KASPERSKY SECURITY CENTER 10 Proof of Concept Deployment Guide

Introduction

Kaspersky Security Center 10 offers the ability to manage multiple operating systems and device types in one integrated platform. The security administrator can manage the all Windows Desktops and Servers, OSx, Linux, Novell, VMware, iOS, Android, Symbian and Windows Mobile devices from a single unified console.

This document is intended to provide guidance to successfully test **Kaspersky Security Center 10** and its managed components successfully in a controlled manner.

This guide is divided into five deployment parts:

1. Opening Questionnaire	2
2. Pre-Deployment Checklist	3
3. Security Center Initial Deployment	5
4. Remote Deployment of Kaspersky Endpoint Security for Business	15
5. Group and Policy Recommendations	

Depending on the environment the completion of some of the sections is optional. The mandatory sections have their **installation prerequisites** listed out based on a questionnaire.



1. Opening Questionnaire

This section will be referenced throughout the document. (For ease of use you may want to consider printing it.)

- 1. Approximately how many endpoints (desktops, laptops, servers, virtual machines and mobile devices) need endpoint protection in your environment? (write answer below)
- 2. Which operating systems are you currently running? (circle all that apply)
 - a. Windows XP, Vista, Windows 7, Windows 8, Windows 8.1 (32bit and 64-bit)
 - b. Windows server 2003, 2008, 2008 R2, 2012, 2012 R2 (32bit and 64-bit)
 - c. <u>Mac OSx</u>
 - d. Linux
 - i. Workstations
 - ii. <u>Servers</u>
 - e. Mobile devices: Windows Mobile, Symbian, Blackberry, iOS and Android
- 3. Is your organization in a single location or multiple locations?
 - a. Single location
 - b. If multiple locations
 - i. How many sites are there?
 - ii. Do the sites have VPN or direct connectivity to one another?
 - iii. How fast are the inter-site links?
- 4. What is your domain topology?
 - a. Single domain for all users
 - b. Multiple domains within a forest
 - c. Multiple separate domains
 - d. Workgroups only
- 5. What is the separation of responsibilities?
 - a. One person/team handles endpoint security for my entire organization
 - b. Multiple people/teams handle security for different groups within my organization but we *can* make adjustments to each other's departments if necessary.
 - c. Multiple people/teams handle security for different groups within my organization but we *cannot* make adjustments to each other's departments
- 6. Which endpoint security/antivirus is currently deployed in your environment?
- 7. Do you have remote workers? (skip if no otherwise circle all that apply)
 - a. Do remote workers have VPN connectivity?
 - i. Yes
 - ii. No
 - iii. Mix of Both

2. Pre-Deployment Checklist

Recommended/Example Test Environment

- □ Windows 2008 R2 server with 60-140 GB primary disk and at least 4 GB RAM
- 2 or more non-production Windows physical or virtual machines representative of your environment with at least 1 GB RAM available and 2 GB of disk space. Ideally these are nonproduction machines.

Required Steps:

- □ A server has been allocated with the recommended hardware requirements.
- □ The latest distribution of security center has been downloaded to an accessible location
- □ One or more "test" machines have been allocated for the duration of the proof of concept

Custom Options:

Items within this section relate directly to **Opening Questionnaire** questions:

- 1. You have the option of using the included version of SQL Server Express or an existing SQL Server instance. The included version will scale to support approximately 1,500 users, depending on transaction activity. If your environment is near or exceeds this number you will need to create an instance of SQL in your environment. Optionally, you may still offload the SQL process in a sub 1,500 user environment to reduce resource usage on your Security center server:
 - □ Use Included SQL Server Express
 - □ Offload database to existing SQL Server
 - i. Requires SQL or Windows access to an existing database
 - ii. The database has TCP/IP communication available
 - iii. SQL browser is turned on for the remote database or the server name and instance is known
- 2. Additional Kaspersky Endpoint Protection downloads:
 - □ a. no action required
 - □ b. <u>Download Windows Server Enterprise Edition</u>
 - i. Recommended for Citrix, terminal servers, back-up servers or any server where performance optimization is desired.
 - ii. Kaspersky Endpoint Security 10 for Windows is also compatible with these server operating systems and includes additional functionality: firewall, vulnerability monitor, application privilege control and network attack blocker.
 - □ c. <u>Download Kaspersky Endpoint Security for Mac</u>
 - i. Download Mac network agent
 - □ d. Download Kaspersky Endpoint 8 Security for Linux
 - i. Please note supported operating systems and required components in systems requirements section
 - ii. Download Linux network agent



