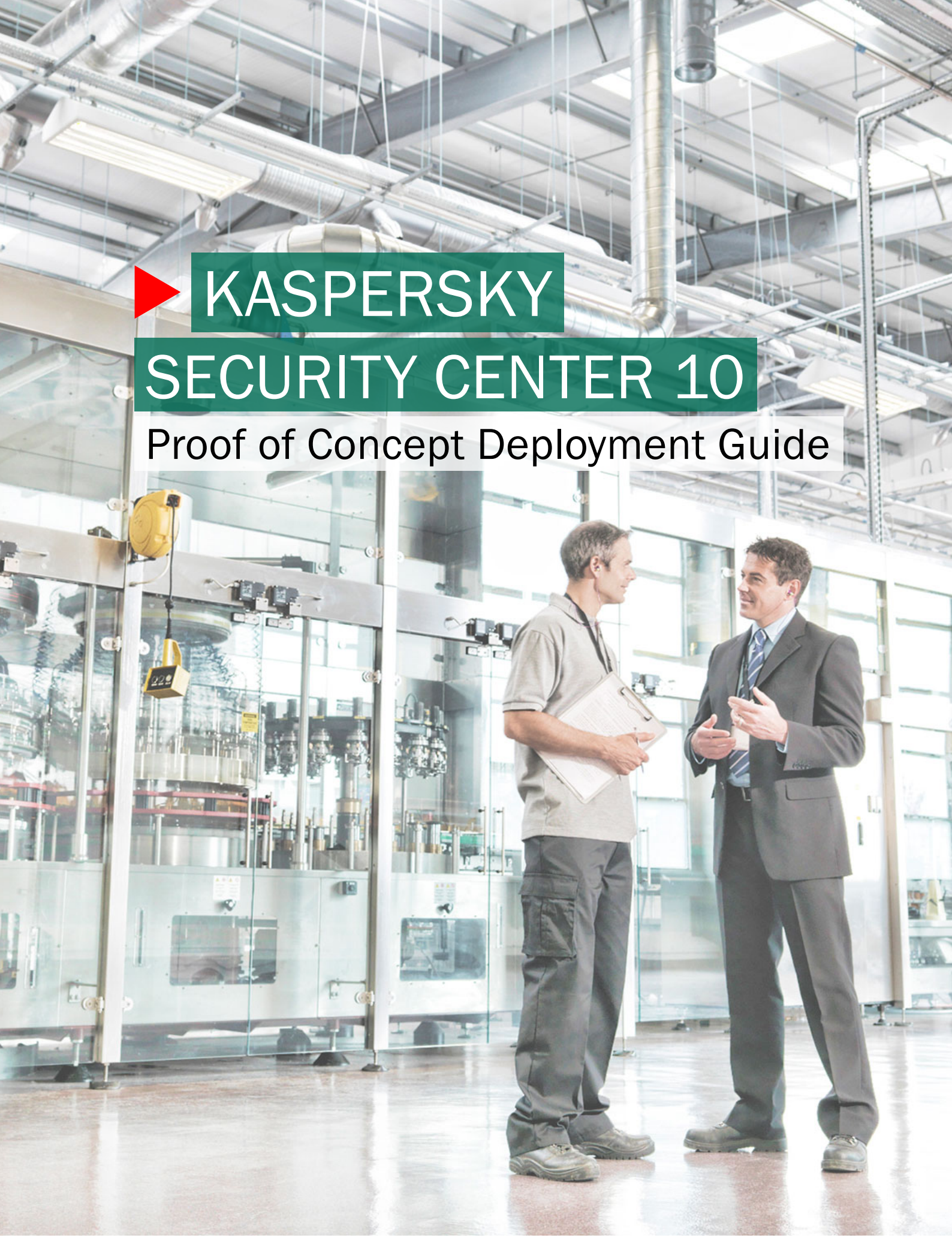


# KASPERSKY SECURITY CENTER 10

## Proof of Concept Deployment Guide

KASPERSKY lab

# 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:**



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. Mac OSx
   d. Linux
      i. Workstations
      ii. Servers
   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 non-production 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. Download Windows Server Enterprise Edition
     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. Download Kaspersky Endpoint Security for Mac
     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. Download Kaspersky Security 10 for Mobile
- ☐ g. Extract all downloaded files to an accessible location

3. Site survey
   - ☐ No action required at this time

4. Domain topology
   - ☐ 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 download 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 here

7. Remote Users
   - ☐ a. Remote users can log on during a test deployment
   - ☐ b. Approximately 500 MB of files can easily be transferred to a remote user for testing
   - ☐ 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

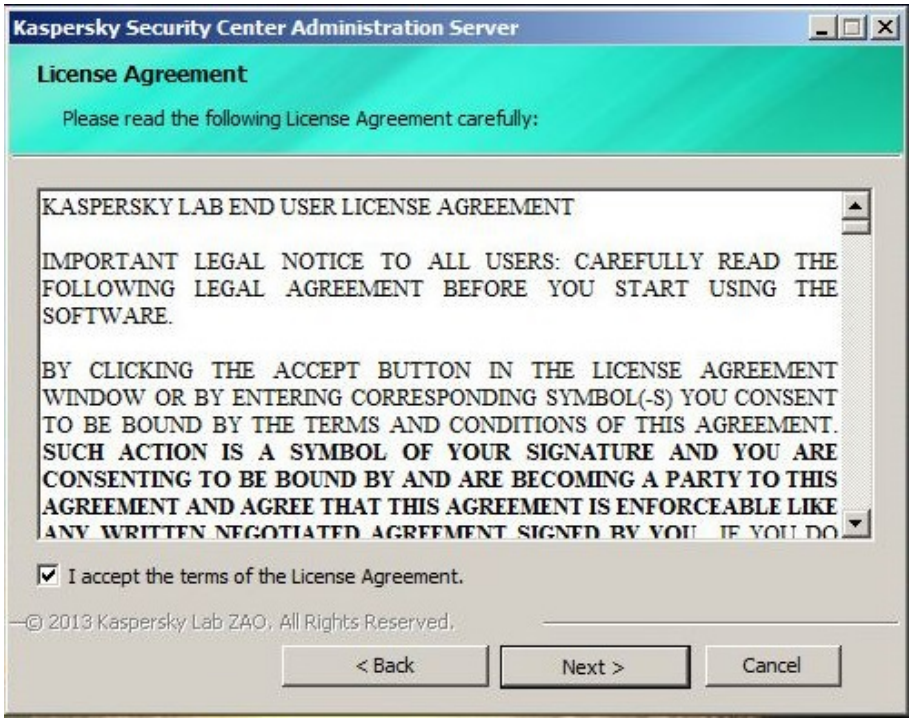
a. For stability reasons, it is recommended the Security Center server should be assigned **a static IP address** to avoid name resolution issues
b. If the server will be part of a domain, or top level domain if you are running a forest, please do so prior to installing the software

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**

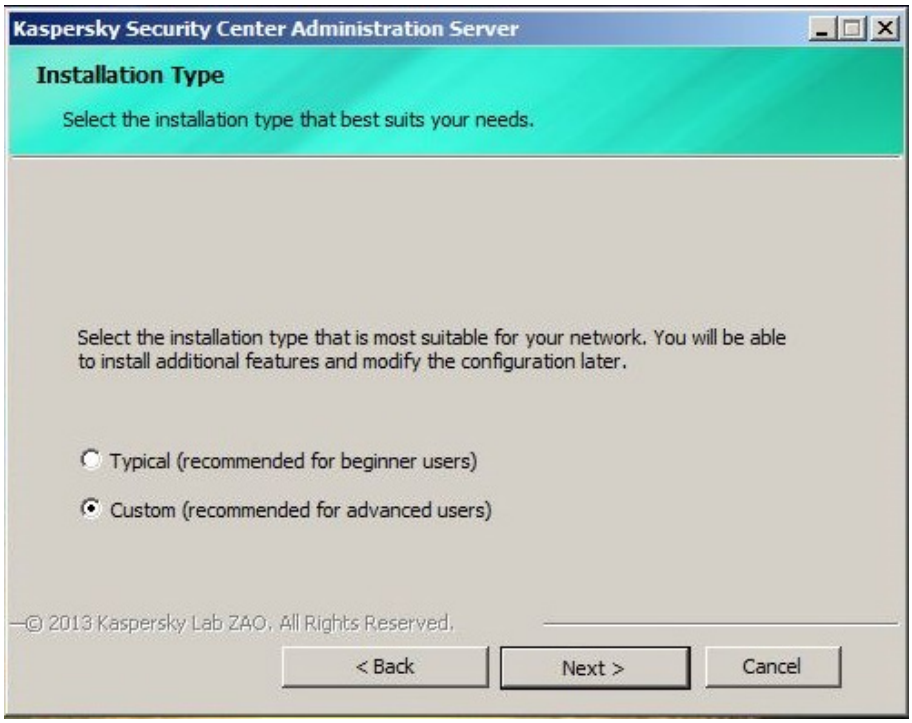
## 2. Installing Security Center

a. Welcome Screen:

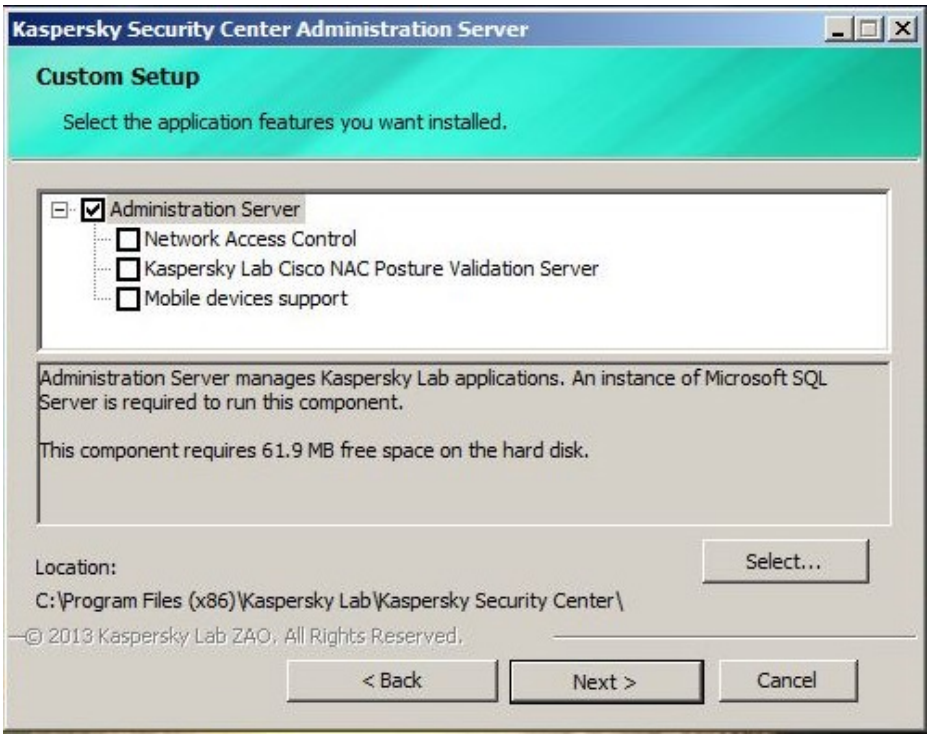
b. Accept the End User License Agreement:




c. Select Custom Installation:



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



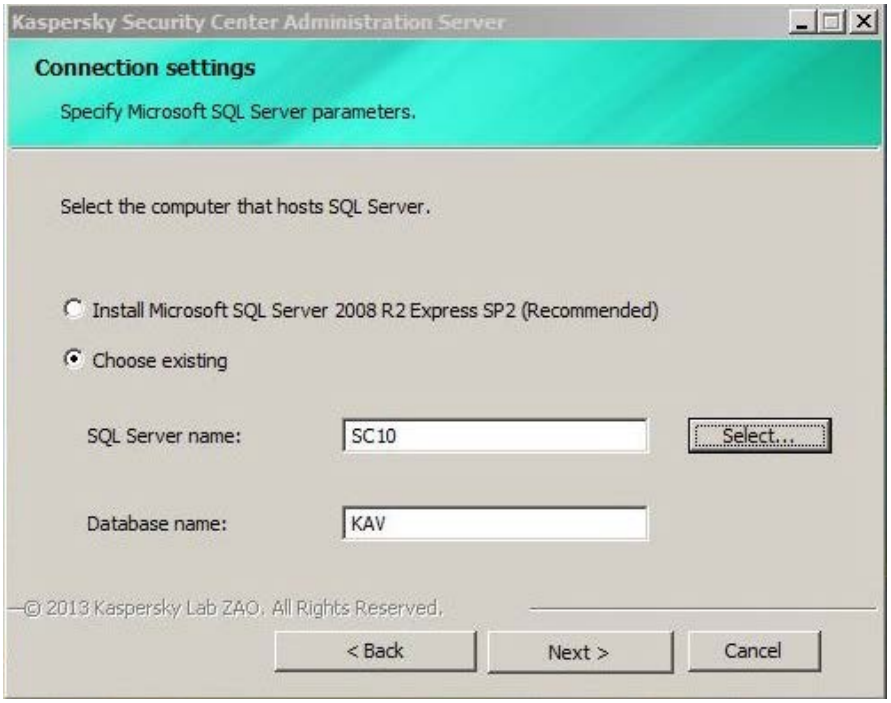

e. Choose the size of your environment:

