
General Protection Settings	On	Allow all	e	Everyone		DIOCKEU	
File Anti-Virus	Off off	Trusted updaters		Everyone			
Mail Anti-Virus	Off	Golden Image		Everyone			
Web Anti-Virus							
IM Anti-Virus							
Firewall	Generat	e test verdict for default	rule				
Network Attack Blocker	Advanced S	ettings					
System Watcher Configure the template of the message that is displayed when the start of an							
Advanced Settings 🗸 🗸		application is blocke	a and or die	complaint to the LAN	aariinisu ator		
Help				OK	Cancel	<u>A</u> pply	/



#### **Application Privilege Control**

این Component وضعیت و فعالیت Application ها را بر روی سیستم پیگیری می کند و پس از چک کردن وضعیت هر Application و اختصاص دادن آن به یکی از گروهای Low restricted , Low restricted و اختصاص دادن آن به یکی از گروهای Application می دهد. برای این کار بروی Setting در قسمت اجازه فعالیت را بر اساس گروه بندی انجام شده به آن Application می دهد. برای این کار بروی Application در قسمت اضافه کنید.

📧 Properties: Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows 🛛 🗌 🗙						
Sections	Application Privilege Control					
General ^	Application Privilege Control 🖷					
Event notification	This component keeps track of application activities in the system and regulates the activity of					
Endpoint control	applications depending on their status.					
Application Startup Control	Application rules					
Application Privilege Control	Settings Configure application rights to access user files and application settings or to access operating system processes and objects.					
Vulnerability Monitor	Settings Configure application rights to access various categories of operating system					
Device Control	resources and personal data.					
Web Control	Application processing rules					
Anti-Virus protection	Update control rules for previously unknown applications from KSN databases					
General Protection Settings	✓ Trust applications that have a digital signature					
File Anti-Virus	For unknown applications:					
Mail Anti-Virus	$\bigcirc$ Automatically move to group: Low Restricted $\checkmark$					
Web Anti-Virus	Use heuristic analysis to define group					
IM Anti-Virus	Maximum time to define group: 30 🐳 sec					
Firewall	$\checkmark$ Delete rules for applications that are not started for more than 60 $\checkmark$ day(s)					
Network Attack Blocker						
System Watcher						
Advanced Settings 🗸 🗸						
Help	OK Cancel Apply					



#### **Vulnerability Monitor**

فعال بودن این گزینه سبب می شود زمانی که Application ای شروع به کار می کند و یا در حال اجرا شدن است آنتی ویروس کسپرسکی آسیب پذیری این Application را بررسی کند، در صورتیکه این گزینه فعال نباشد بررسی آسیب پذیری به صورت اتومات انجام نمی گیرد ودر صورت نیاز می بایست می بایست می را از داخل find Vulnerabilities را کنید.





#### **Device Control**

این Component به شما اجازه می دهد تا Removable Device ها را بر روی سیستم های داخل شبکه مدیریت کنید.به طور مثال شما می توانید از این طریق دسترسی به Flash Memory و یا CD\DVD-ROM را روی سیستم های کاربران بیندید.

🔳 Properties: Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows - 🛛 🛛 🗙						×
Sections	Device Control					
General ^	Device Control	1				
Event notification	The component allows con	trolling the connection of	removable drives.			
Endpoint control	- Device Control Settings					
Application Startup Control		Connection buses	Trusted devices			
Application Privilege Control		connection buses	musicu ucinicis	-		
Vulnerability Monitor	C Luit	Devices			Access	
Device Control	Hard drives	Devices			() ()	
Web Control	📋 Removable drives				0	
Anti-Virus protection	Printers					- 11
General Protection Settings	CD/DVD drives					_
File Anti-Virus	Modems					
Mail Anti-Virus	Tape devices				•	
Web Anti-Virus	Multifunctional devi     Smart card readers	ces				-
IM Anti-Virus		morary access				
Firewall	C Allow request for ter	nportar y access				
Network Attack Blocker	Advanced Settings	ure the templater of more	and that are display	od when acco	aa ia blacka	
System Watcher Templates Templates device or its contents, and the template of the complaint letter to the LAN administrator.				uwa		
Advanced Settings 🗸 🗸						
Help OK Cancel App				Apply	у	

بروی Removable drives کلیک کرده و به صورت پیش فرض در قسمت Depend On bus ، Accessمی باشد که میتوانید Allow یا blockرا انتخاب نمایید و یا می توانید برای تعیین دسترسی برای تعدادی از کاربران دکمه Edit را بزنید و با اضافه کردن کاربران دسترسی Read ,Write مشخص کنید.