- □ f. <u>Download Kaspersky Security 10 for Mobile</u>
- g. Extract all downloaded files to an accessible location
- 3. Site survey
 - $\hfill\square$ No action required at this time
- 4. Domain topology
 - $\hfill\square$ a. POC tester has domain admin privileges
 - □ b. The security center server can be installed within the top level domain
 - □ c. The POC tester or testers know the IP subnets of the individual domains and have administrative credentials to each of them
 - □ d. Shared folder access can be achieved from the Security Center server to the workgroup machines
- 5. Separation of responsibilities
 - □ a. No action required
 - □ b. (optional) other groups may wish to <u>download</u> and install the MMC console to manage the Security Center server remotely.
 - □ c. Each organization has procured a Security Center server, database, installation packages and test machines for the POC.
- 6. While a rare occurrence, some incompatible applications cannot be removed via Kaspersky's remote uninstallation utility. A list is provided <u>here</u>
- 7. Remote Users
 - □ a. Remote users can log on during a test deployment
 - $\hfill\square$ b. Approximately 500 MB of files can easily be transferred to a remote user for testing
 - $\hfill\square$ c. I can satisfy the requirements of a and b.



3. Security Center Initial Deployment

Security Center is Kaspersky's central management platform. Updates, reporting, and deployment throughout your IT environment are all handled through this single console. This section will guide you through a custom installation step-by-step.

- 1. Security Center server preparation
 - a. For stability reasons, it is recommended the Security Center server should be assigned **a static IP address** to avoid name resolution issues
 - b. If the server will be part of a domain, or top level domain if you are running a forest, please do so prior to installing the software

If you have a **single location**, are running or managing only Windows operating systems, and have fewer than 250 machines to manage, click through the typical installation and skip to the next section: **Initial Configuration and Deployment to Client Devices**

- 2. Installing Security Center
 - a. Welcome Screen:



b. Accept the End User License Agreement:



c. Select Custom Installation:



d. If you plan to manage mobile devices or integrate with Cisco NAC, select the relevant modules:

Kaspersky Security Center	r Administration Ser	ver	
Custom Setup			
Select the application fea	tures you want installed	d.	
E- Administration Serve	er		
Network Access	Control	tion Conver	
	Support	ation Server	
Administration Server mana Server is required to run thi This component requires 61	ges Kaspersky Lab appl s component. .9 MB free space on the	ications. An instance o hard disk.	f Microsoft SQL
Location:			Select
C: \Program Files (x86) \Kasp	ersky Lab Kaspersky Se	ecurity Center\	
HG 2013 Kaspersky Lab 240,	All Rights Reserved,		-
	< Back	Next >	Cancel
	01		1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -

e. Choose the size of your environment:

Kaspersky Security Center	Administration Ser	ver	
Network Size			
Specify network size.			
Select the approximate nur information will be used to able to edit these settings	nber of computers that configure Kaspersky Se ater.	you are planning to m curity Center properly	anage. This . You will be
C Fewer than 100 compu	ters in the network		
• From 100 to 1,000 com	puters in the network		
C From 1,000 to 5,000 co	mputers in the network	k	
C More than 5,000 compu	Iters in the network		
G 2012 Karperdul ak 750	SII Diabte Deserved		
G 2010 Kasperský Lab 2AO, A	in Rights Reserved.		1 1
	< Back	Next >	Cancel

Allow Security Center setup to create an administrative account or select an existing administrator from Active Directory:

Kaspersky Security Center A	dministration Serv	/er	
Account			
Select the user account to s	tart the Administratio	n Server service.	
Assign an account to start A administrator permissions to	dministration Server s edit the Administratio	ervice. The account n Server database.	musthave
C KL-AK-F4708E14E1F638			
User account			
Account:	kladmin@klder	mo.net	Select
Password:	********		
Confirm password:	*********		
—© 2013 Kaspersky Lab ZAO, All I	Rights Reserved.		
	< Back	Next >	Cancel

Select the type of database to be used:



Select a local or remote instance of SQL:

onnection settings		
Specify Microsoft SQL Serv	er parameters.	
Select the computer that h	osts SQL Server.	
Install Microsoft SQL Se	rver 2008 R2 Express SP2 (Re	commended)
C Choose existing		
SQL Server name:	Γ	Select
Database name:	KAV	
013 Kaspersky Lab ZAO. Al	Rights Reserved	
	(P-d) []	Control 1

For environments larger than 1,500 endpoints, or if you wish to conserve resources, select **Choose existing** and select a database:

Kaspersky Security Center A	dministration Ser		
Connection settings			
Specify Microsoft SQL Serve	er parameters.		
Select the computer that he	osts SQL Server.		
C Install Microsoft SQL Se	rver 2008 R2 Express	SP2 (Recommended)	
 Choose existing 			
SQL Server name:	SC 10]	Select
Database name:	KAV		
—© 2013 Kaspersky Lab ZAO, All	Rights Reserved.		
	100 C 100		The second se



Select SQL authentication mode:

spersky Security Center	Administration Se	rver	
SQL Authentication Me	ode		
Choose Authentication Mo	ode.		
Choose the authentication you select SQL Server Au	n mode you want to u thentication, enter th	se to connect to Micros e account and confirm	oft SQL Server. If the password.
Microsoft Windows Au	thentication Mode		
C SQL Server Authentica	ation Mode		
Account:			
Password:	Γ		
Confirm password:	<u> </u>		
) 2013 Kaspersky Lab ZAO, A	All Rights Reserved.		



