kaspersky

How to integrate Kaspersky Industrial CyberSecurity 2.6 into Simatic PCS 7 9.1 process control infrastructure

Step-by-step installation and configuration guide

17.11.2021

kaspersky

Contents

kaspersky

What this document is about

This document provides detailed instructions on how to install and configure **Kaspersky Industrial CyberSecurity 2.6 (Hotfix[1] 12)** within **Siemens Simatic PCS 7 9.1** process control environment. It will guide you through several sequential steps of product installation and its subsequent configuration.

Who would find this document useful

This document might be interesting to the following audience:

- Specialists involved in industrial cybersecurity.
- Process operating staff.
- Automation system engineers.
- DCS implementation and maintenance engineers.
- Test engineers verifying compatibility of **Kaspersky Industrial CyberSecurity** with DCS software.

Other specialists may also benefit from using this document as a reference guide.

What is KICS

Kaspersky Industrial CyberSecurity (or **KICS**, in brief) is the software solution developed by **Kaspersky Lab**. It enables robust protection of automatic control systems against a broad variety of cybersecurity threats, either known or "zero-day". It is equally applicable to different industries and is easily adaptable to various control system configurations.

KICS software components

KICS consists of several protection components, which are optionally selected and utilized according to your specific requirements. In general, **KICS** includes the following software components:

- **KICS for Nodes**. This component protects Windows-based endpoints such as operator workstations, engineering workstations, historians, HMI-servers, etc. Therefore, it has the potential of interfering with the HMI software and engineering software unless it is configured correctly.
- **KICS for Networks**. This component acts as a real-time analyzer of industrial networks traffic. As opposed to the previous one, this component remains 100% passive and by no means affects the monitored system. It remains invisible from the DCS perspective and architecturally has no mechanisms of interfering with DCS operation.
- **Kaspersky Security Center** (from now on, **KSC**). It is an administration tool, which enables management of the **KICS** components in a centralized and user-friendly manner.

[1] If **KICS for Nodes** is deployed onto critical infrastructure production sites located in Russia, the **Hotfix** installation may not be compulsory. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section.

Each of the cited components has a few functional modules. Each module is responsible for performing some specific function like anti-virus protection or device control.

The **KICS for Nodes** component incorporates the following modules:

- **Application launch control**. It restricts execution of files and scripts according to the user-defined white list.
- **Device control**. It restricts connection of peripheral devices to the protected host. It solely deals with USB-interface storage devices such as USB memory sticks, USB hard drives, etc.
- **Anti-malware protection (real-time file protection)**. It performs an anti-viral inspection of a file every time it is accessed, modified, moved or copied.
- **On-demand antimalware scanner**. It performs on-demand search for malicious objects in locations specified by users.
- **Virus database updater**. It is essential for keeping anti-virus databased up to date.
- **Untrusted host blocker**. It blocks network access to shared folders for the remote hosts that show malicious activity.
- **Anti-cryptor**. It prevents malicious encryption activity. It is designed to work in conjunction with the **Untrusted host blocker**.
- **Vulnerability scanner**. It is used to obtain comprehensive and up-to-date information on software vulnerabilities found on the managed hosts.
- **File integrity monitor**. It is designed to track/alert modifications made to the specified files and folders of the monitoring scope according to the task settings. You can use the task to detect file changes that may indicate a security breach on the protected computer.
- **Log inspection.** It is designed to monitor the integrity of the protected environment based on the results of an inspection of Windows Event Logs. The application notifies the administrator upon detecting abnormal behavior in the system, which may be an indication of attempted cyber-attacks.
- **Exploit prevention.** Kaspersky Industrial CyberSecurity for Nodes 2.6 provides the ability to protect process memory from exploits. You can change the component activity status and configure process protection settings.
- **PLC Integrity Checker**. It periodically verifies consistency of control logic, executed by the monitored PLC. It reacts to any modification of a process control program. At present, this module supports **SIMATIC S7-300**, **S7-400(H)** series controllers.

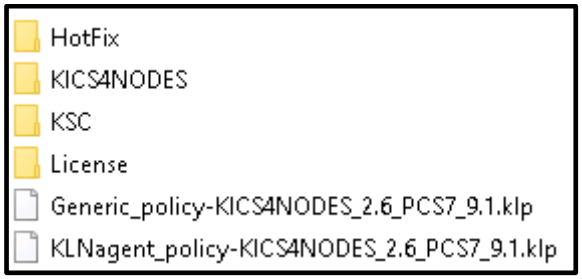
Please note, that the **KICS for Nodes Firewall management** feature does not apply to DCS installations and, therefore, the corresponding software module should not be installed. Alternatively, it is highly recommended to rely on the **Windows Firewall** configured according to the DCS vendor's recommendations. The more detailed recommendations as to the installation scope are given in the "Remote installation of KICS for Nodes onto target computers via KLnagent" section.

This document does not cover **KICS for Networks** installation and its configuration techniques.

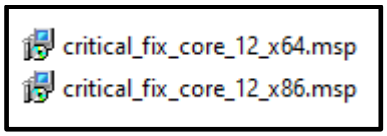
kaspersky

Distribution package composition

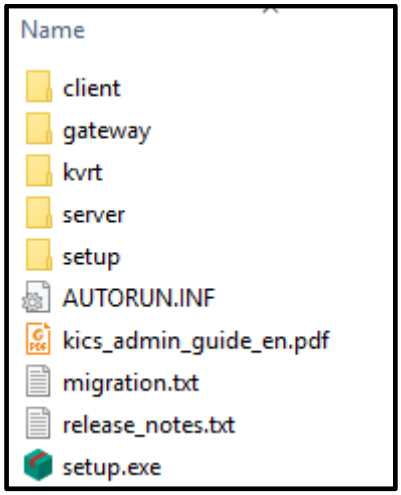
Before starting the product installation, please check the contents of the **KICS** distribution package and make sure you have obtained all the necessary files. The distribution package includes the following items.



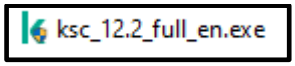
The **Hotfix** folder contains **Hotfix 12**[2] for **KICS for Nodes 2.6**. The **Hotfix** is cumulative and in most cases its installation is compulsory[3].



The **KICS4NODES** folder contains the **KICS for Nodes 2.6** installation files, **KICS for Nodes 2.6** administrator's guide. The **client** subfolder contains the **KICS for Nodes 2.6 management console**. The installation of **KICS for Nodes 2.6 management console** is optional. The **server** folder contains the **administration plugin for KSC.**



The **KSC** folder contains the **Kaspersky Security Center** installation package (version 12). The **KSC** product manuals are available online at https://support.kaspersky.com/KSC/12/en-US/5022.htm



[2] As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a subsequent version has become available.
[3] If **KICS for Nodes** is deployed onto critical infrastructure production sites located in Russia, the **Hotfix** installation may not be compulsory. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section.

The **License** folder contains the **KICS for Nodes** license activation key-file.

The **Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp** file is a preconfigured set of the high-level security settings optimized for **Simatic PCS 7 9.1**. These predefined settings, which **KSC** makes use of, significantly facilitate the **KICS for Nodes** deployment process. The similar file (**KLNagent_policy-KICS4NODES_2.6_PCS7_9.1.klp**) aids the **KLnagent** configuration.

System requirements

We recommend installing **KSC** on a separate PC designated for the centralized management of **KICS for Nodes** instances. Please make sure that this computer conforms to the software and hardware requirements as specified in https://support.kaspersky.com/KSC/12/en-US/96255.htm.
Every target station hosting **KICS for Nodes** should be compliant with the system requirements as specified in pages 29-30 of the supplied **"KICS for Nodes 2.6 Administration Guide"** (**kics_admin_guide_en.pdf**).
The following ports should also be open for normal KICS for Nodes infrastructure management from KSC:

- From DCS network segments to the **KSC** server TCP: 13000-13001.
- From the **KSC** server to DCS network segments UDP: 15000-15001.