#### Web Control

این Component این امکان را به شما می دهد تا از طریق آن دسترسی کاربران به وب سایت های خاصی را براساس Content و یا بر اساس URL ، مدیریت کنید.

📧 Properties: Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows 🦳 🗌 🗙				
Sections	Web Control			
General A Web Control				
Event notification	The component allows controlling access to web resources depending on the	air content and	d location.	
Endpoint control	Web Control Settings		8	
Application Startup Control	Access rules sorted by priority:	🔎 Everyv	where 🔹	
Application Privilege Control	🕂 Add 🖉 Edit 💥 Delete 🐐 Move up 🌡 Move down			
Vulnerability Monitor	Status Rule name Users		Action	
Device Control	On Scripts and Stylesheets		<ul> <li>✓</li> </ul>	
Web Control	On Default rule		~	
Anti-Virus protection				
General Protection Settings				
File Anti-Virus				
Mail Anti-Virus				
Web Anti-Virus				
IM Anti-Virus				
Firewall				
Network Attack Blocker	Advanced Settings		<b>a</b>	
System Watcher	System Watcher Configure templates of the messages that are shown when unwanted web pages websites are visited, and the template of the complaint letter to the LAN			
Advanced Settings 🗸 🗸	administrator.			
<u>Help</u>	OK Ca	ncel	Apply	

بروی گزینه Addکلیک کرده در قسمت filter Content، همانطور که مشاهده می کنید بر اساس محتوا می توانید سایت های مد نظرتان را فیلتر نمایید . در صورتی که بخواهید آدرس سایت خاصی را فیلتر نمایید در قسمت apply to addressحالت To jindividual address را می زنید و مانند نمونه سایت را وارد می نمایید.در صورتی که برای گروه یا کاربران خاص میخواهید این فیلترینگ را انجام دهیددر قسمت Specify User and Group می توانید خاصیت Allow یا Block را تنظیم نمایید.



Name:	
Filter content:	By content categories and types of data $\sim$
Content categories Adult content Software, audio, video Alcohol, tobacco, narcotics Violence Profanity, obscenity Weapons, explosives, pyrotechnics Gam Inte Kapply to Example: *kaspersky.com Help Add	Types of data     Video     Sound     Office files     Executable files     Archives     Graphic files     Sk     Cancel     ✓
Action	Allow
Actor:	Allow
Rule schedule:	Always ~ Settings

## Anti-Virus protection

#### **General Protection Setting**

🔲 Properties: Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows 🛛 🗌 🗙					
Sections	General Protection Settings				
General Event notification Endpoint control Application Startup Control Application Privilege Control Vulnerability Monitor Device Control	<ul> <li>General Settings</li> <li>Launch Kaspersky Endpoint Security 10 for Windows at computer startup</li> <li>Enable Advanced Disinfection technology</li> <li>Objects for detection</li> <li>Detection of the following object types is enabled:</li> <li>Viruses, worms, Trojans, and malicious tools</li> <li>Adware and auto-dialers</li> </ul>		<u>S</u> ettings,,		
Web Control Anti-Virus protection General Protection Settings File Anti-Virus Mail Anti-Virus	- Packed files that may cause harm, and multi-packed files  - Exclusions and trusted zone  Scan exclusions: 308 (total 308)  Trusted applications: 14 (total 14)  - Monitored ports  Munitor all network ports	S	Gettings		
Web Anti-Virus IM Anti-Virus Firewall Network Attack Blocker System Watcher Advanced Settings	<ul> <li>Monitor only selected ports</li> </ul>	S	ettings		
Help	OK Cancel		<u>A</u> pply		



امکان بسیار خوبی که این Component در اختیار شما می گذارد این است که در قسمت Component در اختیار شما می گذارد این است که در قسمت component وی ویروس بر روی zone می توانید یک Component یا یک Folder را Exclude کنید که چه component هایی از آنتی ویروس بر روی آن فعال نباشد(و یا حتی تمامیComponentهای آنتی ویروس بر روی آن غیر فعال باشد).