Kaspersky Security Center will create a networked shared folder for things like standalone installation packages; you can modify the location of that folder here:

Kaspersky Security Center 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	Select
Shared folder name: KLSHARE	
C Select existing shared folder	
	Select
2013 Kaspersky Lab ZAO, All Rights Reserved,	
< Back Next >	Cancel

By default, the Kaspersky Network Agent will communicate over ports 13,000 and 14,000 - you have the option of changing this default:

Kaspersky Security Center Adm	inistration Server	
Connection settings		
Specify settings to connect to A	dministration Server.	
Enter the Administration Ser to 65535.	ver ports. Port numbers must be w	iithin the range of 1
Port number:	14000	
SSL port number:	13000	
—© 2013 Kaspersky Lab ZAO, All Righ	its Reserved.	
	< Back Next >	Cancel

Select how you wish the server to be identified. It is recommended to use a **static IP address** to avoid DNS resolution issues, handle split domain environments, and deploy Kaspersky Security for Virtualization and Mobile Device Management most effectively:

Kaspersky Security Cente	r Administration S	erver	
Administration Server	address		
Specify Administration Se	erver address.		
Set the Administration Se	erver address to one	of the following option	s:
a. DNS name. Used i address of Administration	if a DNS server is pre n Server from it.	sent and client comput	ers can get the
b. NetBIOS name. Us Server via the NetBIOS p	ed if dient computers protocol, or if a WINS	s can get the address o server is present in th	of Administration ie network.
c. IP address. Used o will not be changed in the	only if the Administrat e future.	ion Server has a static	: IP address which
Administration Server ad	dress:		
10.75.83.102		•	
@ 2013 Kaspersky Lab ZAO,	All Rights Reserved.		
	< Back	Next >	Cancel



f. Based on **question #2 of the environment questionnaire**, select application plug-ins to manage Kaspersky applications for non-Windows operating systems:

spersky Security Cente	r Administration Se	rver	ļ	- 🗆
Plug-ins				
Select plug-ins to be inst	alled.			
ist of plug-ins:				
Kaspersky Anti-Viru	s 6.0 for Windows Ser	vers Enterorise Editio	n Console Pluain	
Kaspersky Anti-Viru	s 6.0 for Windows Wo	rkstations MP4 Conso	le Plug-in	
Kaspersky Anti-Viru	s 8.0 MP1/MP2 for Linu	ux File Server Console	e Plug-in	
Kaspersky Anti-Viru	s 8.0 for Windows Ser	vers Enterprise Editio	n Console Plug-in	
Kaspersky Endpoint	Security 10 for Windo	ws Console Plug-in nsole Plug-in		
Kaspersky Endpoint	Security 8 for Smartpl	hone		
Kaspersky Endpoint	Security 8 for Window	vs Console Plug-in		
Kaspersky Endpoint	Security 8.0 for Linux	Console Plug-in		
Kaspersky Security	10 for Mobile			-
Raspersky Security				
2012 Kassovsky Lab 200	All Rights Reserved.			
2010 Kaspersky Lau 240.				

g. Accept End User License Agreements for application plug-ins:

End User License Agreement Please read the following License Agreement care	efully.	
Please read the License Agreement. You must acc the product.	cept the terms of this Agreement to insta	
KASPERSKY LAB END USER LICENSE AGREEMENT	T	
IMPORTANT LEGAL NOTICE TO ALL USERS: CA AGREEMENT BEFORE YOU START USING THE SO	AREFULLY READ THE FOLLOWING LEGAL OFTWARE.	
BY CLICKING THE ACCEPT BUTTON IN THE L ENTERING CORRESPONDING SYMBOL(-S) YOU (AND CONDITIONS OF THIS AGREEMENT, SUC SIGNATURE AND YOU ARE CONSENTING TO PARTY TO THIS AGREEMENT AND AG	LICENSE AGREEMENT WINDOW OR BY CONSENT TO BE BOUND BY THE TERMS ICH ACTION IS A SYMBOL OF YOUR DE BOUND BY AND ARE BECOMING A GREE THAT THIS AGREEMENT IS	
YOU DO NOT AGREE TO ALL OF THE TERMS A CANCEL THE INSTALLATION OF THE SOFTWARE	ATED AGREEMENT SIGNED BY YOU. IF AND CONDITIONS OF THIS AGREEMENT, E AND DO NOT INSTALL THE SOFTWARE.	-
✓ I accept the terms of the License Agreement		
© 2013 Kasperský Lab ZAO, Ali Rights Reserved,		_

Finalize the installation:



Launch Kaspersky Security Center from the Start Menu, and follow the prompts of the Quick Start Wizard. During this process, the initial virus definition database download will begin and will take several minutes to complete, depending on your internet connection speed. At this point, the initial installation of the management is considered to be complete.