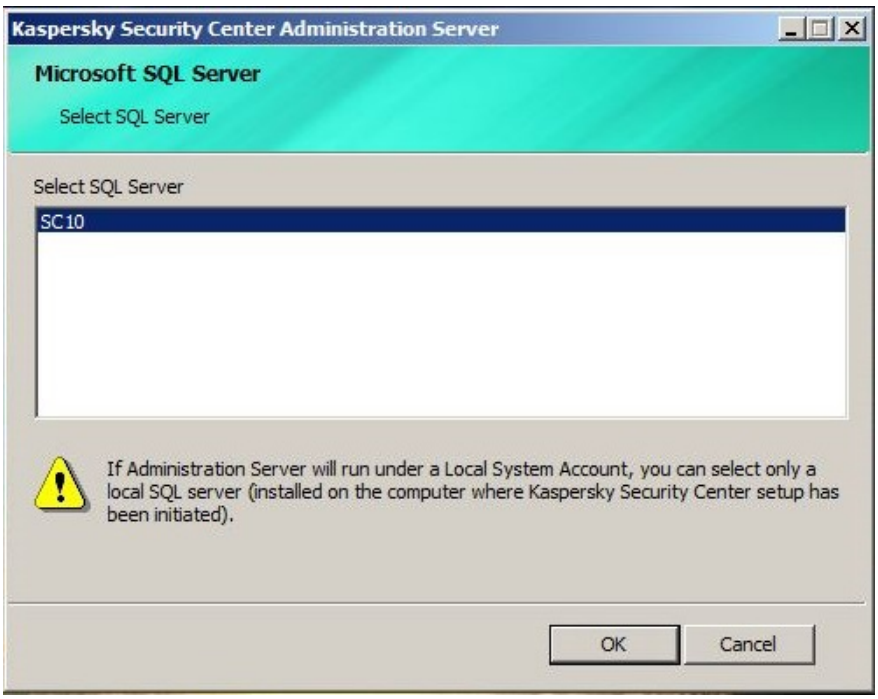
Allow Security Center setup to create an administrative account or select an existing administrator from Active Directory:


Select the type of database to be used:

Select a local or remote instance of SQL:

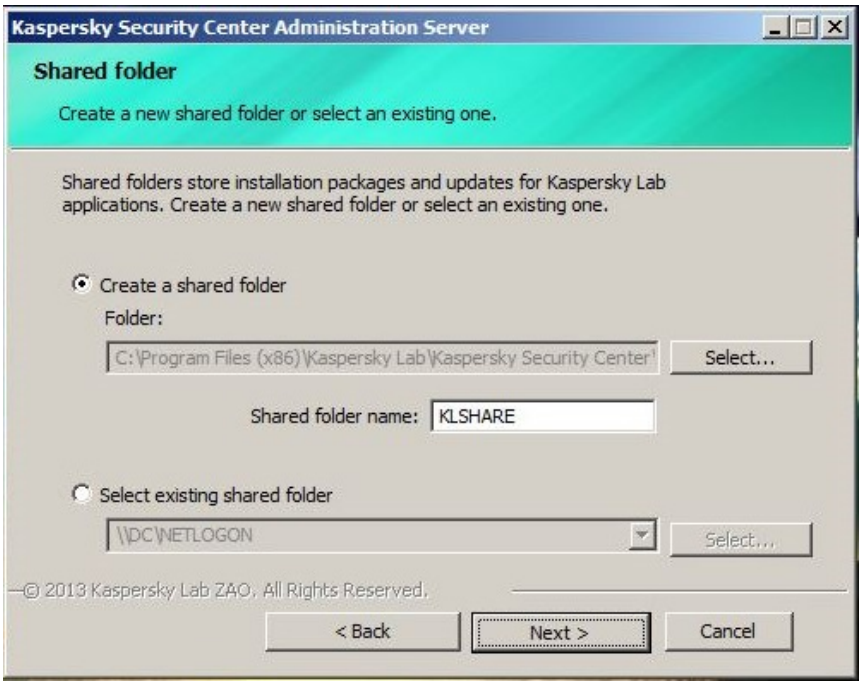

For environments larger than 1,500 endpoints, or if you wish to conserve resources, select **Choose existing** and select a database:



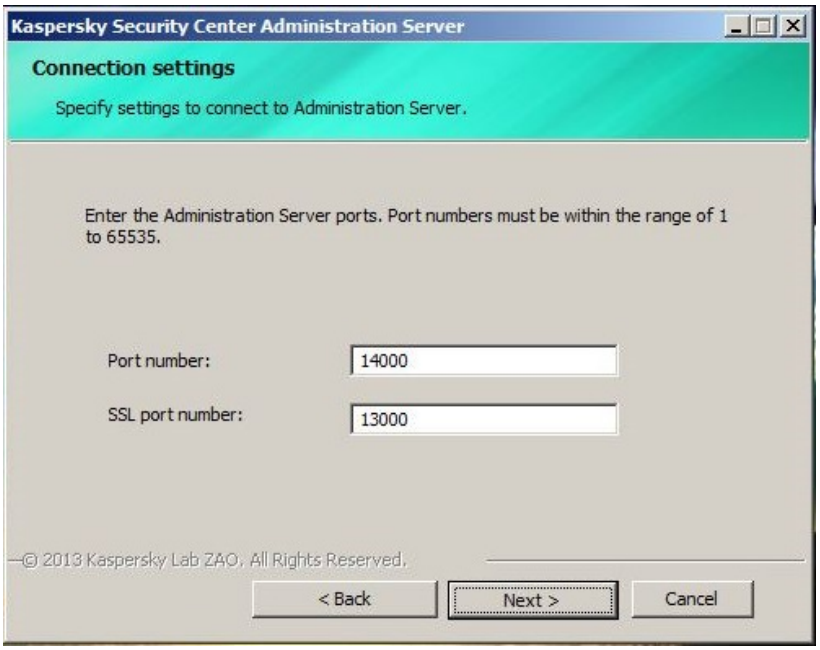



Select SQL authentication mode:

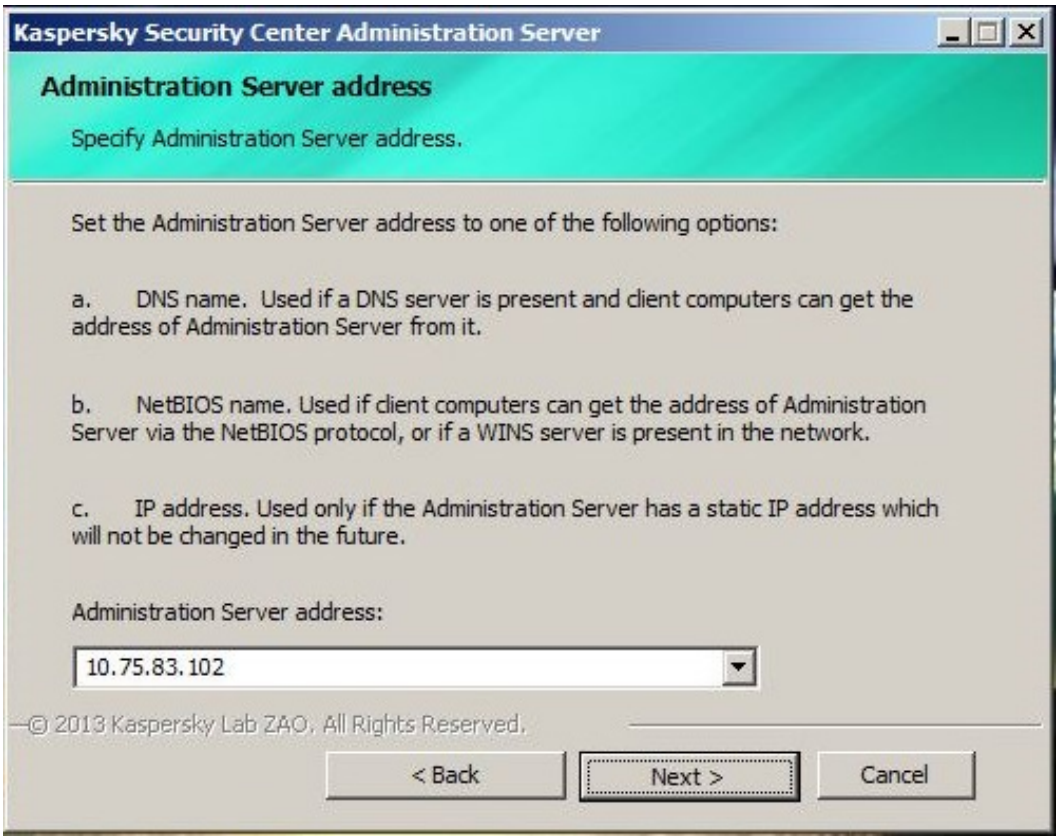
**Kaspersky Security Center** will create a networked shared folder for things like standalone installation packages; you can modify the location of that folder here:



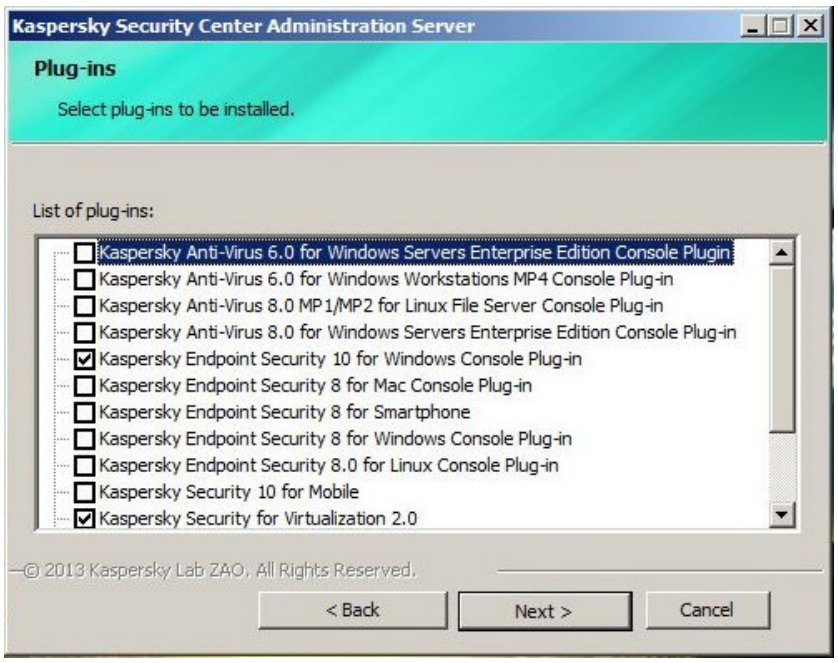

By default, the Kaspersky Network Agent will communicate over ports 13,000 and 14,000 - you have the option of changing this default:



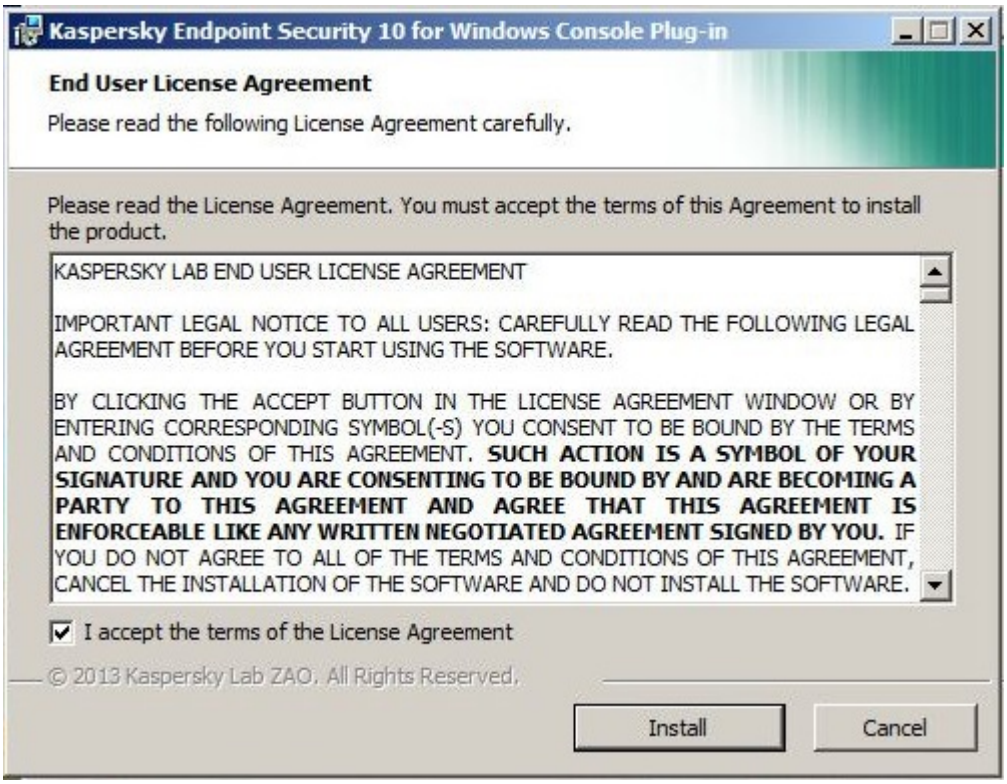
Select how you wish the server to be identified. It is recommended to use a **static IP address** to avoid DNS resolution issues, handle split domain environments, and deploy Kaspersky Security for Virtualization and Mobile Device Management most effectively:



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




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



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

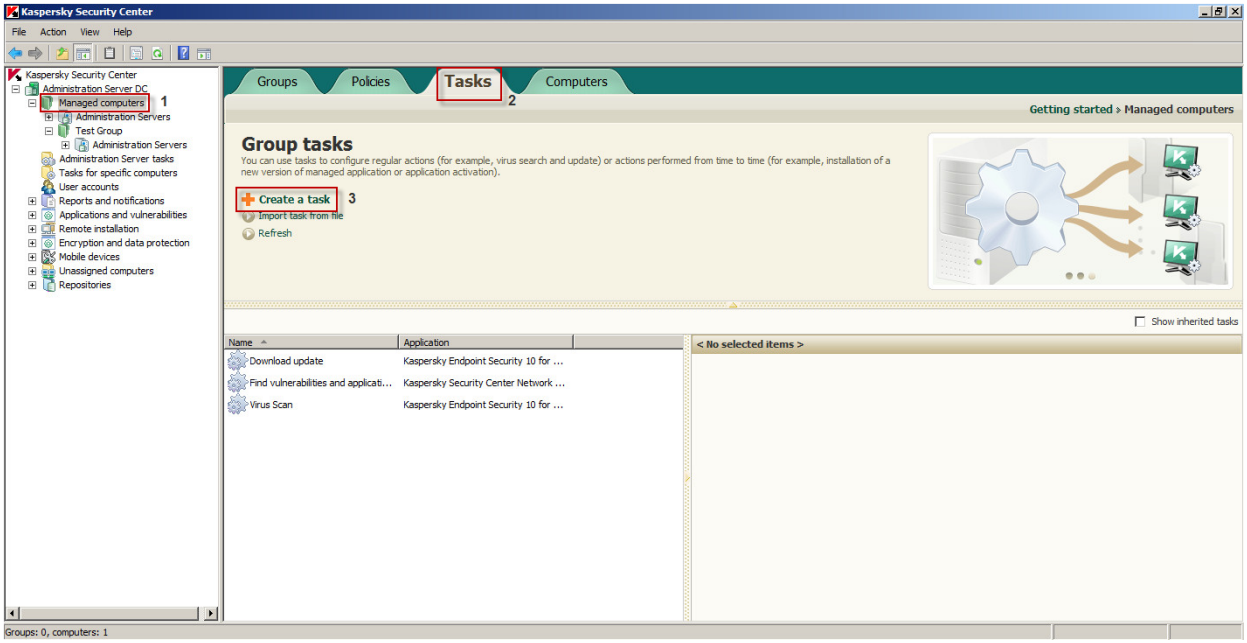
When installed, the Network Agent will run a query against the Windows software registry and identify any applications that are not compatible with Kaspersky Endpoint Security 10 for Business. It is important to identify and remove these applications prior to installing Kaspersky.

## Requirements for Client Computers:

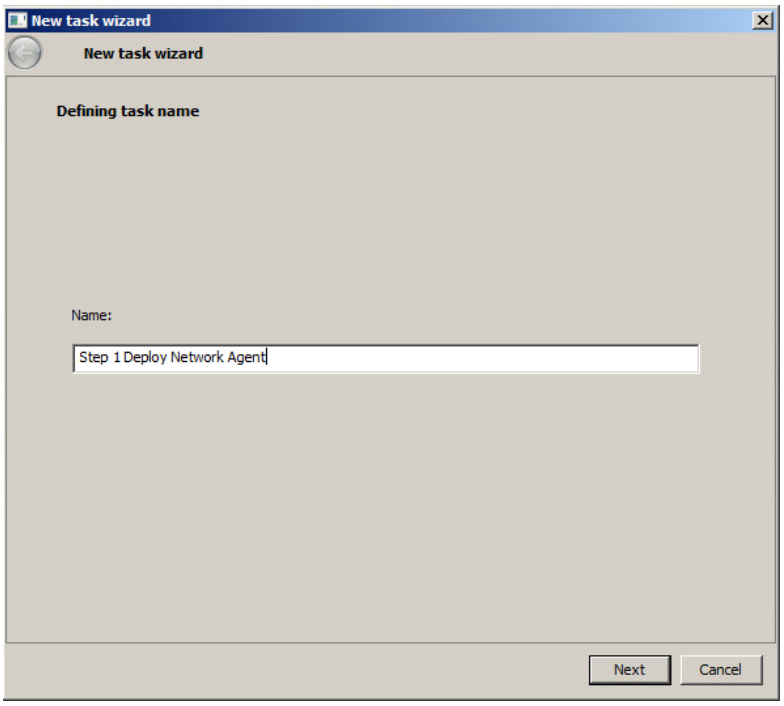
*Necessary Firewall Ports are open:  TCP: 139, 445 UDP: 137, 138 or Firewall is turned off.*

## Phase 1: Deploy the Network Agent

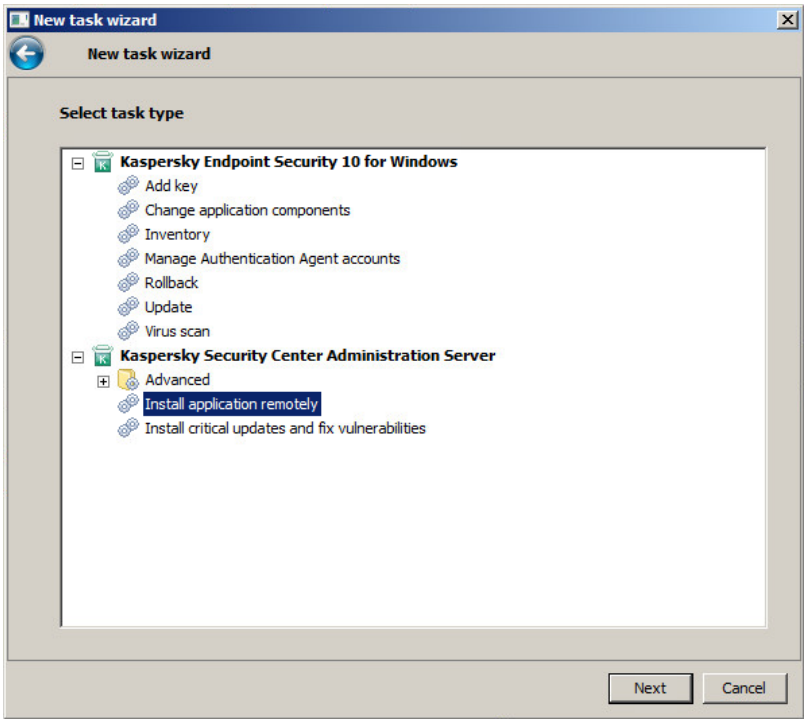
**Step 1:** Go to the “Tasks” tab in the “Managed Computers” group or to the desired sub-group and create a new task.



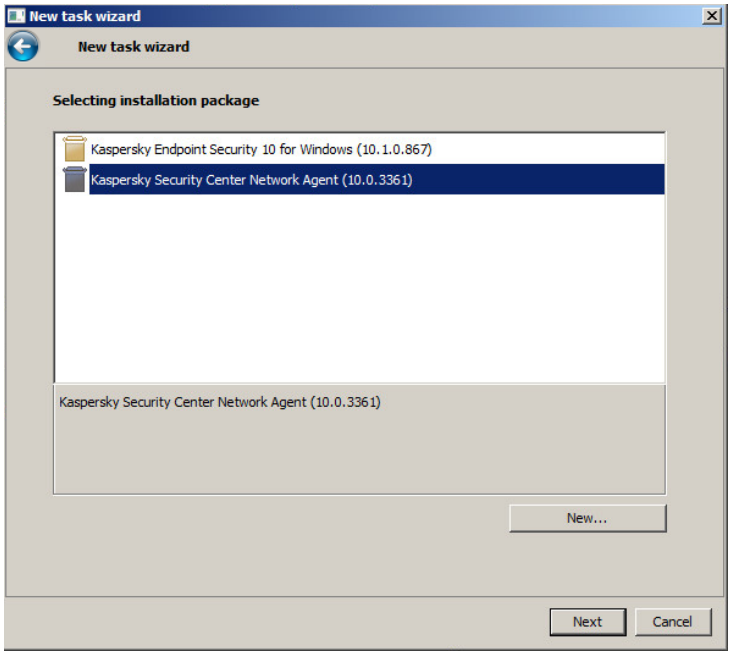
**Step 2:** Name your Task, and then click next to move on.



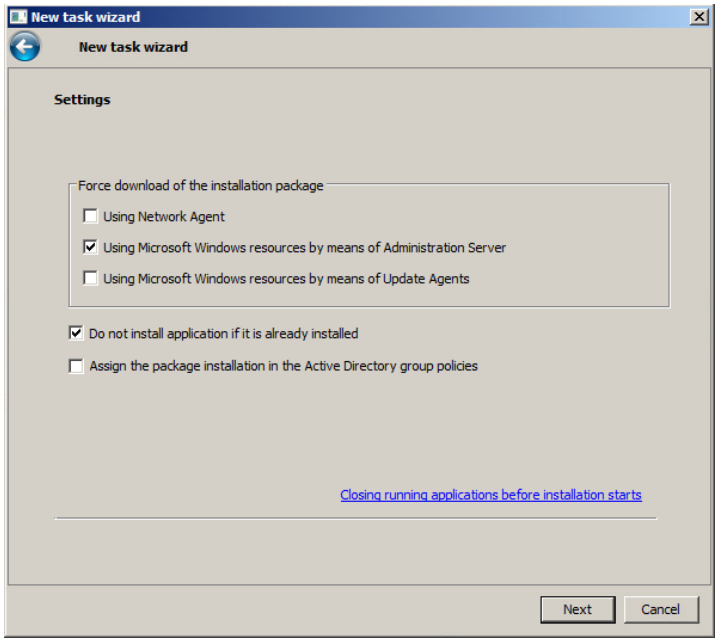

**Step 3:** Choose “Install Application Remotely”, and then click next to move on.



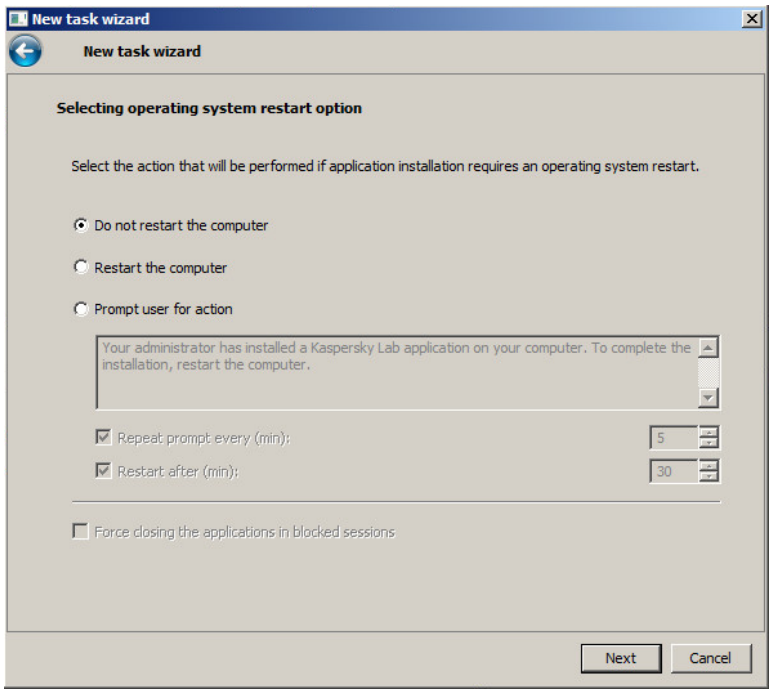
**Step 4:** Choose the Network Agent Installation Package from the list and then click next to move on.



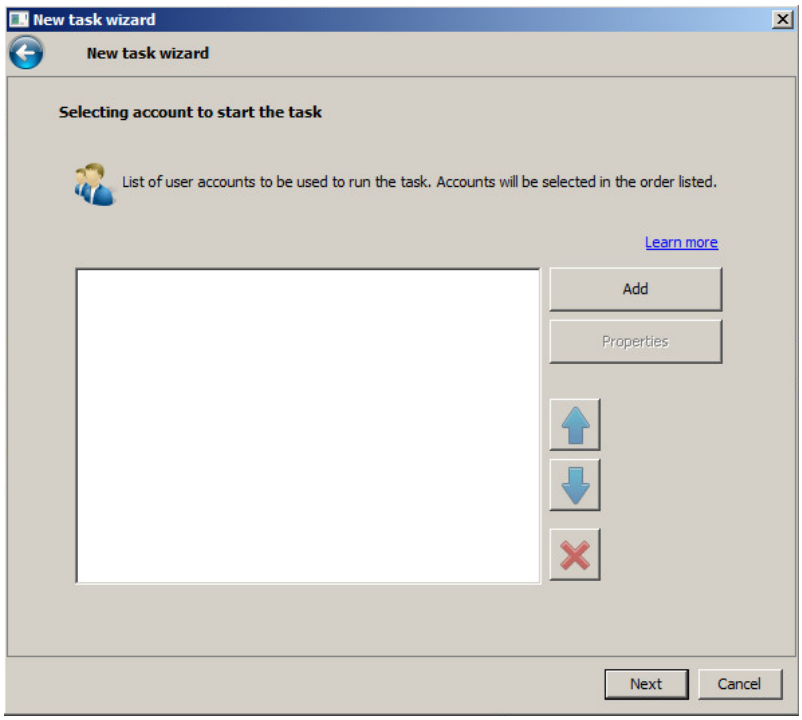

**Step 5:** Choose how to upload the package to your clients. You will want uncheck "Using Network Agent" if you do not already have a network agent installed on the client. Click next to move on.