Additional access from control system network to the **KSC** server is advised during installation (this access can be closed after installation and tuning is finished):

- From DCS network segment to the **KSC** server – ICMP (Ping).
- From DCS network segment to the **KSC** server – Microsoft-ds (TCP: 445).
- From DCS network segment to the **KSC** server – NetBIOS-ssn (TCP: 139).
- From DCS network segment to the **KSC** server – TCP: 13291.

Optionally, the **KSC** server may utilize network access to the **Kaspersky Lab download servers** via port TCP: 80 (HTTP).
For correct external name resolution, it is recommended to grant the **KSC** server full access to DNS servers via TCP: 53 and UDP: 53.
To ensure smooth interaction between the **KSC** server and target stations, Ethernet connection with at least 10Mbit/s throughput is required.

Installation and configuration steps

This document describes how to install and configure multiple **KICS for Nodes** instances in a centralized manner (using **KSC**), whereas the stand-alone installation of **KICS for Nodes** is not overviewed. The entire procedure of **KICS for Nodes** deployment includes the following sequence of installation/configuration steps:

- Installation of **KSC** on a management PC.
- Initial configuration of **KSC**.
- Remote installation of the network agent **KLnagent** onto target computers.
- Installation of the **KICS for Nodes** management plugin on the top of **KSC**.
- Import of the security policy for the network agent **KLnagent** from a file.
- Import of the generic security policy for **KICS for Nodes** from a file.
- Remote installation of **KICS for Nodes** onto target computers via **KLnagent**.
- Remote installation of **Hotfix 12**[4] onto target computers via **KLnagent**. Please note that in some specific cases no **Hotfix** should be installed and this deployment step should be omitted. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section for details.
- Optional activation of **KICS for Nodes** delayed startup.
- Optional remote installation of **KICS for Nodes management console**.
- Initial update of antivirus databases.
- Launching the **On-Demand virus scan** task to inspect target computers.
- Setting up **Application Launch Control** and **Device Control** whitelisting and fine-tuning the generic security policy.
- Configuration of **PLC Integrity Checker**.

Installation of KSC on a management PC

The **KSC** deployment is commenced with installation of **MS SQL Server 2016 Express Edition** or a later version (for small and medium-size control systems including less than 100 nodes). The **MS SQL** installer is available at https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-52470555DB90/ENU/SQLEXPR_x64_ENU.exe. However, for the larger systems we recommend installing full functional **MS SQL Server**.

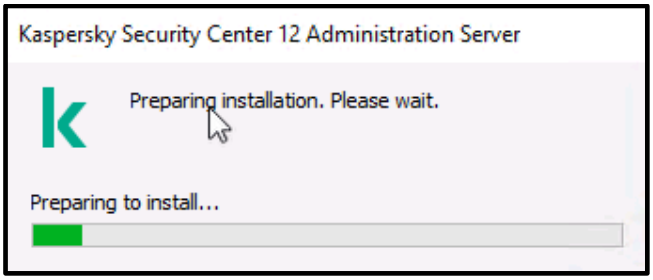
Please perform the following operations:

1. Log in on your PC using an account with administrative privileges.
2. Install **MS SQL Server Express Edition** or **MS SQL Server** depending on your system scale. Follow Microsoft installation guideline.
3. Copy **ksc_12.2_full_en.exe** from the supplied distribution package to the desktop and launch it.
4. Acknowledge UAC for the file launch if requested.

[4] As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a newer **Hotfix** version has become available.

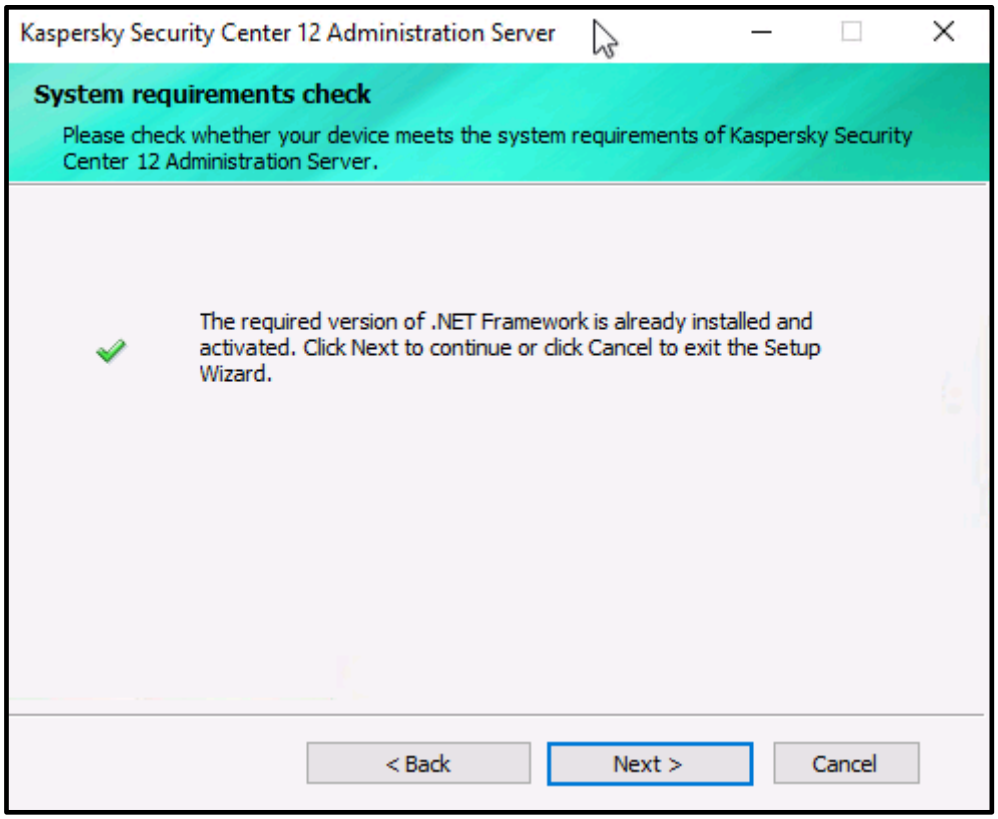
5. The following component selection window should pop up.

6. Choose **Install Kaspersky Security Center 12**. Wait for some minutes while the installation package is being uncompressed and the installation is being prepared.