4. Remote Deployment of Kaspersky Endpoint Security for Business

When installed, the Network Agent will run a query against the Windows software registry and identify any applications that are not compatible with Kaspersky Endpoint Security 10 for Business. It is important to identify and remove these applications prior to installing Kaspersky.

Requirements for Client Computers:

Necessary Firewall Ports are open: TCP: 139, 445 UDP: 137, 138 or Firewall is turned off.

Phase 1: Deploy the Network Agent

Step 1: Go to the "Tasks" tab in the "Managed Computers" group or to the desired sub-group and create a new task.

Kaspersky Security Center					X
File Action View Help					
🗢 🤿 🖄 📅 🗈 🗐 💁 🖉 🖬					
Kaspersky Security Center Kaspersky Security Center Administration Server Administration Servers Administration Administration	Groups Policies Group tasks You can use tasks to configure regulation You can use tasks to configure regulation Create a task Upport task from the Refresh	Tasks 2 Com	uputers	from time to time (for example, installation of a	Getting started > Managed computers
Repositories					
				<u> </u>	Show inherited tasks
	Name A	Application	1	< No selected items >	
	Download update	Kaspersky Endpoint Security 10 for			
	Find vulnerabilities and applicati	Kaspersky Security Center Network			
	Virus Scan	Kaspersky Endpoint Security 10 for			
a] []]					
Groups: 0, computers: 1	1		19		



Step 2: Name your Task, and then click next to move on.

🔜 Ne	w task wizard	×
\bigcirc	New task wizard	
	Defining task name	
	Name:	
	Step 1 Deploy Network Agent	
	Next	ancel

Step 3: Choose "Install Application Remotely", and then click next to move on.

🔜 New	task wizard	x
0	New task wizard	
9	Select task type	
	Image: Second Secon	
	Next Cancel	

Step 4: Choose the Network Agent Installation Package from the list and then click next to move on.

task wizard		x
New task wizard		
electing installation package		
Kaspersky Endpoint Security 10 for Windows (10.1.0.867)		
Kaspersky Security Center Network Agent (10.0.3361)		
Caspersky Security Center Network Agent (10.0.3361)		
	New	
	Next Ca	ncel
	task wizard New task wizard electing installation package Kaspersky Endpoint Security 10 for Windows (10.1.0.867) Kaspersky Security Center Network Agent (10.0.3361) Gaspersky Security Center Network Agent (10.0.3361)	task wizard New task wizard electing installation package Kaspersky Endpoint Security 10 for Windows (10.1.0.867) Kaspersky Security Center Network Agent (10.0.3361) Gaspersky Security Center Network Agent (10.0.3361) New

Step 5: Choose how to upload the package to your clients. You will want uncheck "Using Network Agent" if you do not already have a network agent installed on the client. Click next to move on.

w	task wizard New task wizard
5	ettings
	Force download of the installation package
	Using Network Agent
	Using Microsoft Windows resources by means of Administration Server
	Osing Microsoft Windows resources by means of opdate Agents
	☑ Do not install application if it is already installed
	Assign the package installation in the Active Directory group policies
	Closing running applications before installation starts
-	

Step 6: A reboot is NOT required after the agent is installed. Choose the "Do not restart the computer" option and then click next to move on.

-
-

Step 7: Please enter in Credentials with local Administrative Rights. If this is left blank, the Security Center will use the default account that was assigned to it during installation.

🔜 New	r task wizard	X
0	New task wizard	
	Selecting account to start the task	
	List of user accounts to be used to run the task. Accounts will be	selected in the order listed.
		Learn more
		Add
		Properties
		_
		×
		Next Cancel

Step 8: Choose the schedule you want to start the deployment. Manually is usually used for the first step.

New task wizard	
Configure task scheduling settings	
Scheduled start: Manually	
Rup missed tasks	
) Run misseu tasks	
Define task launch delay automatically	
 Randomize the task start with interval (min); 	1 =
 Randomize the task start with interval (min); 	1

Step 9: Leave the option to "Run task after Wizard completion" unchecked and click Finish to complete the wizard.