از این ویژگی زمانی استفاده می شودکه به طور مثال نرم افزاری که تحت شبکه کار می کند پس از نصب آنتی به کندی کار کند و یا به عنوان ویروس شناخته شود یا به نحوی جلوی یکسری فعالیت های آن گرفته شودو موجب شود قسمتی ازآن کار نکند.همچنین در مواردی که Crack های یک نرم افزار به عنوان ویروس شناخته می شود، از این ویژگی استفاده می شود.

جهت تنظيم اين قسمت روى setting كليك نماييد، سپس وارد تب Trusted application شويد.

دراین قسمت می توانید یک application را Add کنید تا دیگر Component های آنتی ویروس بر روی آن کار نکند.

🔀 Trus	ed zone	
Scan e	exclusions Trusted applications	
Kaspe applic contr	rsky Endpoint Security 10 for Windows a ation added to the list of trusted applica ol.	loes not control activities of trusted applications. For each tions, you can specify the types of activities to exclude from
4	Add 🖉 Edit 💥 Delete	
	Application	Path
	svchost.exe	%SystemRoot%\system32\svchost.exe
	osk.exe	%SystemRoot%\system32\osk.exe
	r_server.exe	%ProgramFiles%\Radmin\r_server.exe
	r_server.exe	%ProgramFiles(x86)%\Radmin\r_server.exe
	WINVNC.EXE	%ProgramFiles%\ULTRAVNC\WINVNC.EXE
	WINVNC.EXE	%ProgramFiles(x86)%\ULTRAVNC\WINVNC.EXE
	r_server.exe	%SystemRoot%\system32\r_server.exe
	r_server.exe	%winDir%\SysWOW64\r_server.exe
	awhost32.exe	%ProgramFiles%\Symantec\pcAnywhere\awhost32
	awhost32.exe	%ProgramFiles(x86)%\Symantec\pcAnywhere\awh
	tb2pro.exe	%ProgramFiles%\Timbuktu Pro\tb2pro.exe
	tb2pro.exe	%ProgramFiles(x86)%\Timbuktu Pro\tb2pro.exe
	DWRCS.exe	%SystemRoot%\system32\DWRCS.exe
	DWRCS.exe	%winDir%\SysWOW64\DWRCS.exe
		Import Export
Help		O <u>K</u> Close

برای اینکار این بار مسیر مورد نظر را در قسمت Application rules وارد می کنیم.

گزینه ی Add را انتخاب کنید و سپس مسیر Application مورد نظر را در قسمت Applicationوارد کنید و در قسمت Add Action تعیین کنیدچه عملیاتی بر روی این Application صورت گیرد.



🔀 Scan excl	usions for application	x				
Path						
Do not sca	an opened files					
Do not inh	Do not monitor application activity Do not inherit restrictions of the parent process (application)					
Do not mo	nitor child application activity raction with application interface					
Do not sca	an network traffic					
Help		ose				

درصورتی که بروی تعداد خاصی client مدنظرتان باشد با زدن تیک Do not scan network trafic بروی Any در قسمت IP addresses کلیک کرده و گزینه spacifyرا زده و IPهای کامپیوتر های مد نظر را وارد نمایید.

#### **File Antivirus**



همان طور که مشاهده می کنید قفل ها به صورت پیش فرض بسته است و بنا به نیاز می توانیدآنها را باز کنید، با گذاشتن یا برداشتن تیک گزینه Enable File Anti-virus می توانیداین Component را روی سیستم ها فعال یا غیر فعال کنید.در قسمت Security level سطح امنیتی این Component را تعیین می کنیم و درقسمت Action نحوه ی برخورد با



ویروس های پیدا شده را مشخص می کنید که آیا آنتی ویروس جهت انجام عملیات خود از کاربران سوالی مبنی برچگونگی برخورد آنتی ویروس با ویروس های شناسایی شده بپرسد یا خیر.پیشنها ما تنظیم Action روی گزینه ی Belect action را است و تیک گزینه های Disinfect و Delete if disinfection fails را بزنید.

Disinfect: با انتخاب این گزینه در صورتیکه تنها قسمتی از فایل آلوده شده باشد، آنتی ویروس تنها قسمت آلوده را پاک می کند (حذف ویروس)

Delete if disinfection fails: در صورتیکه عملیات Disinfect انجام نشود آنتی ویروس کل فایل را پاک خواهد نمود.