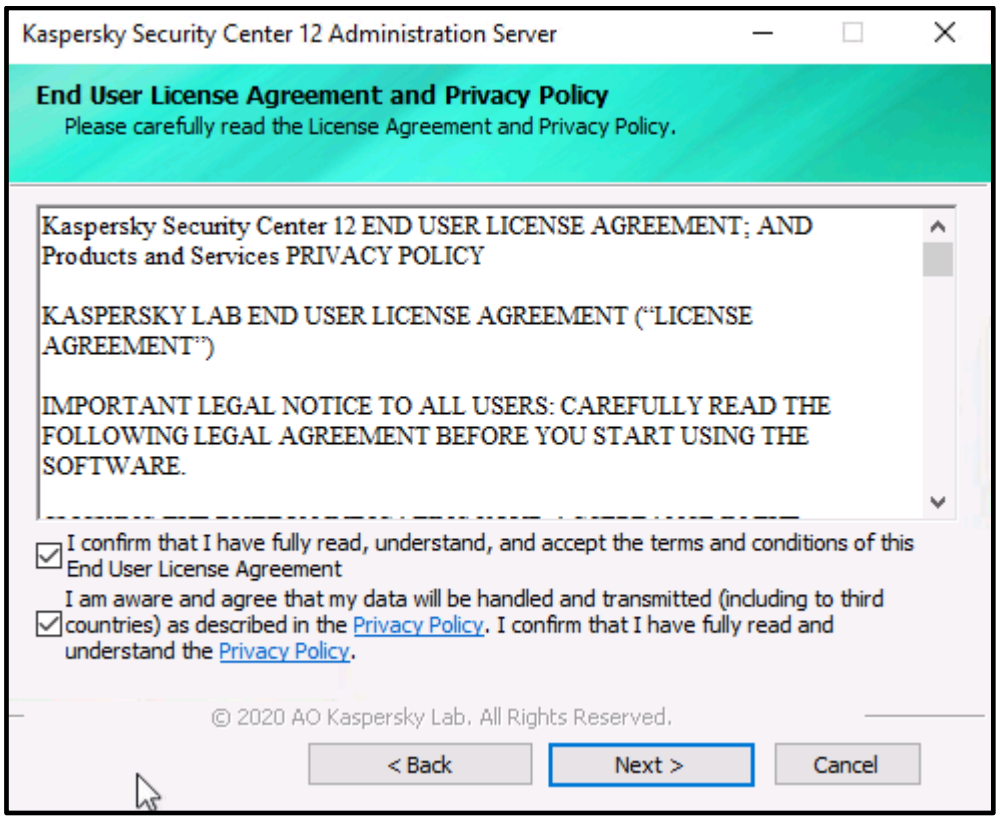


7. The following setup wizard should appear. Click **Next >**.

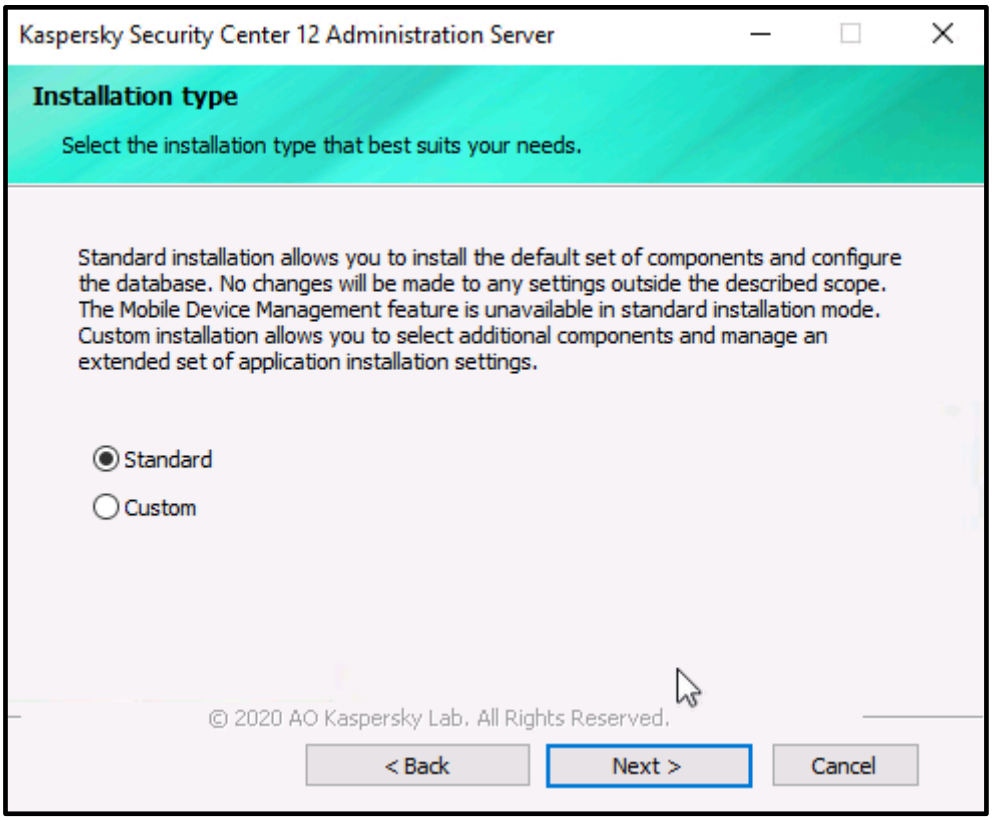
8. Please make sure that the system has passed the requirements check and press **Next >**.



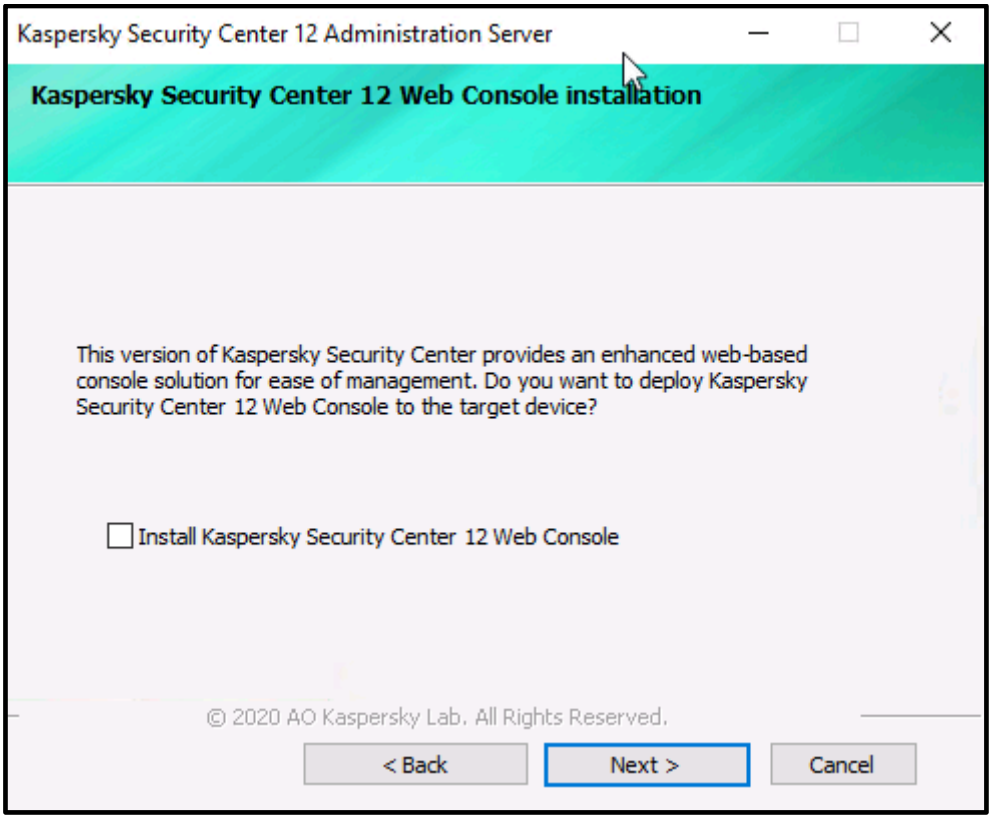
9. Accept the terms of the **License Agreement** and click **Next >**.