New task wizard
ishing creation of the task
lick the Finish button to create "New task" and complete the Wizard.
Run task after Wizard completion
Finish Cancel



Phase 2: Remove your old Antivirus

Step 1: Go to the "Tasks" tab in the "Managed Computers" group or to the desired sub-group and create a new task.

Kaspersky Security Center					_ 8	
File Action View Help						
🗢 🔿 🖄 📅 📋 🖻 🧟 📝 🖬						
Kaspersky Security Center	Groups Policies	Tasks 2 Com	puters			
Managed computers 1 Administration Servers					Getting started > Managed computers	
□ If Test Group IF (0) Administration Servers Administration Server tasks Tasks for specific computers IF (0) Administration Server tasks IF (0) Administration Servertasks <td colspan="6">Group tasks To use tasks to configure regular actions (for example, virus search and update) or actions performed from time to time (for example, installation of a rew version of managed application activation). Create a task 3 in priori task from file in Refresh</td>	Group tasks To use tasks to configure regular actions (for example, virus search and update) or actions performed from time to time (for example, installation of a rew version of managed application activation). Create a task 3 in priori task from file in Refresh					
					Show inherited task	
	Name 🔺	Application		< No selected items >		
	Download update	Kaspersky Endpoint Security 10 for				
	Find vulnerabilities and applicati	Kaspersky Security Center Network				
	Step 1 Deploy Network Agent	Kaspersky Security Center Administr				
	Virus Scan	Kaspersky Endpoint Security 10 for				
<						
Groups: 0, computers: 1						

Step 2: Name your Task, and then click next to move on.

🔜 Nei	w task wizard	×
\bigcirc	New task wizard	
	Defining task name	
	News	
	Step 2 Remove Old AntiVirus	
]	Next Cancel



Step 3: Expand the Advanced container and select "Uninstall application remotely", then click next to move on.



Step 4: Choose "Uninstall incompatible application".

🔜 Ne	ew task wizard	×
\bigcirc	New task wizard	
	Select application to be removed	
	Uninstall application supported by Kaspersky Security Center	
	Uninstall incompatible application	
	Uninstall application from applications registry	
	Remove specified update for application	
	NextCano	el

Step 5: Choose Add to select the removal scripts you need.

💷 New	task wizard New task wizard	×
5	ettings	
	Application to be removed:	
		Add Delete
		Next Cancel

Step 6: Select the Scripts you need. You can select multiple scripts at once by holding down CTRL or Shift as you select from the list. Choose OK when you are finished. Note: If you do not see your Antivirus product on the list or if it fails to remove your product, please contact your Systems Engineer or our Corporate Support Team.



Step 7: Make sure the scripts you wanted are on the list to be removed, and then choose next to move on.

Application to be removed: Acer LANScope Agent 2.2.25.84 Acer LANScope Agent 2.2.25.84 x64 Adaptive Security Analyzer 2.0 AdAware 7-8 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		New task wizard		
Application to be removed: Acer LANScope Agent 2.2.25.84 Add Acer LANScope Agent 2.2.25.84 x64 Adaptive Security Analyzer 2.0 AdAware 7-8 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Personal Firewall 4.0.0.1305 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK	50	ettings		
Acer LANScope Agent 2.2.25.84 Acer LANScope Agent 2.2.25.84 x64 Adaptive Security Analyzer 2.0 AdAdaware 7-8 AEC TrustPort Netivirus 2.8.0.2237 AEC TrustPort Personal Firewall 4.0.0.1305 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		Application to be removed:		
Acer LANScope Agent 2.2.25.84 x64 Adaptive Security Analyzer 2.0 AdAdware 7-8 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Personal Firewall 4.0.0.1305 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		Acer LANScope Agent 2.2.25.84	_	Add
Adaptive Security Analyzer 2.0 AdAware 7-8 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Antivirus 2.8.0.237 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		Acer LANScope Agent 2.2.25.84 x64		
AdAware 7-8 AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Antivirus 2.8.0.2237 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		Adaptive Security Analyzer 2.0		Delete
AEC TrustPort Antivirus 2.8.0.2237 AEC TrustPort Personal Firewall 4.0.0.1305 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		AdAware 7-8		
Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 X64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		AEC TrustPort Antivirus 2.8.0.2237		
Agnitum Outpost Antivirus Pro 6 Agnitum Outpost Antivirus Pro 6 x64 Agnitum Outpost Firewall 1.0 Agnitum Outpost Firewall 1.0 SDK		AEC TrustPort Personal Firewall 4.0.0.1305		
Agnitum Outpost Antwirus Pro 6 X64		Agnitum Outpost Antivirus Pro 6		
Agnitum Outpost Firewall 1.0		Agnitum Outpost Antivirus Pro 6 x64		
Agritum Outpost Frewail 1.0 SDK		Agnitum Outpost Firewall 1.0	-	
		Carlos Agritum Outpost Pirewaii 1.0 SDK		
				Next Cance

Step 8: A reboot is usually required after this step to fully remove most old Antivirus applications. You can either reboot immediately after the uninstall or prompt the user for action. Choose next to continue.