Properties: Kaspersky Endpoint Security	rity 10 Service Pack 1 Maintenance Release 2 for Windows	_		×
Sections	Mail Anti-Virus			
General	🗹 Mail Anti-Virus 🗎			
Event notification	This component scans incoming and outgoing messages for dangerous objects. T	he follow	ing proto	cols
Endpoint control	are supported: POP3, SMTP, IMAP, MAPI, and NNTP.			
Application Startup Control	Security level			
Application Privilege Control	- Recommended	<u></u>	ettings	
Vulnerability Monitor	- Optimal protection	В	y <u>d</u> efault	
Device Control	- Recommended for most users			
Web Control				
Anti-Virus protection	Action on threat detection			
General Protection Settings	Select action a <u>u</u> tomatically			
File Anti-Virus	O Select action: Disinfect. Delete if disinfection fails			
Mail Anti-Virus	✓ Disinfect ✓ Delete if disinfection fails			
Web Anti-Virus				
IM Anti-Virus				
Firewall				
Network Attack Blocker				
System Watcher				
Advanced Settings	,			
Help	OK Cancel		<u>A</u> pply	



#### Mail Anti-virus

در این بخش نیز Action را در حالت Select action می گذاریم و قفل ها نیز به حالت بسته باقی می ماند در قسمت setting نیز می توانید یک سری تنظیمات را بنا به نیازتان customize کنید.

به طور مثال ممکن است یک سری فایل های آلوده به همراه ایمیل ها وارد شبکه ی شما شوند، برای جلوگیری از آلودگی سیستم ها می توانیم در تب Attachment filter یکسری تنظیمات را روی این ایمیل ها اعمال نمایید.برای اینکار روی گزینه ی setting کلیک نمایید و در پنجره ای که باز می شود وارد لبه attachment filter شوید.

General Attachment filter Additional	
Disable <u>filtering</u>	
<u>     R</u> ename specified attachment types	
Delete specified attachment types	
*.asp	*
🔲 *.bat	=
🔲 *.bin	
🔲 *.chm	
📃 *.da	
*.cmd	
*.com	
*.cpl	
*.doc	
🕂 Add 🖉 Edit 💥 Delete	-

با انتخاب گزینه ی Disable filtering ، هیچ Filtering روی ایمیلها اعمال نمی شود.

همچنین با انتخاب گزینه ی Rename specified attachment type ، در صورت دریافت ایمیلی همراه ایمیاه Script ی با پسوند های انتخاب شده در لیست ، این پسوند تغییر نام خواهد داد (در واقع فایل ویروسی همراه ایمیل، دارای Script ی است که پس از Rename شدن قادر به اجرا نمی باشد.)

در صورتی که بخواهید Attachment ی با پسوند های خاصی هنگام دریافت به صورت اتوماتیک Delete شوند می توانید delete با انتخاب گزینه ی Delete selected attachment types و انتخاب پسوند های مورد نظر از لیست مربوطه آنها را delete کنید.



🔀 Mail Anti-Virus		×
General Attachment filter Additional		
Disable <u>filtering</u>		
Rename specified attachment types		
Delete specified attachment types		
*.asp		*
▼ *.bat		
▼ *.bin		
🔲 *.chm		
🔲 *.da		
▼ *.cmd		
✓ *.com		
*.cpl		
*.doc		
🕂 Add 🖉 Edit 💥 Delete		-
Help	ОК	Cancel

#### Web Anti-virus

برای Web آنتی ویروس Action را به حالت Block می گذاریم و در قسمت setting می توانیم URL های Trust می توانیم URL می مورد نظر خود را مطابق نمونه تعریف کنیم.



برای اینکار وارد قسمت settings شوید ووارد تب Trusted URLs شوید و مطابق نمونه URL مورد نظر خود را وارد کنید.

K Web Ant	i-Virus			×
General	Trusted URLs			
Web Ant	ti-Virus does not scan web traffic from	trusted web reso	ources.	
<b>☑</b> <u>D</u> o 1	not scan web traffic from trustee	i URLs:		
-∰- Ar	<b>dd</b> 🖉 Edit 💥 Delete			
	K Address / Address mask		×	
	1			
	Example: *.kaspersky.com/*			
	Help	OK	Cancel	
Help			ОК	Cancel

#### **IM Anti-Virus**

این Component ترافیک های ورودی و خروجی مربوط به Messenger های Component ترافیک های ICQ, MSN, AIM, Mail.Ru مای می کند. Agent, IRC را حفاظت می کند.