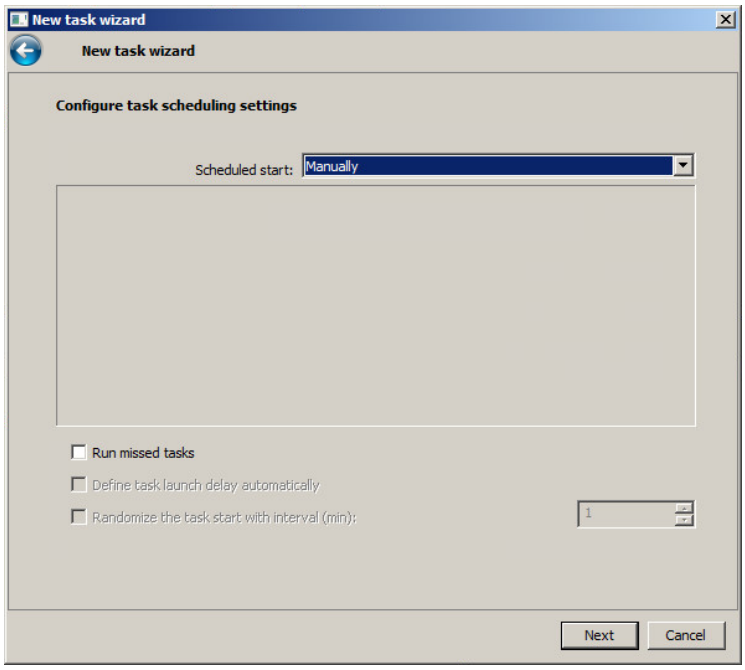
**Step 6:** A reboot is NOT required after the agent is installed. Choose the "Do not restart the computer" option and then click next to move on.



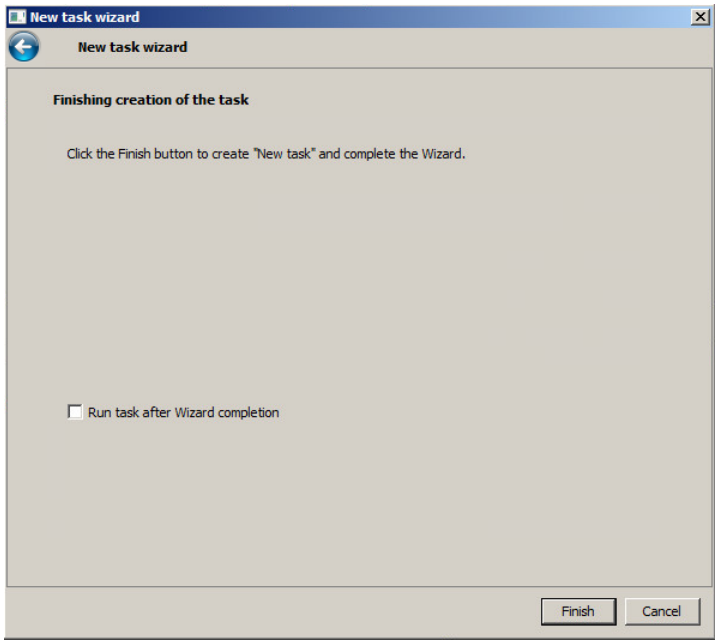

**Step 7:** Please enter in Credentials with local Administrative Rights. If this is left blank, the Security Center will use the default account that was assigned to it during installation.



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

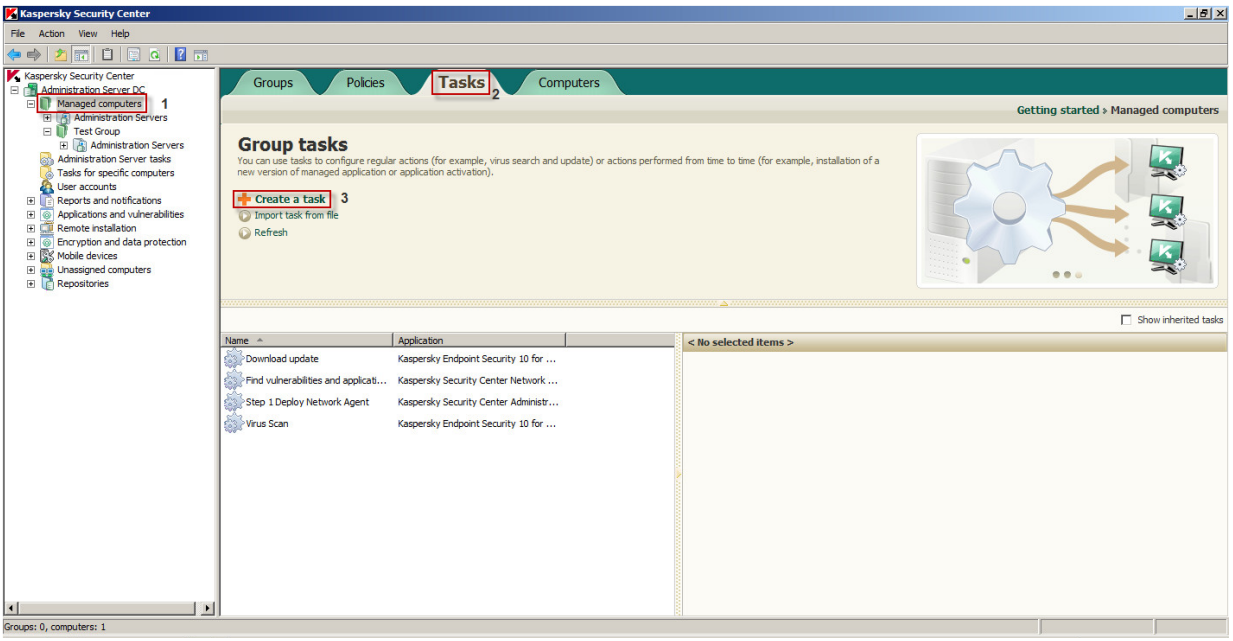



**Step 9:** Leave the option to “Run task after Wizard completion” unchecked and click Finish to complete the wizard.

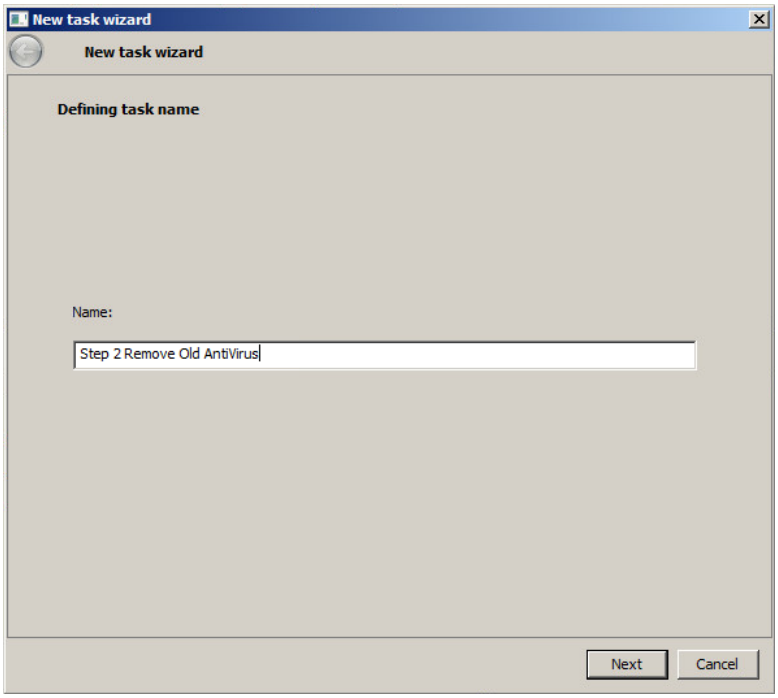


## Phase 2: Remove your old Antivirus

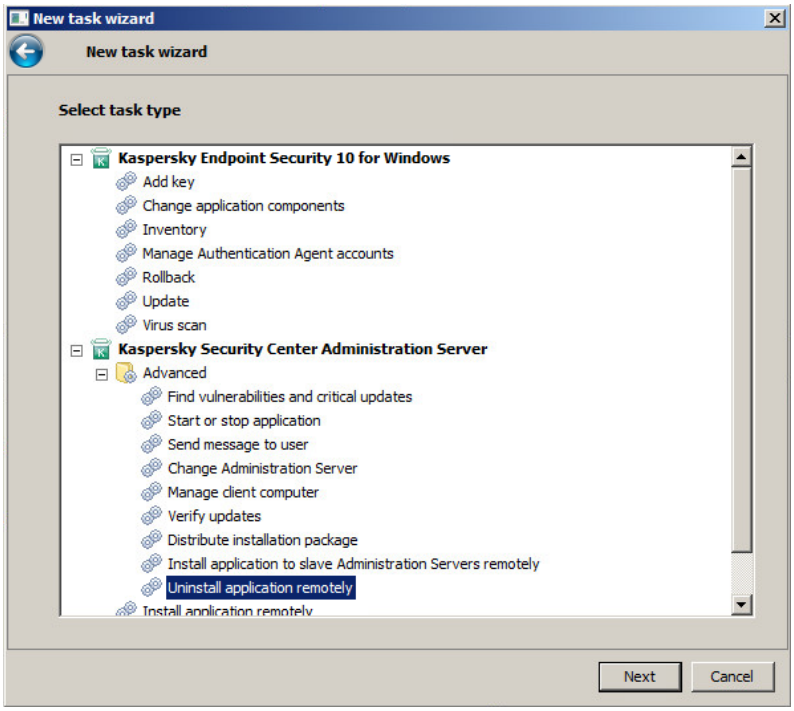
**Step 1:** Go to the “Tasks” tab in the “Managed Computers” group or to the desired sub-group and create a new task.



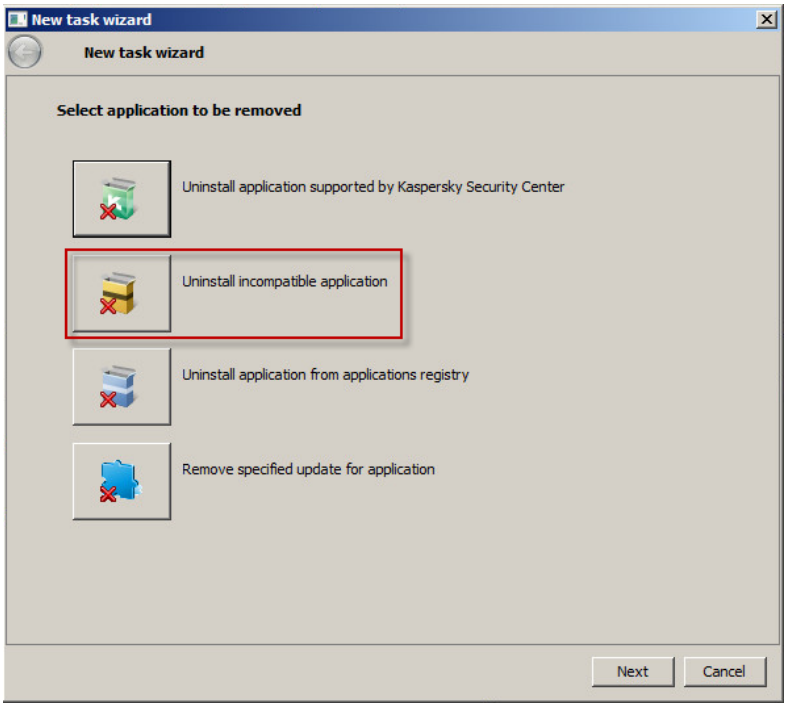

**Step 2:** Name your Task, and then click next to move on.



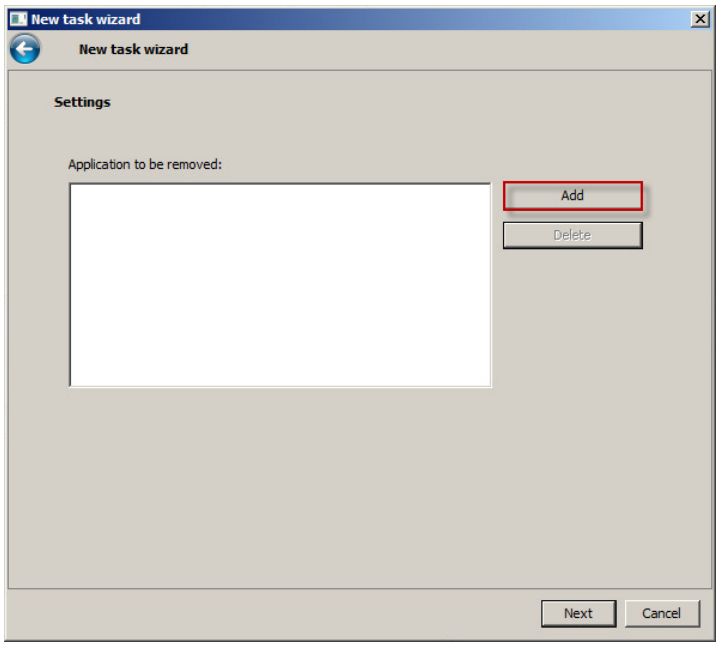
**Step 3:** Expand the Advanced container and select “Uninstall application remotely”, then click next to move on.