Ne	w task wizard	X
•	New task wizard	
	Selecting operating system restart option	
	Select the action that will be performed if application uninstallation requires an operating system restart.	
	C Do not restart the computer	
	C Restart the computer	
	Prompt user for action	
	Uninstallation completed. Your operating system must be restarted to finish the uninstallation.	
	Repeat prompt every (min):	
	Restart after (min):	
	Force closing the applications in blocked sessions	
	Next Cance	

Step 9: Add credentials with local administrative rights for the targeted computers. By default the task will be run through the Network Agent using the local system service account, so credentials may not be needed.



Step 10: Schedule when you want the task to start. To have it run automatically after the deployment of the Network Agent, you can choose to do so as seen below. When finished, choose next to continue.

New task wizard	
Configure task scheduling settings	
Scheduled start: On completing another task	•
Task name:	
Step 1 - Deploy Network Agent Select]
Execution result:	
Completed successfully	1
	1
Run missed tasks	
Run missed tasks Define task launch delay automatically	
Run missed tasks Define task launch delay automatically Randomize the task start with interval (min):	1 12
Run missed tasks Define task launch delay automatically Randomize the task start with interval (min):	1
 Run missed tasks Define task launch delay automatically Randomize the task start with interval (min): 	1 2
Run missed tasks Define task launch delay automatically Randomize the task start with interval (min):	1

Step 11: Leave the option to "Run task after Wizard completion" unchecked and click Finish to complete the wizard.





Phase 3: Deploy Kaspersky Endpoint Security 8 to you Computers

Step 1: Go to the "Tasks" tab in the "Managed Computers" group or to the desired sub-group and create a new task.

Kaspersky Security Center			X
File Action View Help			
🗢 🔿 📶 🗖 🖾 🙆 🖬			
Kaspersky Security Center	Groups Policies	Tasks Computers	
Managed computers			Getting started > Managed computers
Bergensensensensensensensensensensensensense	Group tasks Tou can use task to configure regul a new vestion of managed applicatio Contrast task Controor task from file Refeat	er actions (för example, virus search and update) or nor application activation).	ectors performed from time to time (for example, installation of
			C Show inherited tasks
	Name *	Application	Step 1 - Deploy Network Agent
	Download update	Kaspersky Endpoint Security 10 for	Task type: Install application remotely
	Find vulnerabilities and applicati	Kaspersky Security Center Network	Application: Kaspersky Security Center Administration Server
	Virus Scan	Kaspersky Endpoint Security 10 for	Appled to 0 computers
	Step 1 Deploy Network Agent	Kaspersky Security Center Administr	Ready for execution on 1 computers
	Step 2 Remove Old AntiVirus	Kaspersky Security Center Administr	Plande for Gompaters Plande for Gompaters Compater 0 compaters Retars in equation 0 compaters Bacande error of compaters
			View results
×	1		Task execution
Groups: 0, computers: 1			

Step 2: Name your Task, and then click next to move on.

🔜 Nev	w task wizard		X
\bigcirc	New task wizard		
	Defining task name		
	Name:		_
	Step 3 Deploy KES 10		
		Next	Cancel



Step 3: Choose "Install Application Remotely", and then click next to move on.



Step 4: Choose the Endpoint Security Installation Package from the list and then click next to move on.

🔜 Ne	w task wizard	×
0	New task wizard	
	Selecting installation package	
	Kaspersky Endpoint Security 10 for Windows (10.1.0.867)	
	Kaspersky Security Center Network Agent (10.0.3361)	
	Kaspersky Endpoint Security 10 for Windows (10.1.0.867)	
	New	
	Next Can	cel

Step 5: You can bundle the Network Agent with the install of Endpoint Security, however, we have already done this with the first task, so you can skip it.

🔜 Nev	v task wizard	×
Θ	New task wizard	
	Advanced	
	Install Network Agent along with this application	
	Select Network Agent installation package for combined installation:	
	Name Kaspersky Security Center Network Agent (10.0.3361)	
	Create	
	Next	Cancel

Step 6: Choose how to upload the package to your clients. Defaults are fine in most cases, but it is usually a good idea to uncheck the network agent usage because deployment via Windows shares is usually quicker. Click next to move on.



Step 7: A reboot is NOT required after the Endpoint Security Installation. Click next to move on.



Step 8: Add credentials with local administrative rights for the targeted computers. If the default account for the Security Center has local administrative rights, then you can skip this step and click next to continue.