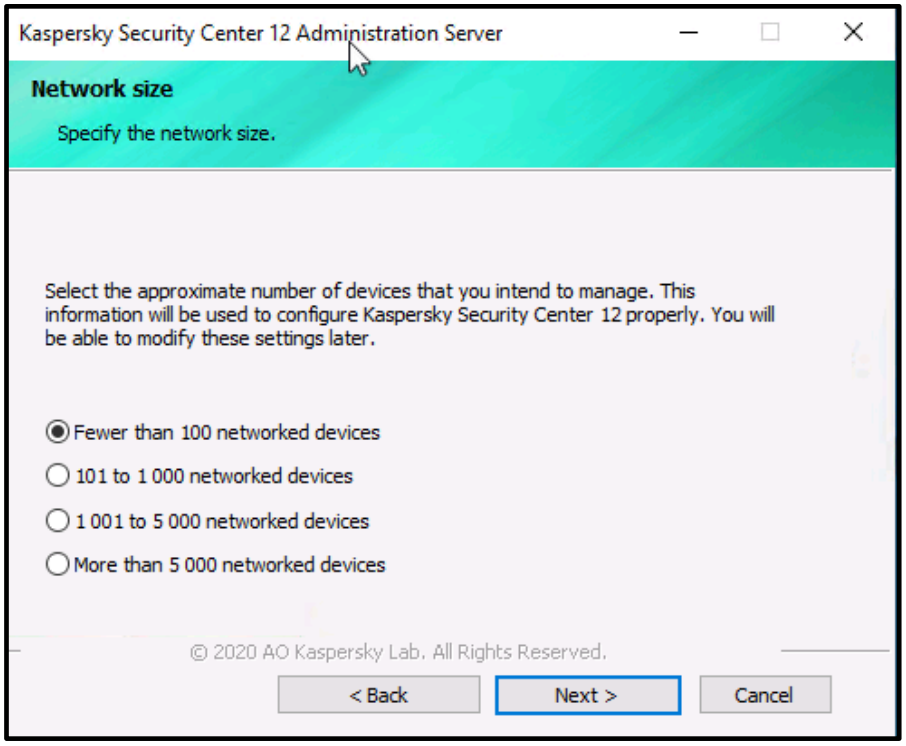
10. Select **Standard** as an installation type and click **Next >**.



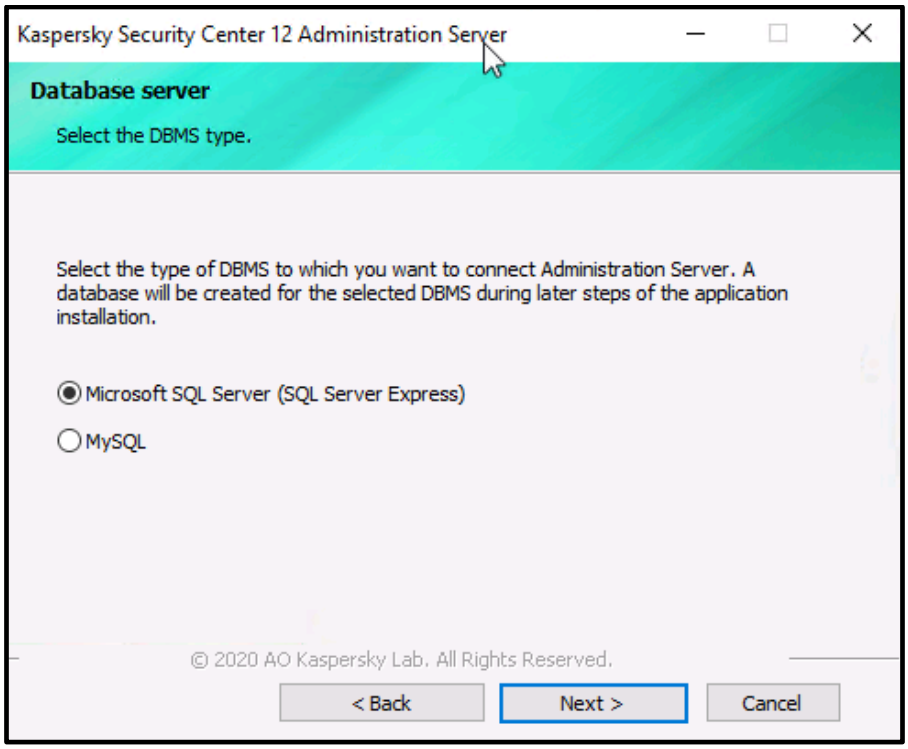
11. You can optionally install the **Web Console** but its operation is not covered within this manual. Click **Next >**.



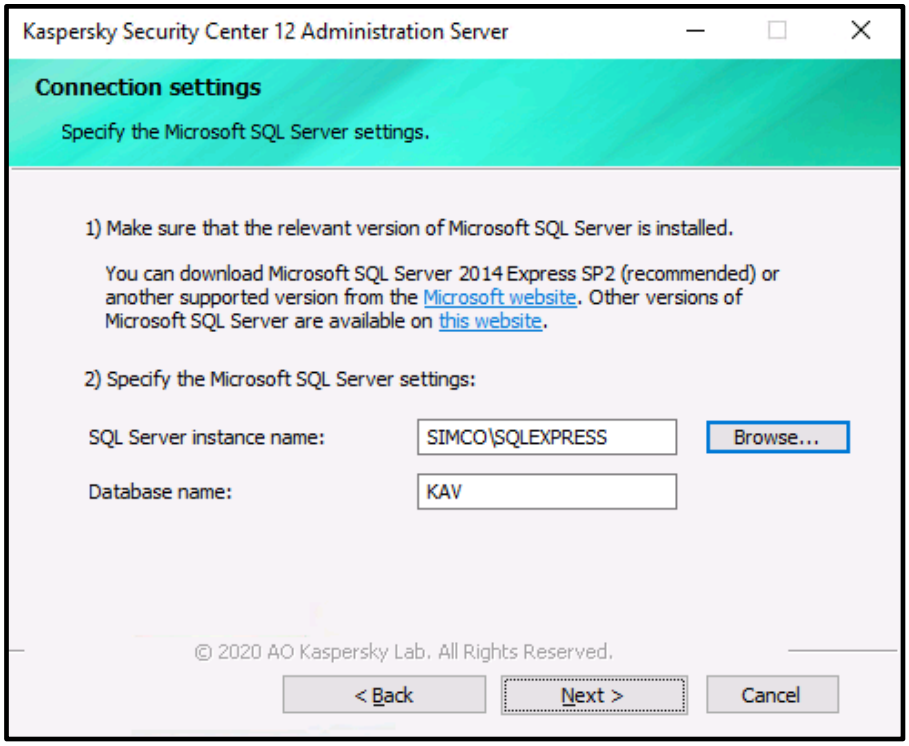
12. Select **Fewer than 100 network devices** (this option normally fits most of the industrial installations) and click **Next >**.



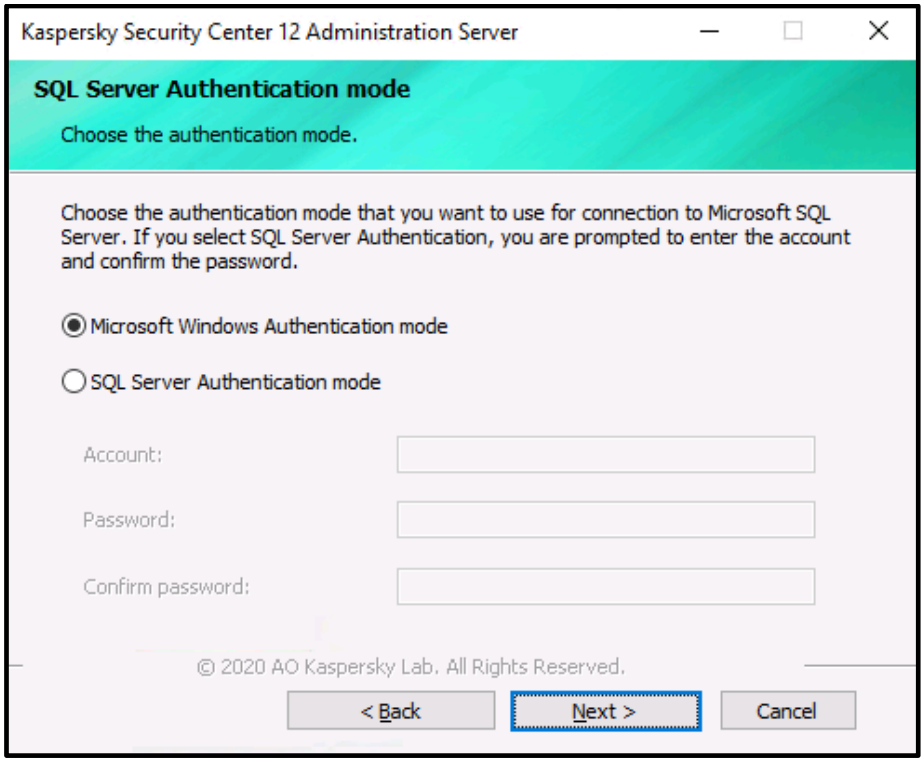
13. Specify the **Database server** type as shown below and click **Next >**.