#### System Watcher

این component یک حفاظت پیشگیرانه در برابر تهدیداتیست که در database آنتی ویروس هنوز نا شناخته است.در واقع این Component با مانیتور کردن فعالیت Application ها داخل سیستم های شبکه، اطلاعات جزیی تری برای سایر Component های آنتی ویروس جهت حفاظتی عمیق تر، فراهم می آورد.

Properties: Kaspersky Endpoint Securit	ty 10 Service Pack 1 Maintenance Release 2 for Windows		×
Sections	System Watcher		
Web Control          Anti-Virus protection          General Protection Settings          File Anti-Virus          Mail Anti-Virus          Web Anti-Virus          IM Anti-Virus          Firewall	<ul> <li>System Watcher</li> <li>General Settings</li> <li>Enable Exploit Prevention (i)</li> <li>Log application activity for the BSS database</li> <li>Do not monitor the activity of applications that have a digital signature</li> <li>Rollback of malware actions</li> <li>Roll back malware actions during disinfection</li> </ul>		
Network Attack Blocker System Watcher Advanced Settings Application Settings Protection Settings Reports and Storages KSN Settings Interface	Proactive Defense Use behavior stream signatures (BSS) On detecting malware activity: Select action automatically		
Policy profiles	OK Cancel	<u>A</u> pply	



#### Firewall

این Component تمامی فعالیت های شبکه را بر اساس قوانین مشخص شده در بخش Firewall rules فیلتر می کند.همچنین بادر نظر گرفتن رنج داخلی شبکه، فعالیت های شبکه را مانیتور می کند.

Properties: Kaspersky Endpoint Sec	curit	y 10 Service Pack 1 Maintenance Release 2 for Windows 🛛 🚽 🗌	×
Sections		Firewall	
Web Control	^	🗹 Firewall 🗎	
Anti-Virus protection		This component filters all network activity according to the specified rules.	
General Protection Settings		Firewall rules	
File Anti-Virus		Settings Configure rules for Application Privilege Control in the operating system.	
Mail Anti-Virus		<u>D</u> -cango	
Web Anti-Virus		Settings Configure rules for network packets and data streams.	
IM Anti-Virus			
Firewall		Available networks	
Network Attack Blocker		Settings Configure settings for network connections.	
System Watcher			
Advanced Settings			
Application Settings			
Protection Settings			
Reports and Storages			
KSN Settings			
Interface			
Policy profiles			
	¥		
Help		OK Cancel Appl	y

در این قسمت شما باید رنج شبکه خود را بعد از نصب Security Center وارد نمایید براین کار در قسمت Available در این قسمت شما باید رنج شبکه خود را بعد از نصب Security Center وارد نمایید براین کار در قسمت Security Center را زده و با زدن دکمه Add پنجره زیر باز خواهد شد به عنوان مثال اگر رنج شبکه شما 192.168.1.25 تا 192.168.1.255 باشد برای وارد کردن اطلاعات به صورت زیر اعمال نمایید

🔏 Network con	nection
Name:	192.168.1.x
Status:	l ocal network 🔹
IP address:	192.168.1.0/24
For example:	1.2.3.4(/24), 1234::cdef(/96)
Help	OK Cancel



#### **Network Attack Blocker**

این component ازشبکه شما دربرابرحملات داخلی و خارجی که ممکن است برای سیستم های شبکه خطرناک باشد، حفاظت می کند.

Properties: Kaspersky Endpoint Secur	ity 10 Service Pack 1 Maintenance Release 2 for Windows	_		$\times$
Sections	Network Attack Blocker			
Web Control	Network Attack Blocker 🖷			
Anti-Virus protection General Protection Settings File Anti-Virus Mail Anti-Virus Web Anti-Virus IM Anti-Virus	Kaspersky Endpoint Security 10 for Windows detects and defends your comactivity and attacks that could be dangerous.         Network Attack Blocker settings         Add the attacking computer to the list of blocked computers for         Exclusions         Configure addresses of exclusions	nputer agains	network	
Firewall Network Attack Blocker System Watcher				
Application Settings Protection Settings Reports and Storages KSN Settings				
Policy profiles				
<u>Help</u>	OK Can	ncel	<u>A</u> pply	



#### **Application Setting**

این قسمت مربوط به تنظیمات آنتی ویروس می باشد، به طور مثال با فعال کردن گزینه ی Allow management of این قسمت مربوط به تنظیمات آنتی ویروس می باشد، به صورت Task ،Local های Update و Scan آنتی ویروس خود را مدیریت کند.