Step 9: Schedule when you want the task to start. To have it run automatically after the deployment of the Network agent, you can choose to do so as seen below. When finished, choose next to continue.

lew	task wizard		
	New task wizard		
C	Configure task scheduling settings		
	Scheduled start: On completing another task		-
	Task name:		
	Step 2 Remove Old AntiVirus Select		
	Execution result:		
	Completed successfully		
	Run missed tasks		
	Define task launch delay automatically		
	Randomize the task start with interval (min):	1	4. 7

Step 10: Leave the option to "Run task after Wizard completion" unchecked and click Finish to complete the wizard.

🔜 Ne	w task wizard	×
Θ	New task wizard	
	Finishing creation of the task	
	Click the Finish button to create "Step 3 Deploy KES10" and complete the Wizard.	
	Run task after Wizard completion	
	Finish Cancel	



Phase 4: Starting and changing the settings on a task after it is created

To start a task, you can either click the Start button as seen below or right click the task and choose start from there.

To change settings on a task, you can choose what you want to do beneath the Start and Stop buttons, or you can right click the task and go to properties.

Kaspersky Security Center					X
File Action View Help					
🗢 🔿 🔰 🖬 📋 🖳 🖓 🖬					
Kaspersky Security Center	Groups Policies	Tasks Co	omputers		
Managed computers Administration Servers					Getting started > Managed computers
Administration Server tasks Administration Server tasks Tasks for specific computers User accounts Der accounts Port and notifications Port and notificati	Group tasks Tou can use tasks to configure regu a new version of managed applicable Create a task Create a task in Import task from file Refresh	lar actions (för example, virus search ar n or application activation).	nd update) or actions perfor	med from time to time (for example, installation of	
				A	Show inherited tasks
	Name A	Application		Step 1 Deploy Network Agent	
	Download update	Kaspersky Endpoint Security 10 for .		Task type: Install application remotely	
	Find vulnerabilities and applicati	Kaspersky Security Center Network .		Application: Kaspersky Security Center Administr	ration Server
	Step 1 Deploy Network Agent Step 2 Remove Old AntiVirus Step 3 Deploy KES 10 Virus Scan	Character Administr Start Stop ter Administr Pause ter Administr Resume urity 10 for . All Tasks			Applied to 0 computers Ready for execution on 1 computers Running on 0 computers Pasad for 0 computers Completed on 0 computers Restant a required on 0 computers Restant and error on 0 computers
		Group by column			View results
		Copy Remove		Task execution	
	1	Export list Properties			
Groups: 1, computers: 1		· · · · · · · · · · · · · · · · · · ·			J. J



5. Group and Policy Recommendations

Organizing your "Managed Computers"

The first step you should take after setting up your Security Center, is organizing your managed computers. In most cases, the best way is to break machines up by Workstations and Servers. This way you can have separate policies and tasks for your servers and workstations.

If you have multiple sites, this also makes it easier to manage them, because you can manage all sites under a single workstation or server policy. If you need different settings for a site, you can also put a policy in that site's folder. This way you can stay organized but allow for scalability and flexibility when managing your clients.



Configuring the default virus scan task

By default, computers are being scanned, however, after 7 days they will turn yellow and warn you they have not been scanned for a long time. After 14 days they will turn red. To change this, add the computer or "My Computer" to the scan scope. This will update the status on client computers once the scan has completed.

Properties: Virus Scan	
Sections	Properties
General Notification Schedule Properties Account Exclusions from task scope	Custom Scan Settings - Security level - Recommended - Optimal protection - Recommended for most users - I - Objects to scan - Objects to scan Settings 2
Scan scope Image: System Memory Image: Startup Object Image: Star	- Run mode - Run mode - Run mo
Help	CK Cancel Apply

Setting exclusions

This next setting involves configuring exclusions that will help with performance



When adding objects to exclude, you can utilize different masks to make your rules more powerful and flexible. Allowed exclusion masks can be found in our knowledgebase article here: http://support.kaspersky.com/fag/?gid=208280713

Typical exclusions to start off with are outlook files such as .pst and .ost files, virtual templates like .ova files, VMware virtual machine disks such as .vmdk files, and lastly if you have installed Kaspersky Endpoint Security 10 on your Security Center Server you should also exclude the Security Center folder we install to. If you have other software you wish to exclude, remember to follow that vendor's recommended exclusions

🔀 Trusted zone	_						
3 Exclusion rules Trusted applications							
Exclusion rules let you specify files or folders and names of objects appearing in the will be excluded from scanning by all or some Kaspersky Endpoint Security 10 for W	e Virus Encyclopedi indows component	a, which ts.					
4 🕂 Add 🖉 Edit 💥 Delete							
File or folder	∇ Object na	ame 🔺					
☑ C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\	*						
Exclusion rule	*						
Properties: V File or folder	*						
Object name	not-a-virus:R not-a-virus:R	emo +					
Comment:		×					
A file or folder is not scanned when the fol							
File or folder select file or folder 5 *.ost 6 Browse							
✓ Indude subfolders							
▲ Folder path must end with "\".							
Нер 7	ОК	Cancel					
Help 8 OK Cancel	Import	Export					
Нер	ОК	Cancel					

Once you have made your exclusion rules, make sure they appear on the list and are checked.