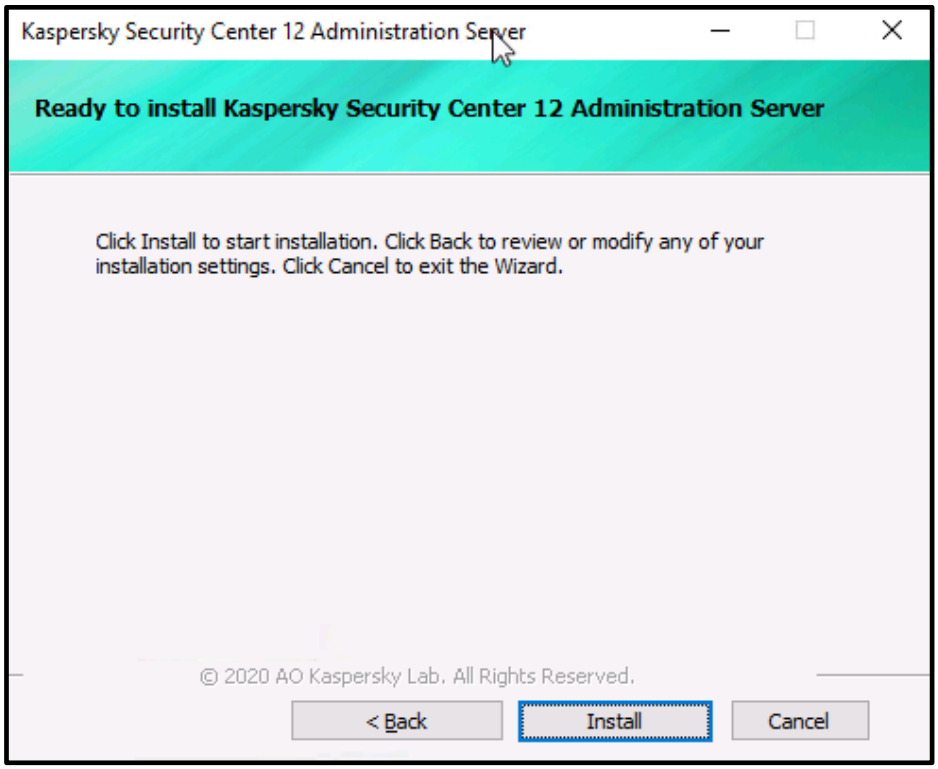
14. Select the **SQL Server** instance using the **Browse…** button, leave the **Database** name intact and click **Next>**.



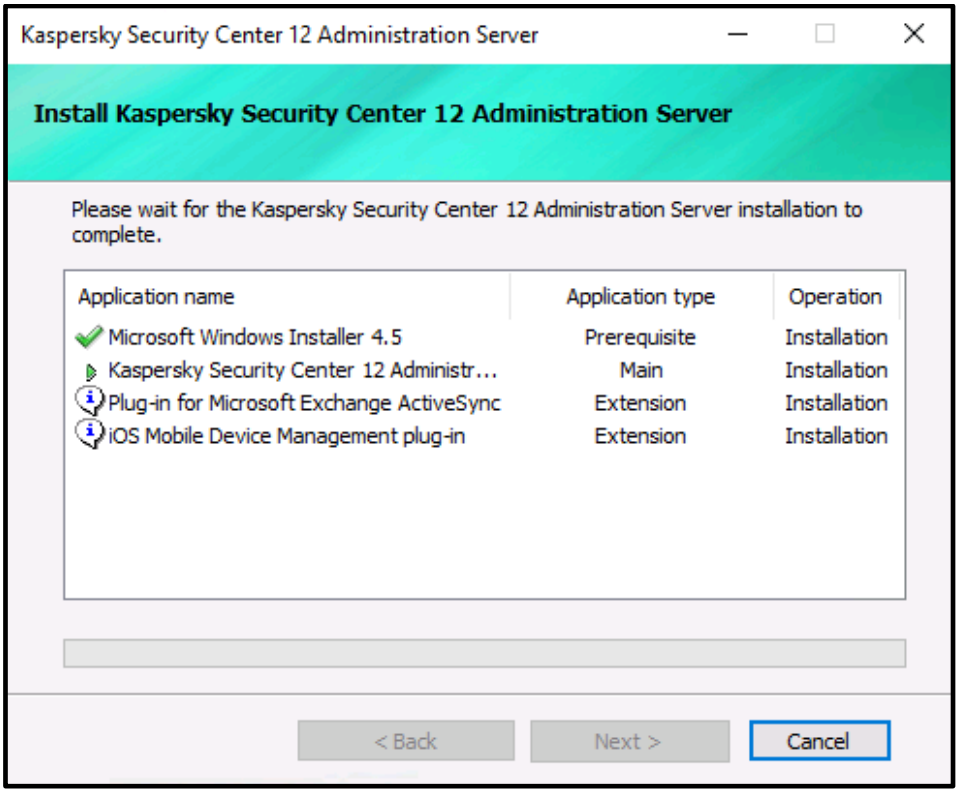
15. Choose the appropriate **SQL Server authentication** method. It should match the one you specified during the **SQL Server** installation. Click **Next >**.



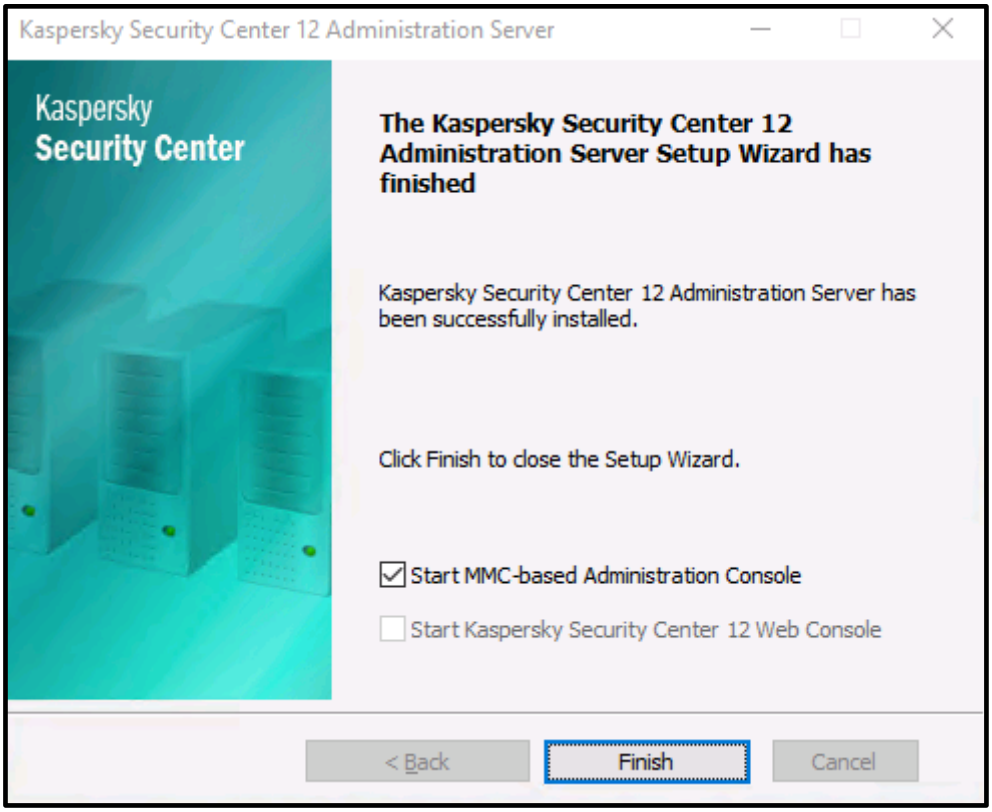
16. Confirm the installation start in the **Ready to install…** window by clicking **Install**.