Properties: Kaspersky Endpoint Sector	rity 10 Service Pack 1 Maintenance Release 2 for Windows		×
Sections	Application Settings		
Web Control Anti-Virus protection General Protection Settings File Anti-Virus Mail Anti-Virus Web Anti-Virus IM Anti-Virus Firewall Network Attack Blocker System Watcher	<ul> <li>Self-Defense Settings</li> <li>Enable Self-Defense</li> <li>Disable external management of the system service</li> <li>Operating mode</li> <li>O not start scheduled tasks while running on battery power</li> <li>Concede resources to other applications</li> <li>Allow local tasks to be displayed and managed (except custom scan)</li> <li>Allow management of group tasks</li> <li>Use Kaspersky Security Center as proxy server for activation</li> <li>Enable dump writing</li> <li>Send dump and trace files to Kaspersky Lab for analysis</li> </ul>		
Advanced Settings Application Settings Protection Settings Reports and Storages KSN Settings Interface Policy profiles	Proxy Server Settings       Settings,     Address is defined automatically, port 80		
<u>Help</u>	OK Cancel	<u>A</u> pply	



#### **Reports and storages**

این قسمت از آنتی ویروس مربوط به تنظیمات گزارش گیری آنتی ویروس ونحوه ی ذخیره سازی آن می باشد.

Properties: Kaspersky Endpoint Securit	ty 10 Service Pack 1 Maintenance Release 2 for Windows 🛛 🗌 🗙
Sections	Reports and Storages
Web Control	
Anti-Virus protection	Store reports to longer than 30 day(s)
General Protection Settings	
File Anti-Virus	
Mail Anti-Virus	I■ – Quarantine and Backup
Web Anti-Virus	Store objects no longer than $30 \clubsuit$ day(s)
IM Anti-Virus	Maximum storage size: 100 MB
Firewall	
Network Attack Blocker	
System Watcher	About files in Backup
Advanced Settings	∠ About unprocessed files
Application Settings	About vulnerabilities found
Protection Settings	About installed devices
Reports and Storages	About started applications
KSN Settings	✓ About file encryption errors
Interface	Send the "Databases out of date" notification if databases
Policy profiles	were not updated 3 day(s)
~	Send the "Databases extremely out of date" notification if databases were not updated day(s)
Help	OK Cancel Apply



#### **KSN Setting**

یک سرویس جهانی است در جهت فراهم آوردن پاسخی فوری به تهدیداتی که ممکن است شبکه ی شما را مختل کند. در واقع این سرویس میلیون ها کاربر را در سطح جهان دور هم گردآوری می کندو زمانی که آنتی ویروس اطلاعات مشکوک یا تایید نشده ای را بر روی یک کامپیوتر عضو KSN شناسایی می کند این اطلاعلت به سرعت برای لابراتوار شناسایی ویروس ها فرستاده می شود.

Properties: Kaspersky Endpoint Sec	curit	y 10 Service Pack 1 Maintenance Release 2 for Windows		_		×
Sections		KSN Settings				
Web Control	^	KSN Settings				
Anti-Virus protection		Kaspersky Security Network (KSN) is a global service that pro	vides instant respo	nse to th	reats and	brings
General Protection Settings		together millions of users worldwide. When the application de computer of a KSN member, this information is instantly relay	etects suspicious or ed to the Virus Lab.	unverifie	d data on	the
File Anti-Virus		- KSN Settings				
Mail Anti-Virus		A Your participation in KSN will improve the chances of	detecting new and	sophistica	ated threa	ts
Web Anti-Virus		and their sources, as well as targeted attacks.				
IM Anti-Virus		✓ I accept the KSN Statement and participation terms	KSN Participation	Statemer	<u>nt</u>	
Firewall		KSN service: Global KSN				
Network Attack Blocker		Application Startup Control	<ul> <li>File Anti-Virus</li> </ul>			
System Watcher		Application Privilege Control	Web Anti-Virus			
Advanced Settings		System Watcher	<ul> <li>Mail Artu-virus</li> </ul>			
Application Settings		Use KSN to check URLs. Used by components:				
Protection Settings		Web Anti-Virus     IM Anti-Virus				
Reports and Storages		- Web Control				
KSN Settings		KSN Proxy Settings				
Interface		Use KSN Proxy				
Policy profiles		Use KSN servers when KSN Proxy is not available				
	¥					
<u>Help</u>		ОК	Cancel		<u>A</u> pply	



موفق باشید پشتیبانی فنی شرکت ایدکو