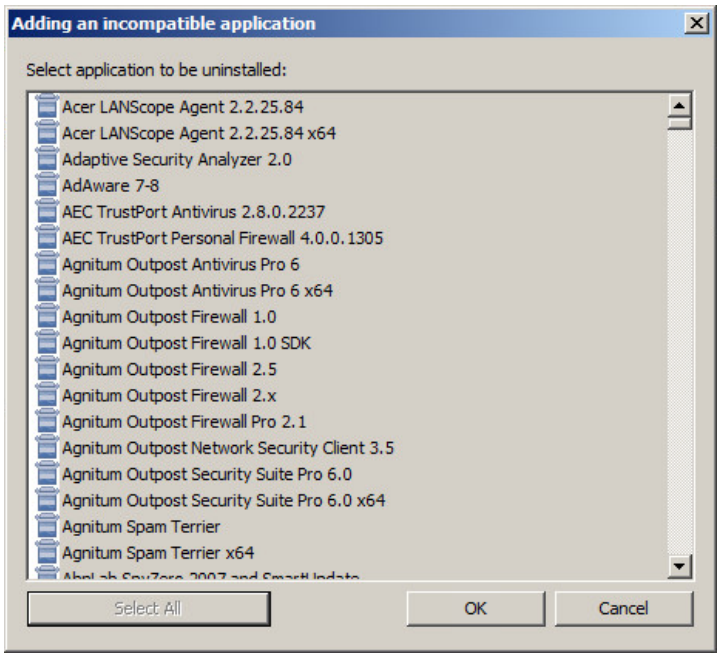

**Step 4:** Choose “Uninstall incompatible application”.



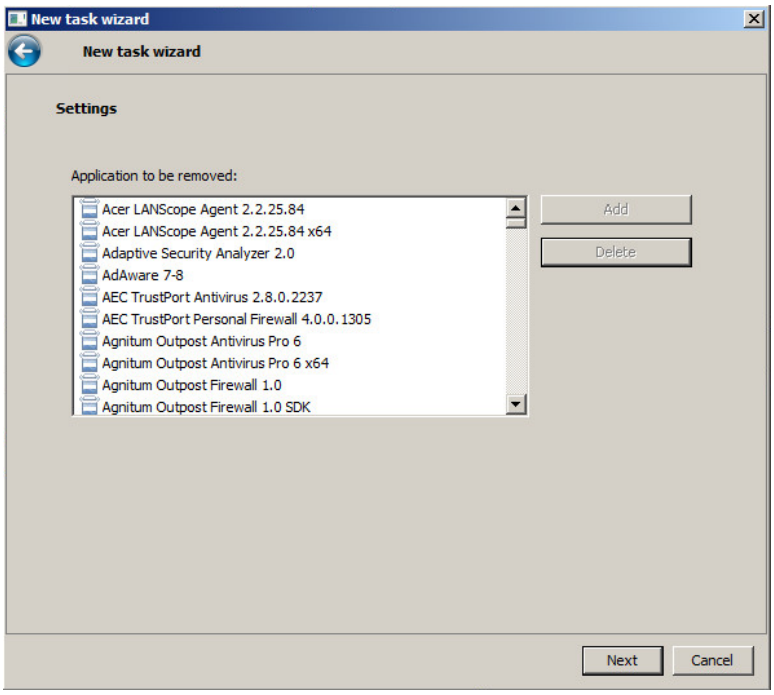
**Step 5:** Choose Add to select the removal scripts you need.



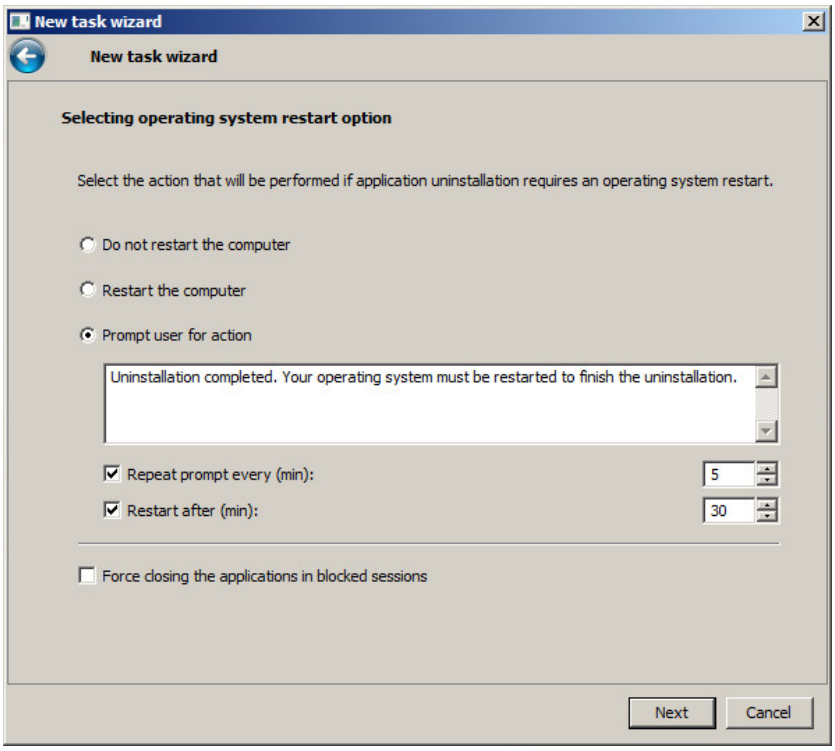

**Step 6:** Select the Scripts you need. You can select multiple scripts at once by holding down CTRL or Shift as you select from the list. Choose OK when you are finished. Note: If you do not see your Antivirus product on the list or if it fails to remove your product, please contact your Systems Engineer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



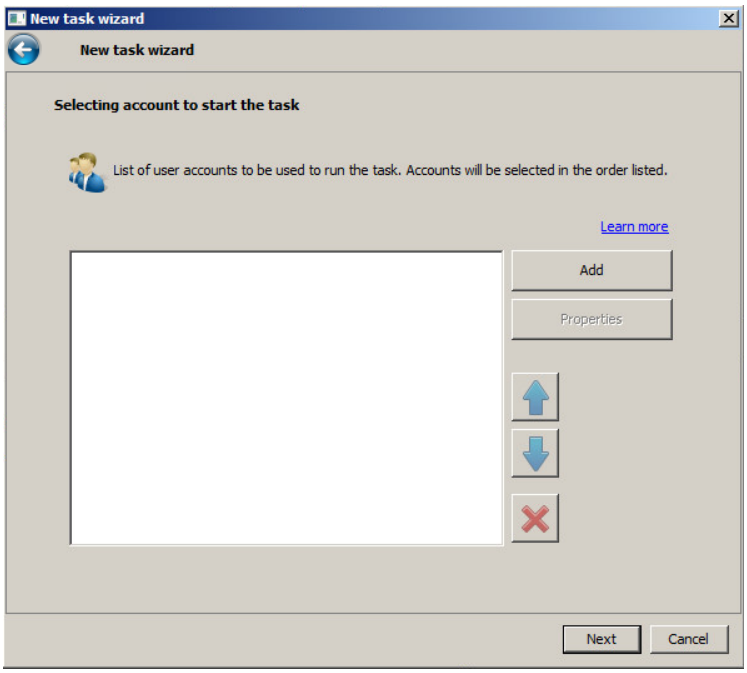
**Step 7:** Make sure the scripts you wanted are on the list to be removed, and then choose next to move on.



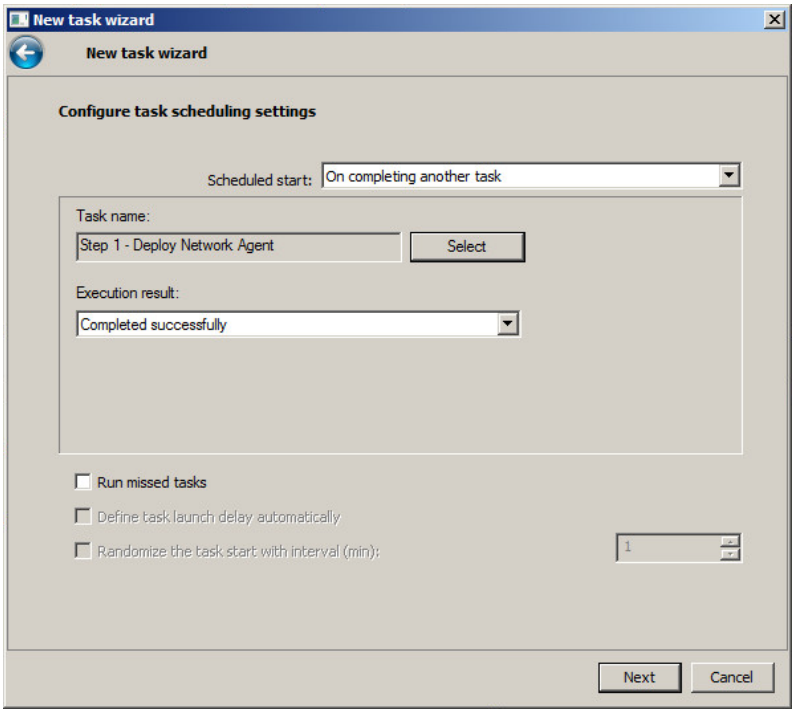

**Step 8:** A reboot is usually required after this step to fully remove most old Antivirus applications. You can either reboot immediately after the uninstall or prompt the user for action. Choose next to continue.



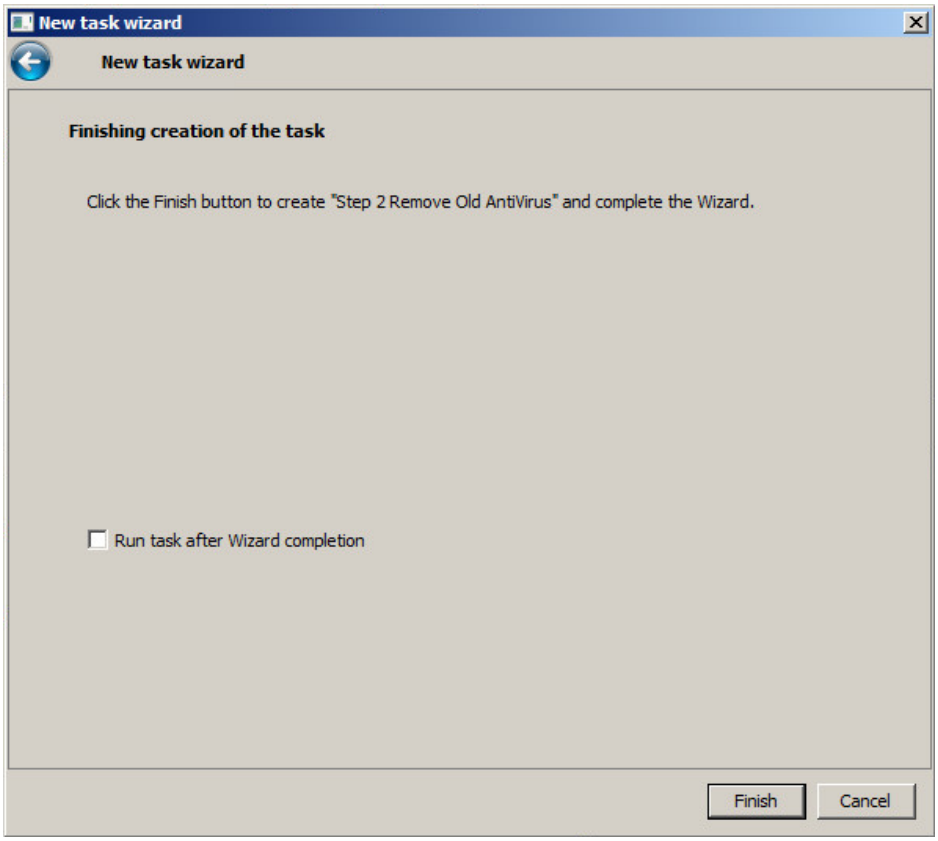
**Step 9:** Add credentials with local administrative rights for the targeted computers. By default the task will be run through the Network Agent using the local system service account, so credentials may not be needed.