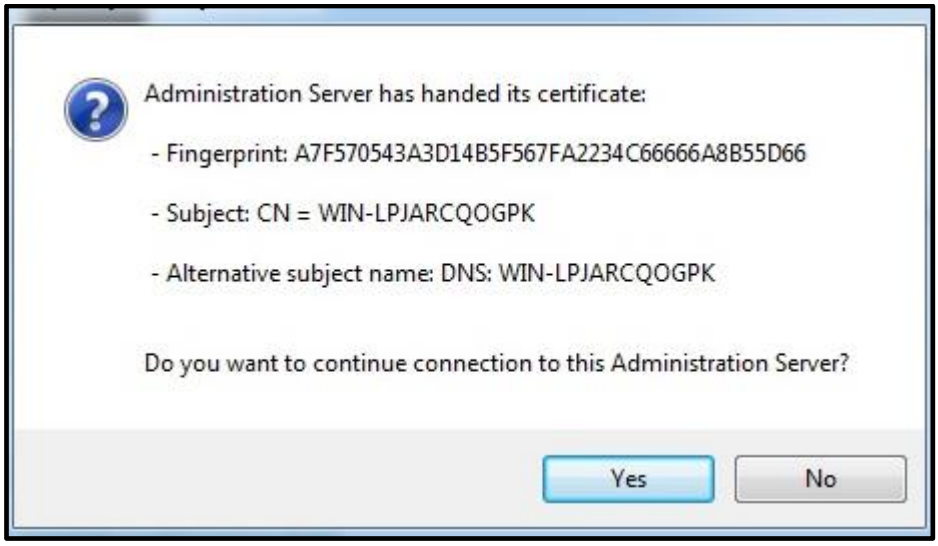
17. Wait until the installation process is completed. Throughout the installation, its progress is displayed in the following window.



18. When the installation is complete, the following window pops up. Only check **Start as MMC-based Administration Console** and click **Finish**.



19. Press **Yes** in the following window in order to launch **Administration Console** and make it use an encrypted connection to the server. This finalizes the **KSC** installation.

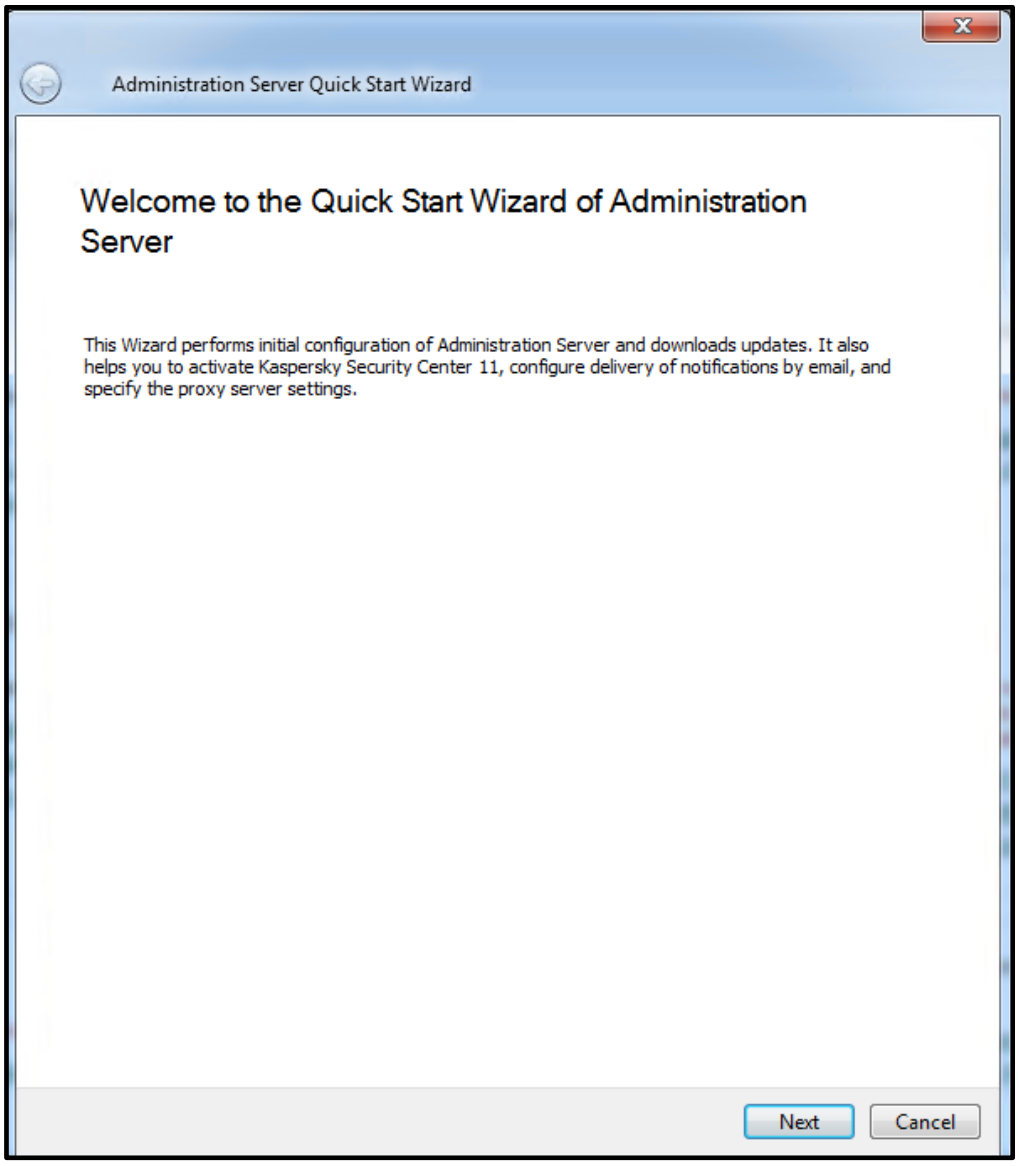


Initial configuration of KSC

The **KSC Administration Console** automatically starts up after the **KSC** server core components are installed[5]. Please note that the screenshots presented hereafter mainly refer to **Kaspersky Security Center 11**. You should not be confused by the version mismatch since all the settings are applicable and identical for version **12**.