K	Trusted zone
	Exclusion rules Trusted applications
	Exclusion rules let you specify files or folders and names of objects appearing in the Virus Encyclopedia, which will be excluded from scanning by all or some Kaspersky Endpoint Security 10 for Windows components.
	🖞 Add 🖉 Edit 💥 Delete
9	File or folder V Object name
	🗹 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\ *
	▼*.vmdk *
	▼*.pst *
	▼ *.ovf *
	🔽 *.ova *
	🗹 *.ost *
	wwinDir%\SvsWOW64\raddrv.dll not-a-virus:Remo 🝸
	Rule description (dick underlined items to change):
	A file or folder is not scanned when the following conditions are met: File or folder: <u>sost</u> Protection components: <u>any</u>
	Import Export
Hel	D OK Cancel



Optimizing scan and application settings

Next you will want to turn off the scanning of network drives in real time. For smaller businesses with NAS devices this may be okay, however for larger networks with public shares or mounted network drives this is not recommended as it may use up extra bandwidth and resources to scan.

General If File Anti-Virus Events This component resides in RAM, scanning all opened, saved, and active files to ensure maximum protection at all times. Endpoint control Application Startup Control Application Startup Control - Security level Object at control - Oppend contaction Device Control - Oppend contaction Web Control - File Anti-Virus Action on threat de - File types Encryption - Select action a: Select action a: - File scanned by sytemion @ Encryption of files and folders - Object for Encryption of files and folders - Protection scope Encryption of files and folders - Protection scope Anti-Virus protection - Al and drives	Sections	File Anti-Virus
General Protection Settings File Anti-Virus Web Anti-Virus IM Anti-Virus IM Anti-Virus Firewal Network Attack Blocker Heb OK Cancel	General Central Application Startup Control Application Startup Control Application Startup Control Vulnerability Monitor Device Control Web Control Encryption Common encryption settings Encryption of hard drives Encryption of files and folders Encryption of removable drives Anti-Virus protection Settings File Anti-Virus Mail Anti-Virus Prevail Mail Anti-Virus Prevail Network Attack Blocker System Watcher	File Anti-Virus This component resides in RAM, scanning all opened, saved, and active files to ensure maximum protection at all times. Security level

The last fixes are to enable the options to concede resources to other applications and to Perform Idle Scans. Conceding resources allows Kaspersky to automatically suspend scheduled tasks when it detects an increased load on the CPU and it will free up operating system resources for user applications. This helps to relieve the load on the CPU and disk subsystems.

The second option starts a scan task when the computer is locked or the screensaver is on for 5 minutes or longer.



Firewall: Though not very restrictive by default, the Firewall component does initially block Remote Desktop Protocol, as this can be an attack vector for malicious actors. If this is required for remote management in your environment, Click **Firewall** on the left pane of the Policy's Properties window, then click the middle **Settings...** button to open the **Configure network packet rules** window: Right-click under the Permission column on the **Remote Desktop network activity** and choose **Allow**:

Kaspersky Endpoint Security 10 for Windows monitors inbound a rules created by default. You can create a new set of conditions by adding or editing network packet rules.	nd outbound and actions	I network activities by using network pack to take on network packets and data stre	et ams
🖞 Add 🖉 Edit 💥 Delete 🛉 Move up 🌡 Move down		Addition	al
Network service	Permission	n Address	+
Requests to DNS server over TCP	-		
Requests to DNS server over UDP			
Sending e-mails			
Any network activity	~	Trusted networks	
Any network activity		Local networks	
Remote Desktop network activity	C -		
TCP connections through local ports	~ ۷	Allow	
✓ UDP connections through local ports	00	Block	
✓ Incoming TCP stream	T 🐨	According to the application rule	
✓ Incoming UDP stream			
 ICMP Destination Unreachable incoming responses 	v =	Log events	
✓ ICMP Echo Reply incoming packets	~		
✓ ICMP Time Exceeded incoming responses	~		
✓ Incoming ICMP stream	0		
✓ ICMPv6 Echo Request incoming packets	0		
✓ - allowed ⊘ - blocked			

For further detailed administrator information please consult the following documents:

- http://docs.kaspersky-labs.com/english/kasp10.0_sc_gsen.pdf
- http://docs.kaspersky-labs.com/english/kasp10.0 sc admguideen.pdf
- http://docs.kaspersky-labs.com/english/kasp10.0 sc implguideen.pdf