**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.

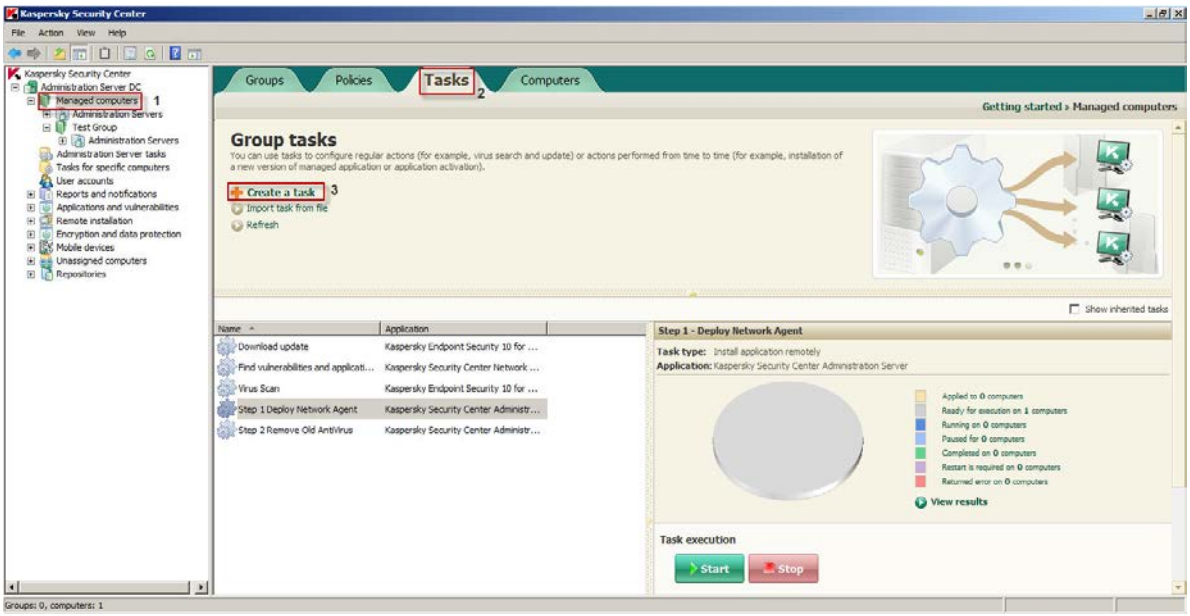


**Step 11:** Leave the option to “Run task after Wizard completion” unchecked and click Finish to complete the wizard.

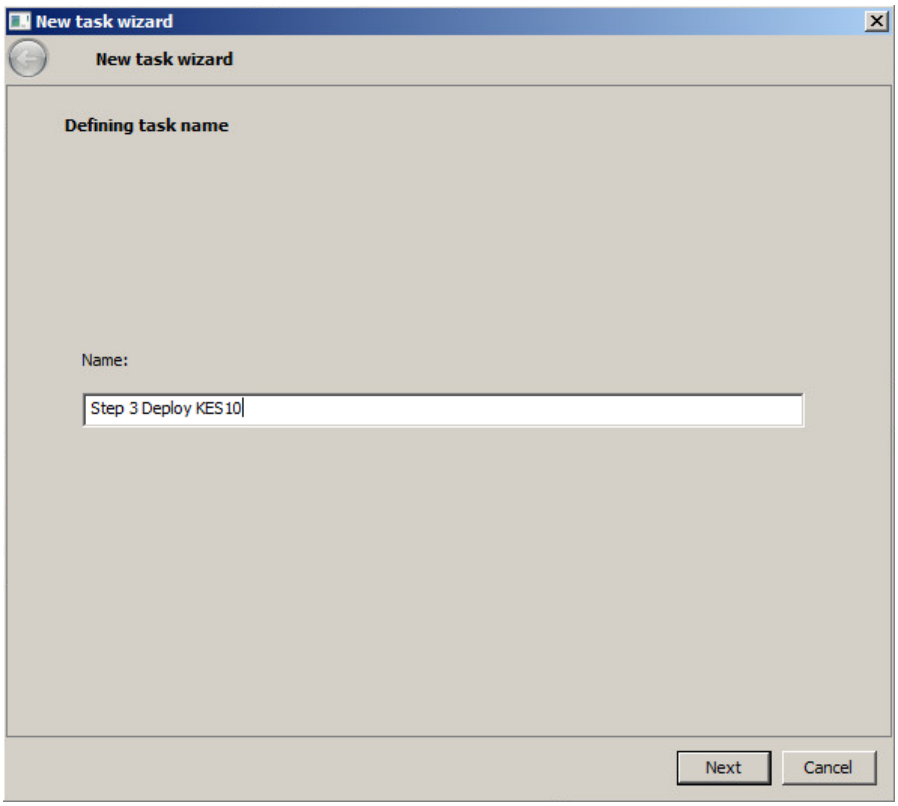


## Phase 3: Deploy Kaspersky Endpoint Security 8 to you Computers

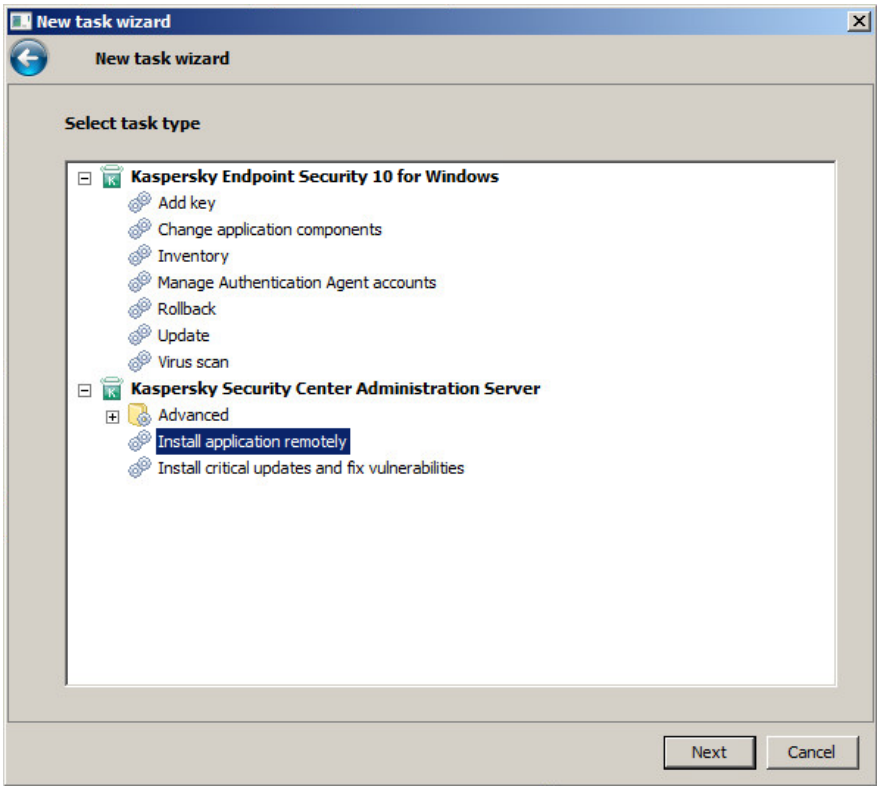
**Step 1:** Go to the “Tasks” tab in the “Managed Computers” group or to the desired sub-group and create a new task.



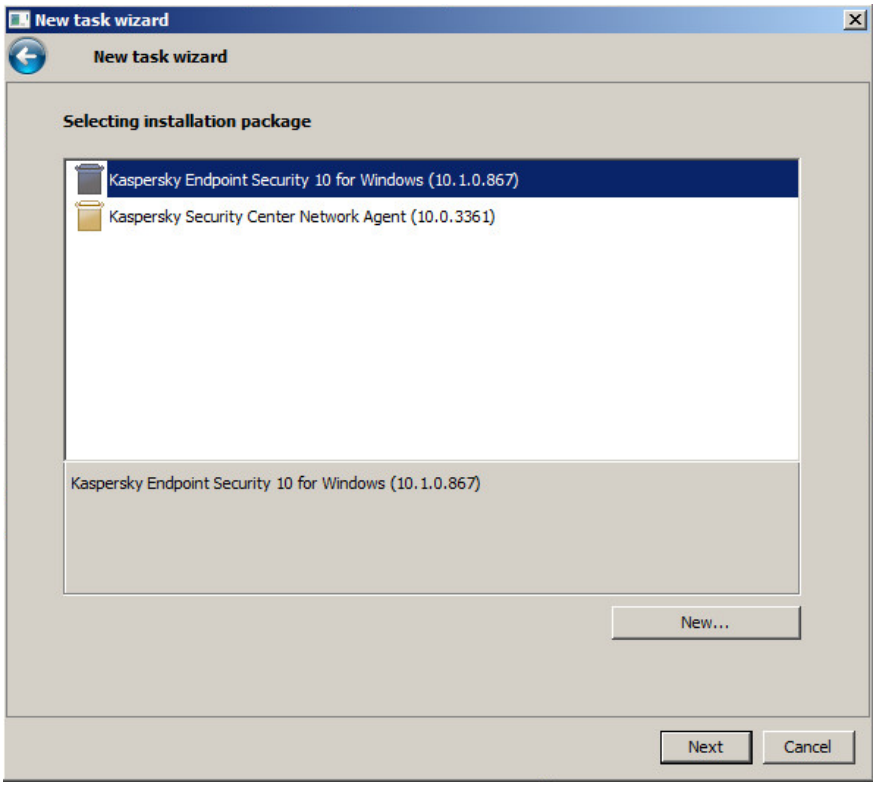

**Step 2:** Name your Task, and then click next to move on.



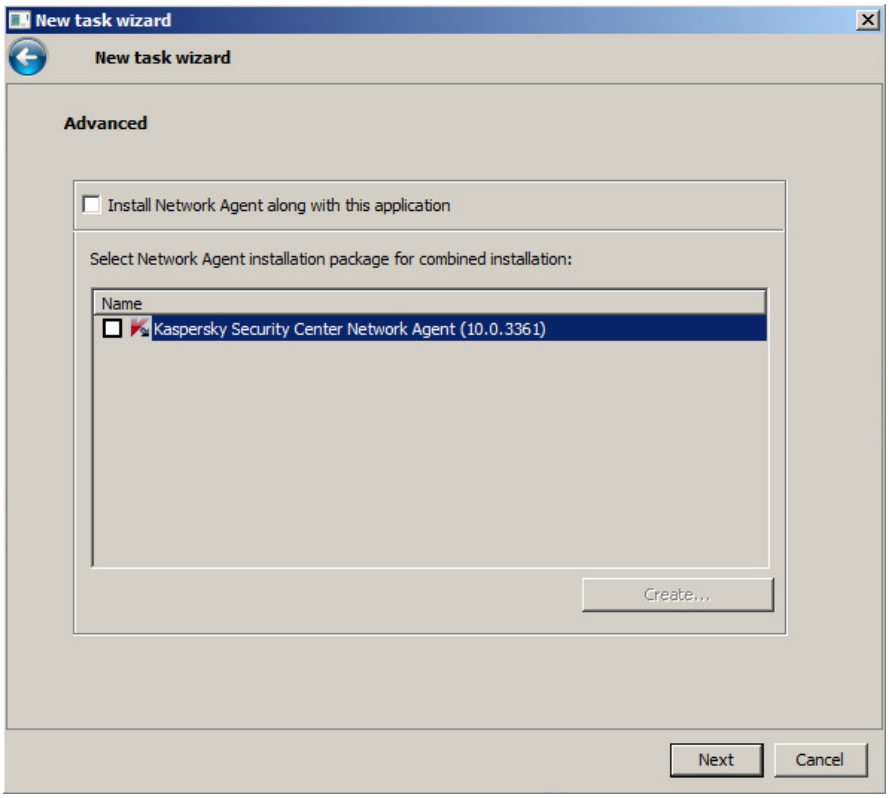
**Step 3:** Choose “Install Application Remotely”, and then click next to move on.



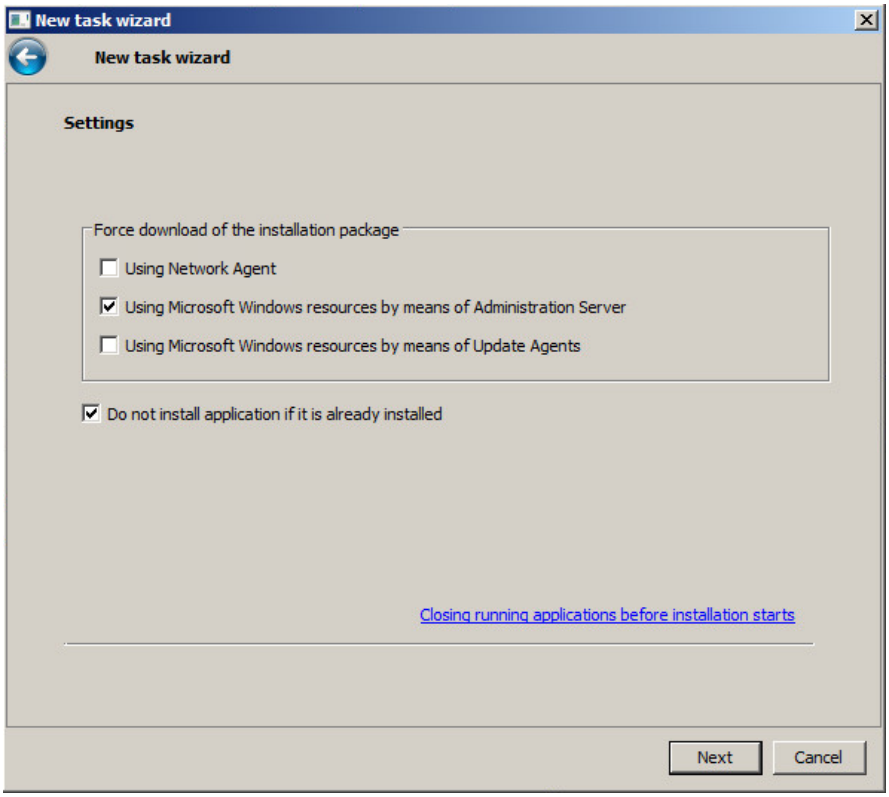

**Step 4:** Choose the Endpoint Security Installation Package from the list and then click next to move on.



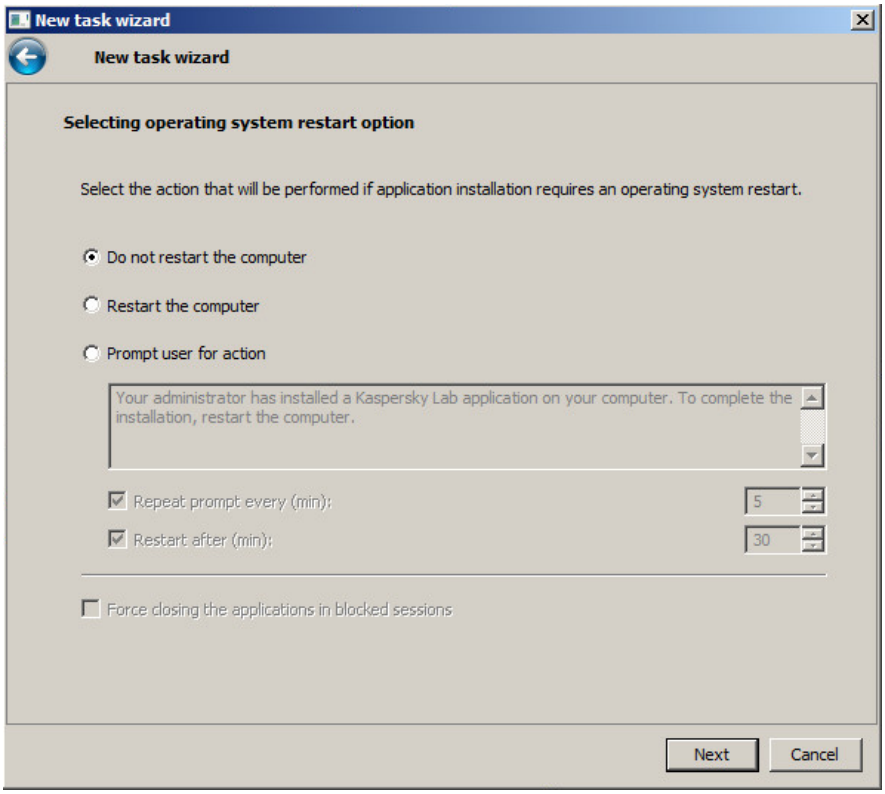
**Step 5:** You can bundle the Network Agent with the install of Endpoint Security, however, we have already done this with the first task, so you can skip it.