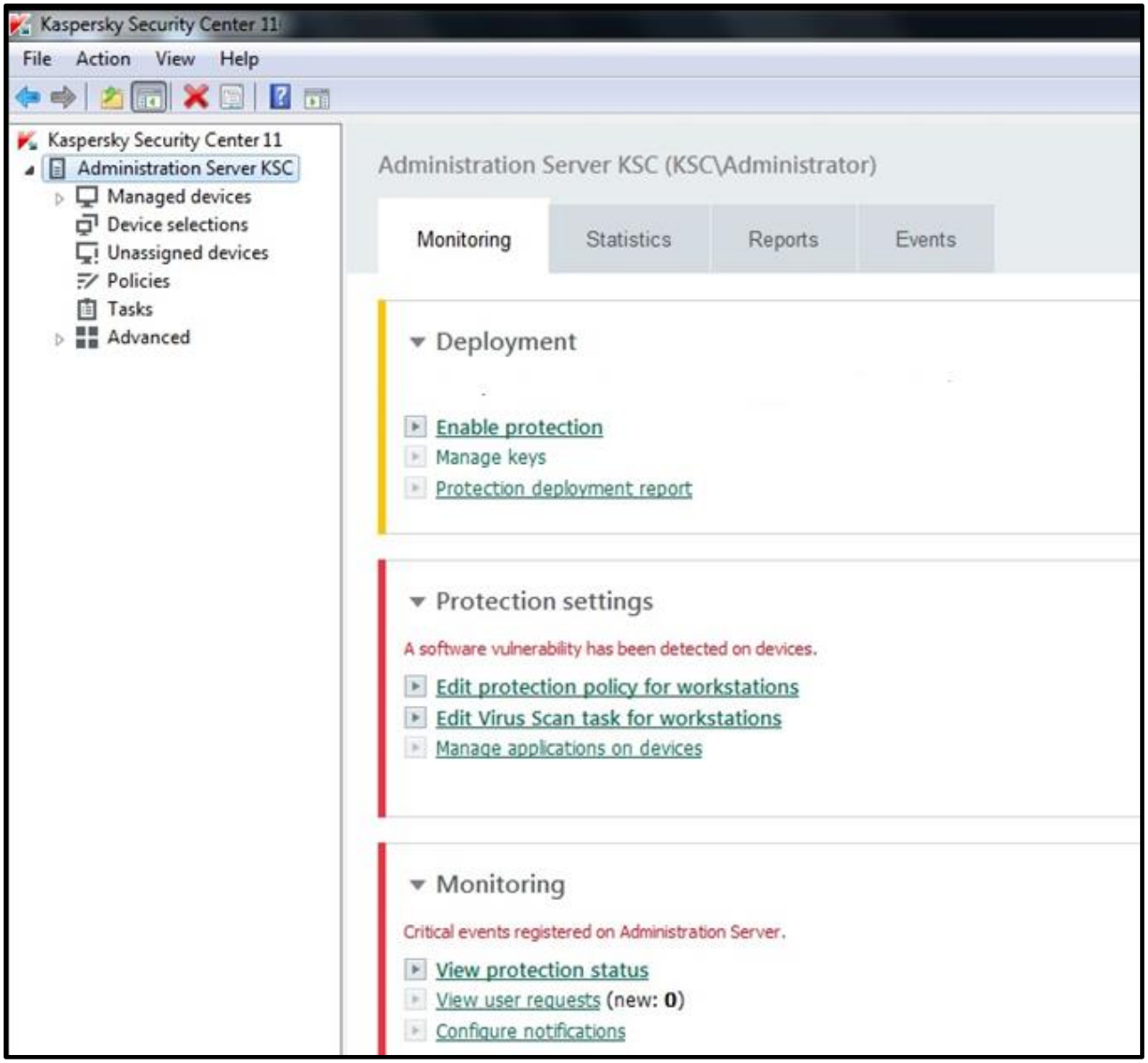
Please perform the following operations to apply basic settings to **KSC**:

1. Cancel the **KSC Administration Server Quick Start Wizard** if it has emerged. We are not going to use it.

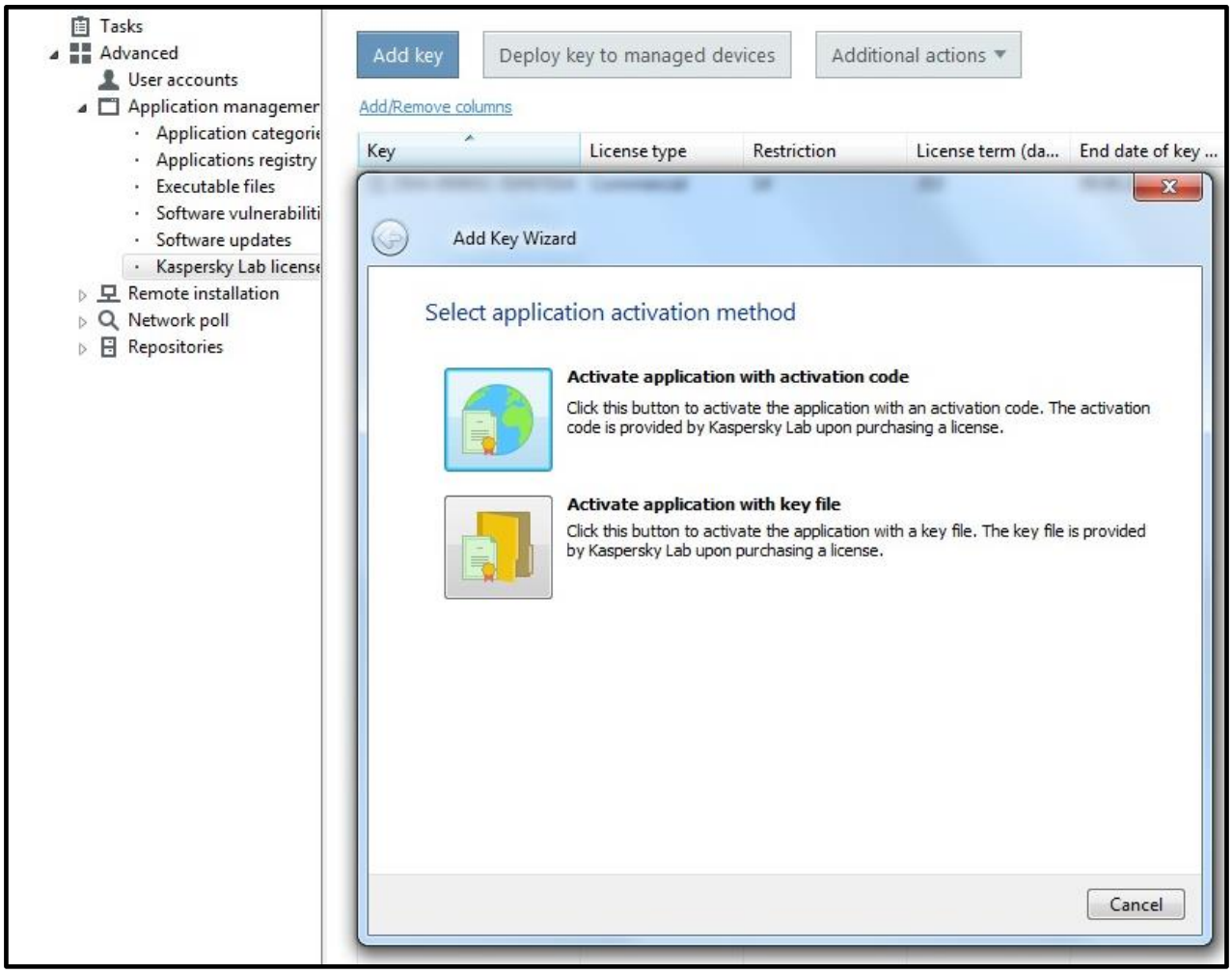


[5] The other way of calling **KSC Administration Console** is using the **Kaspersky Security Center 12** shortcut located on the **Start** menu.

2. Go to the **Administration Server** hierarchical node located in the left-hand pane. The following multi-tab administration pane should appear on the right.