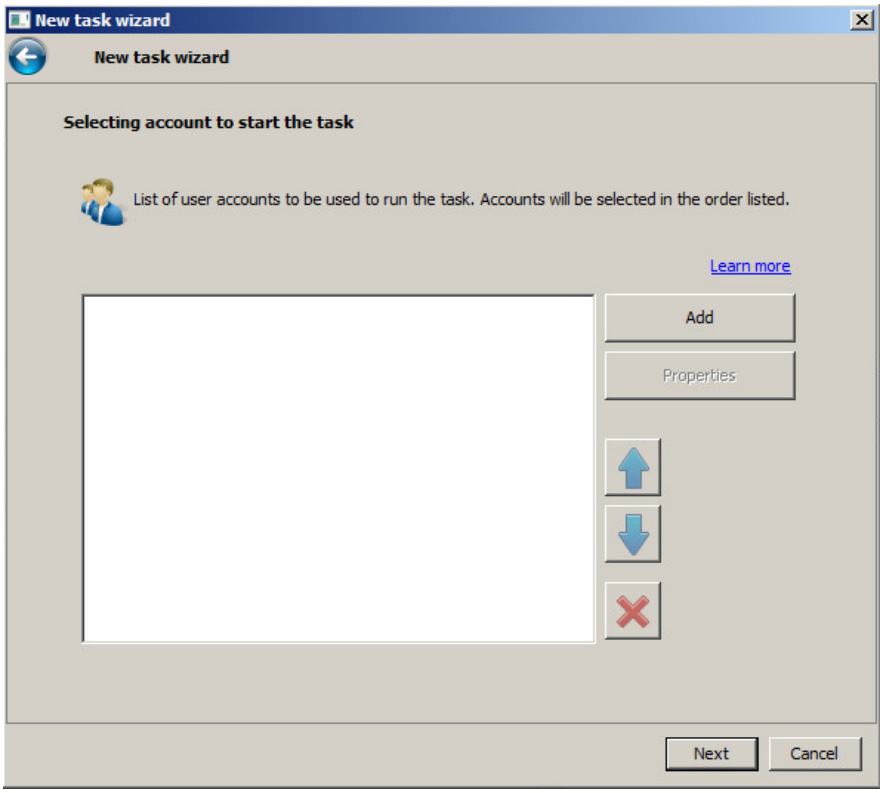

**Step 6:** Choose how to upload the package to your clients. Defaults are fine in most cases, but it is usually a good idea to uncheck the network agent usage because deployment via Windows shares is usually quicker. Click next to move on.



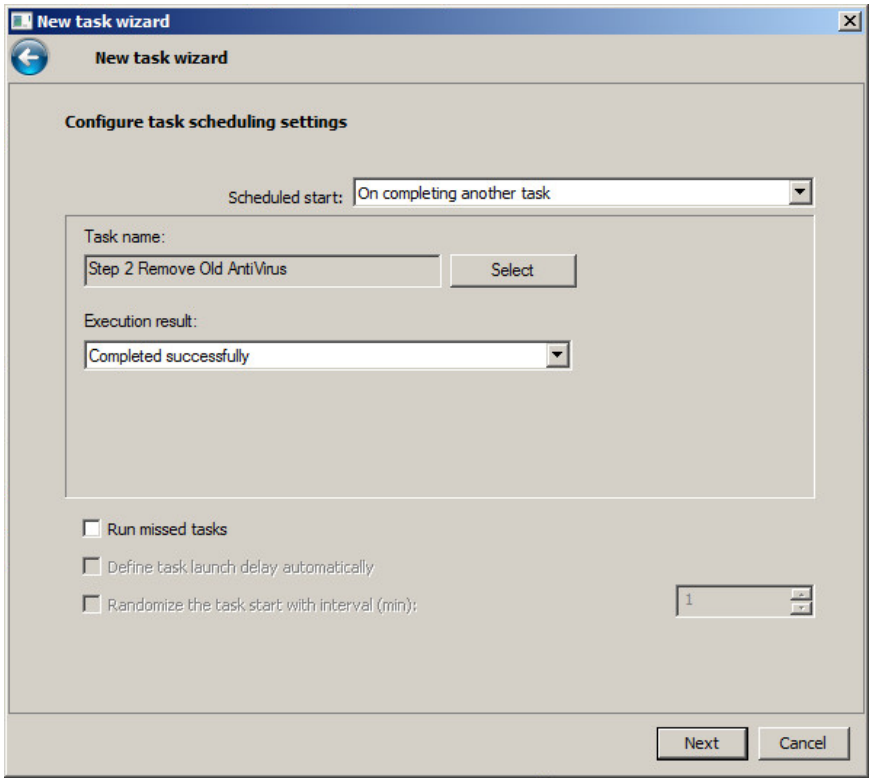
**Step 7:** A reboot is NOT required after the Endpoint Security Installation. Click next to move on.



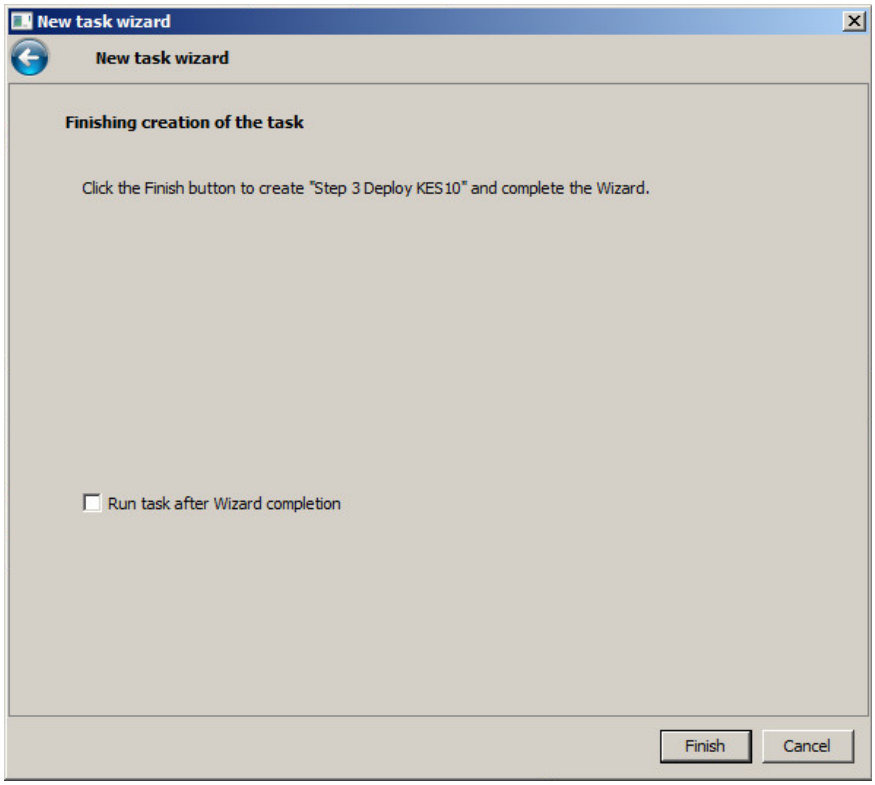

**Step 8:** Add credentials with local administrative rights for the targeted computers. If the default account for the Security Center has local administrative rights, then you can skip this step and click next to continue.



**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.



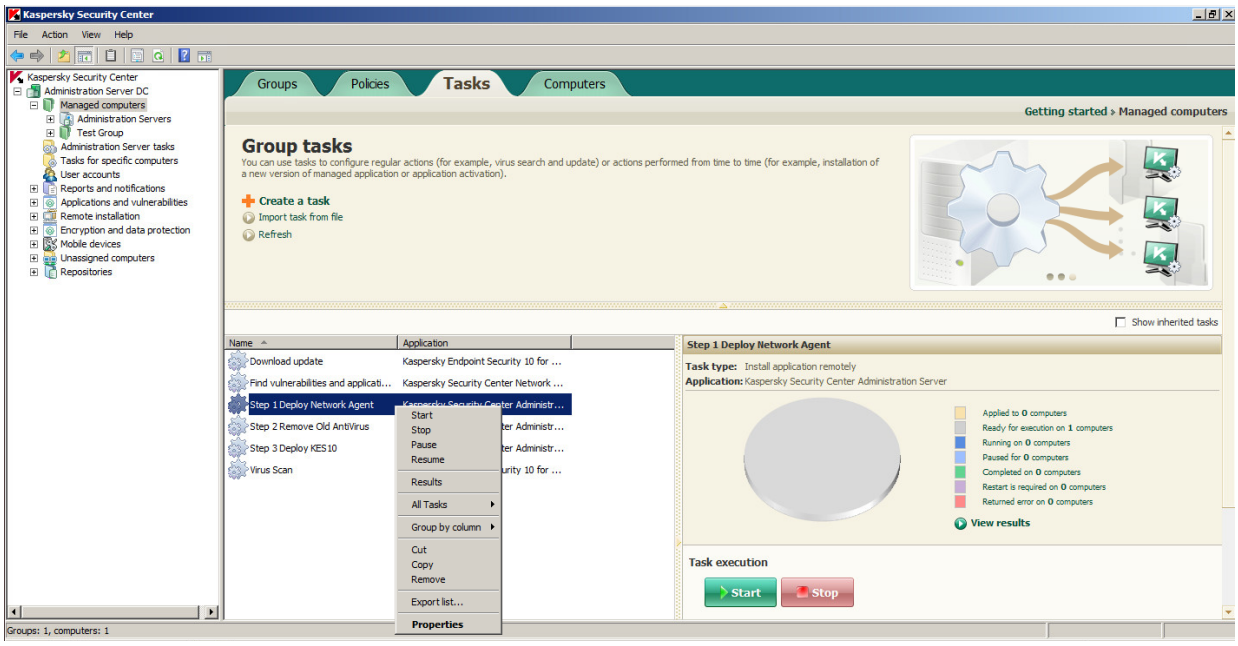

**Step 10:** Leave the option to "Run task after Wizard completion" unchecked and click Finish to complete the wizard.



## 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.

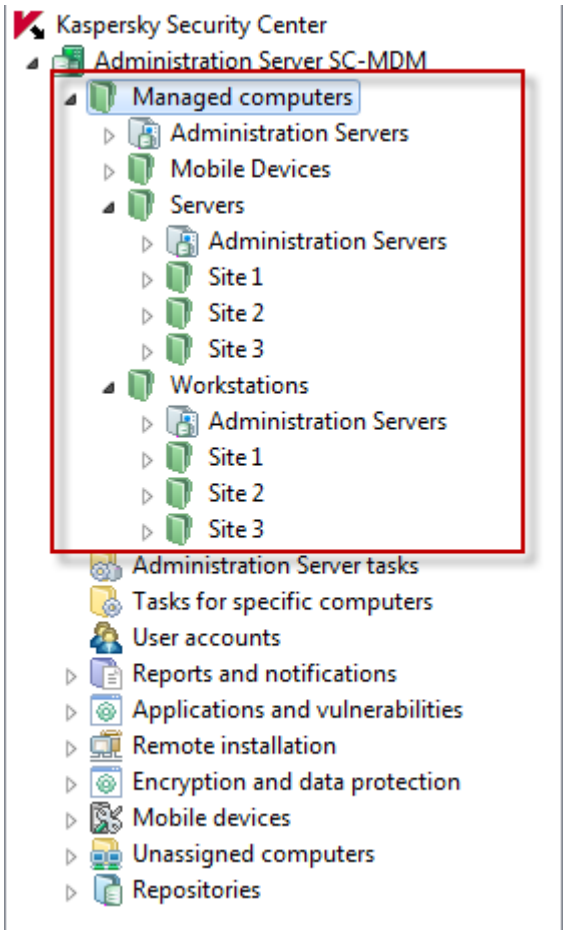


# 5. Group and Policy Recommendations

## Organizing your “Managed Computers”

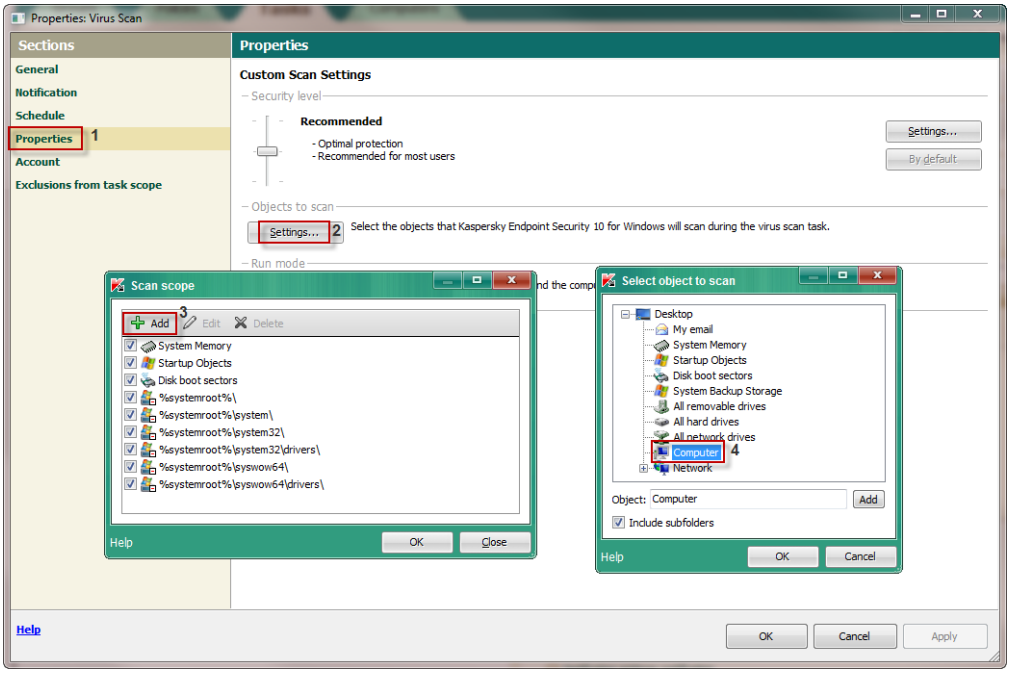
The first step you should take after setting up your Security Center, is organizing your managed computers. In most cases, the best way is to break machines up by Workstations and Servers. This way you can have separate policies and tasks for your servers and workstations.

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.



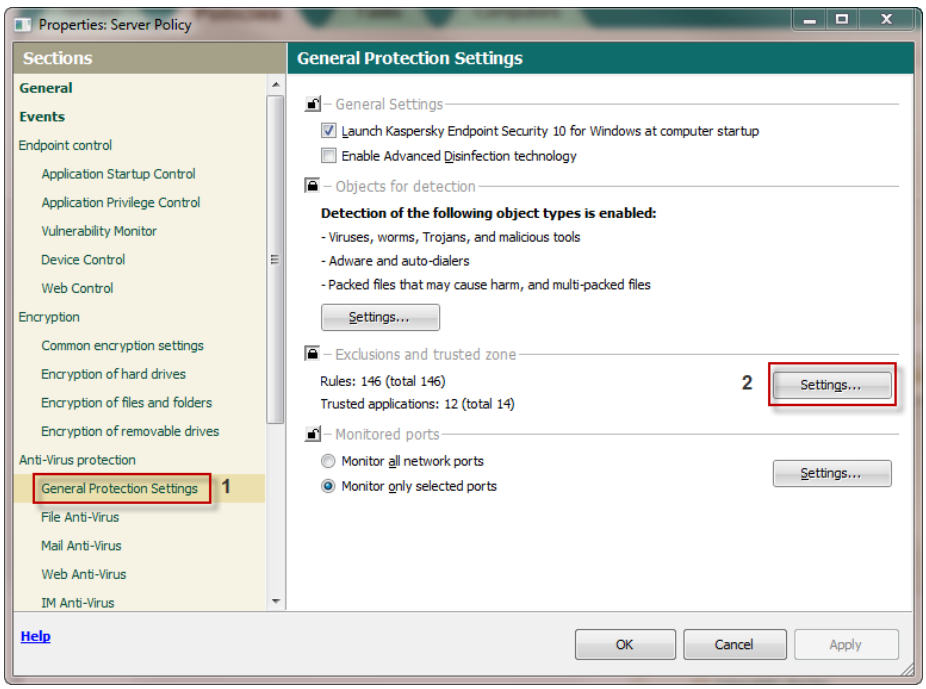
## Configuring the default virus scan task

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.



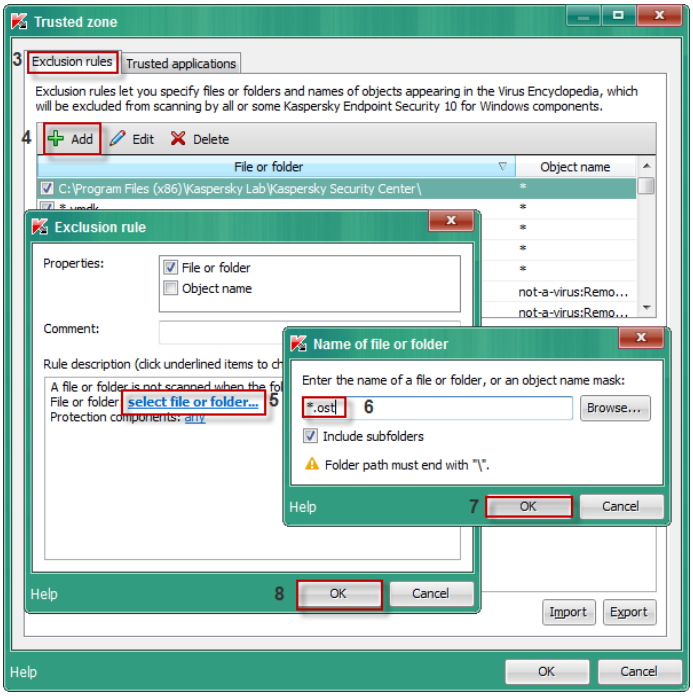

## Setting exclusions

This next setting involves configuring exclusions that will help with performance

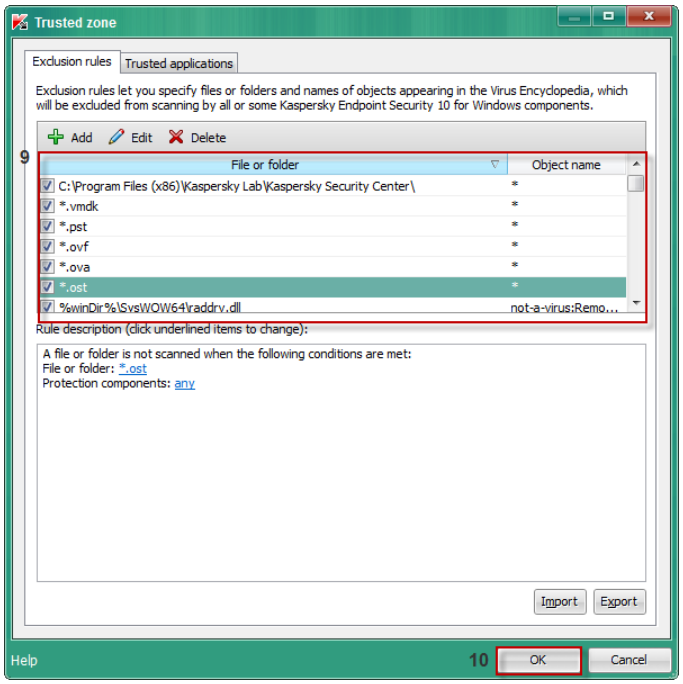


When adding objects to exclude, you can utilize different masks to make your rules more powerful and flexible. Allowed exclusion masks can be found in our knowledgebase article here: http://support.kaspersky.com/faq/?qid=208280713

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

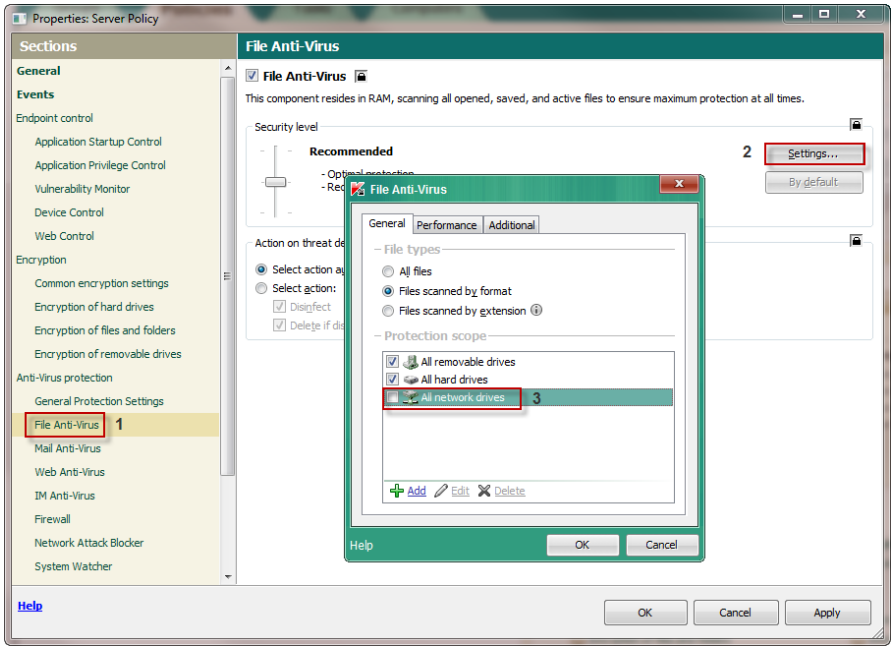



Once you have made your exclusion rules, make sure they appear on the list and are checked.



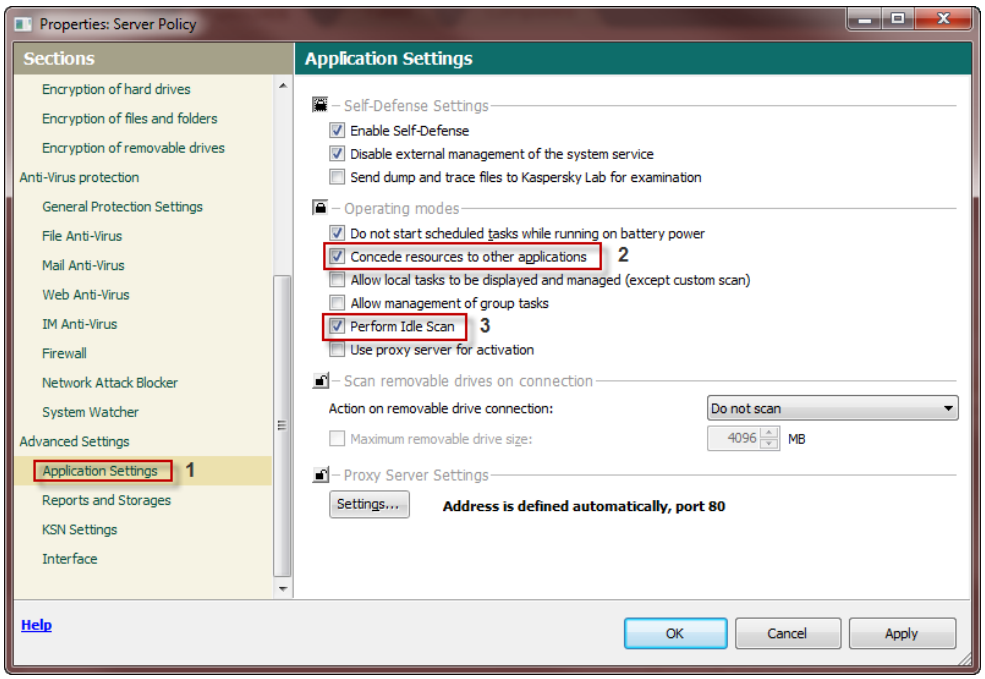
## Optimizing scan and application settings

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.

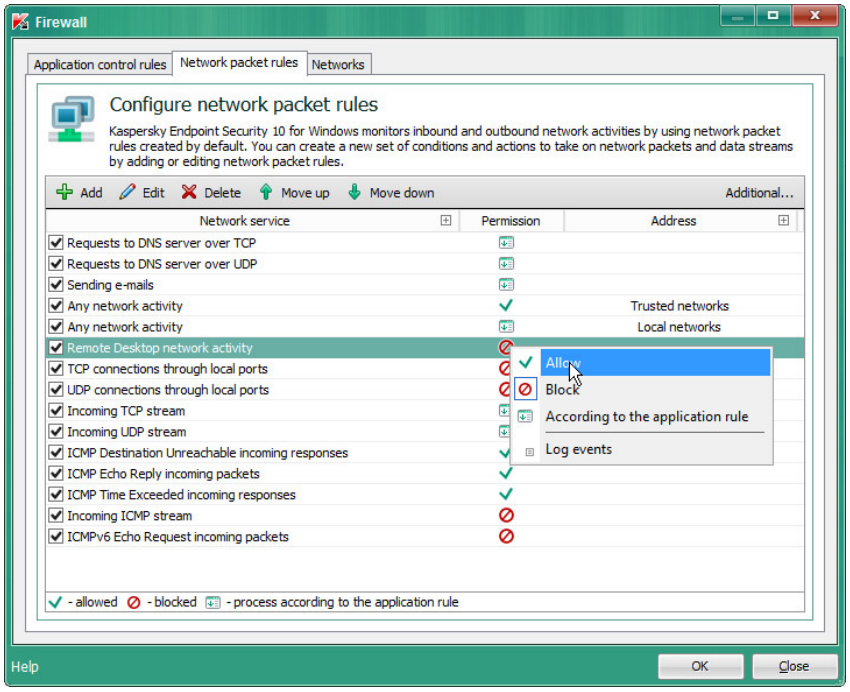



The last fixes are to enable the options to concede resources to other applications and to Perform Idle Scans. Conceding resources allows Kaspersky to automatically suspend scheduled tasks when it detects an increased load on the CPU and it will free up operating system resources for user applications.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




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