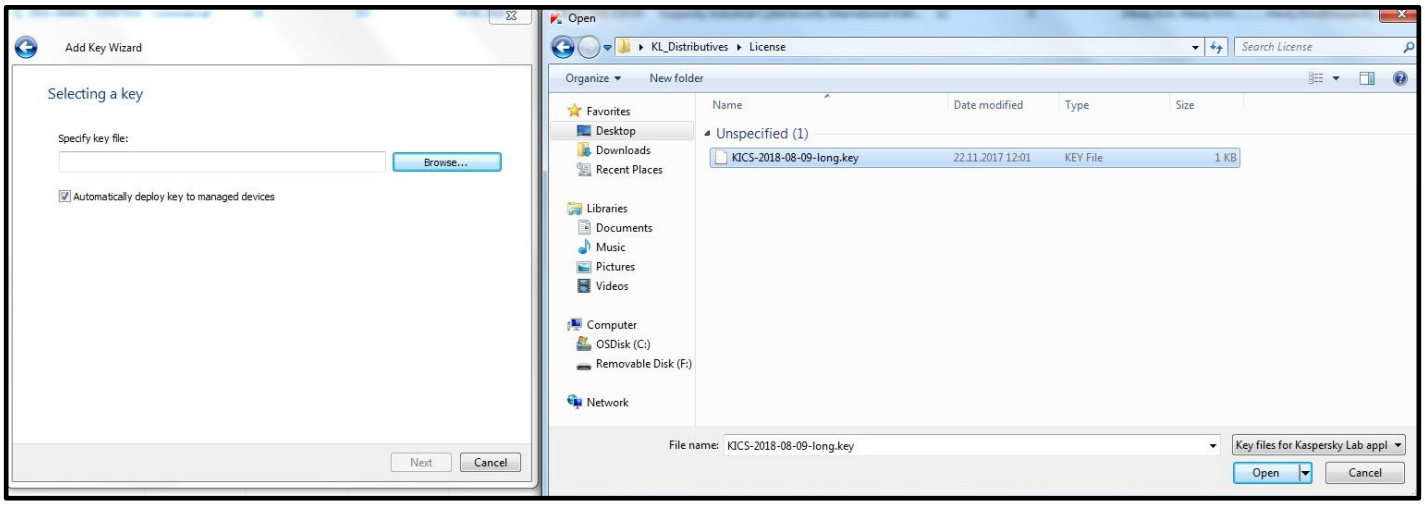


3. Remaining in the **Monitoring** tab, click **Manage keys** to view the list of installed licenses. Apparently, this list is initially blank.
4. Press the **Add Key** button to start the **Add Key Wizard** (as shown in the picture below).

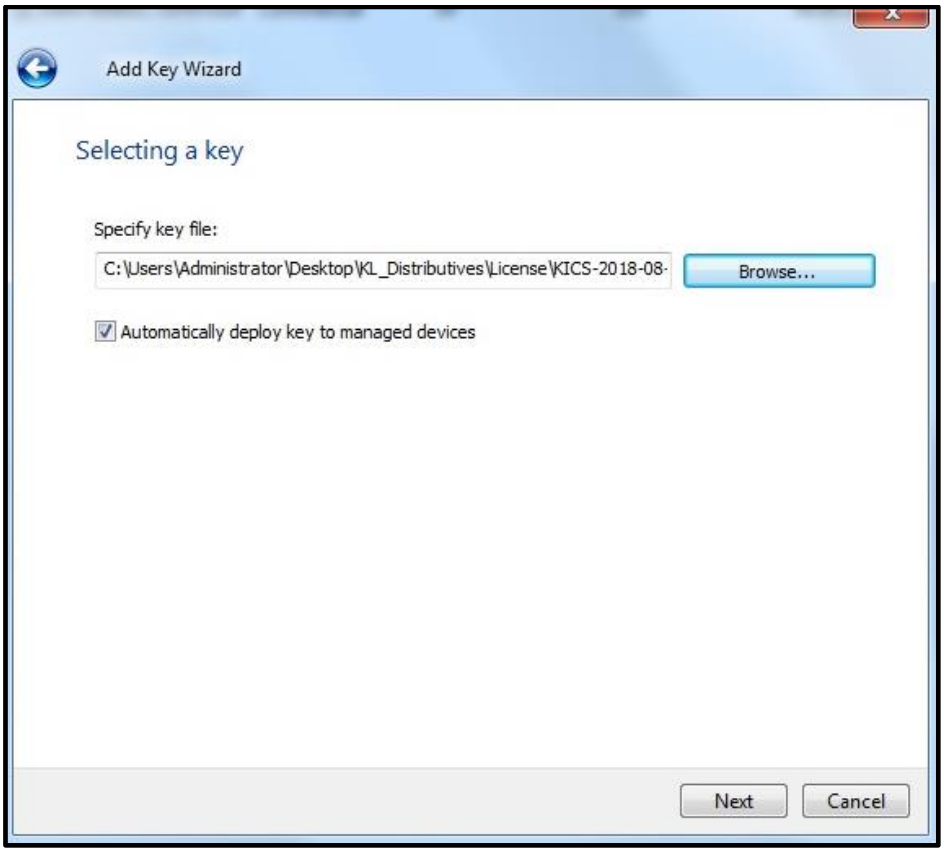


5. In the **Add Key Wizard** that appears, choose **Activate application with a key file**.

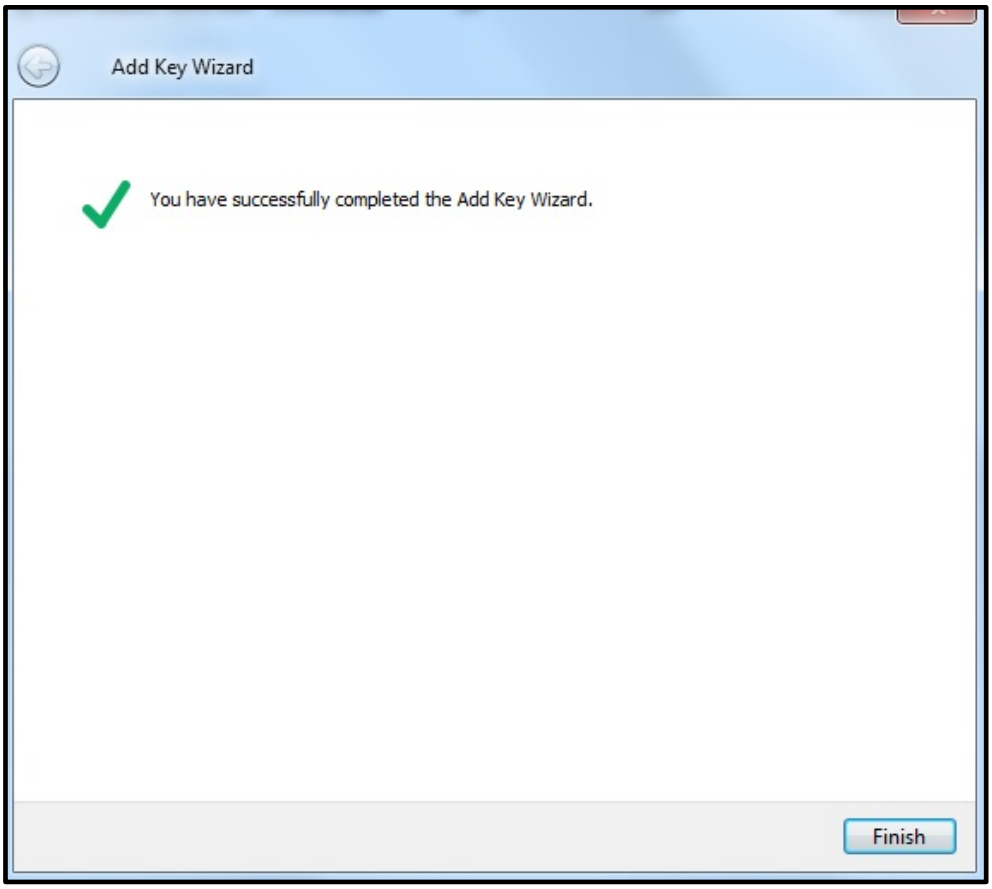
6. In the **Selecting a key** window, check **Automatically deploy key to managed devices** and press **Browse** to locate the key-file supplied. The key file should be supplied with the distribution package and should have the extension ***.key**.



7. After you have picked an appropriate key-file, press **Next**.

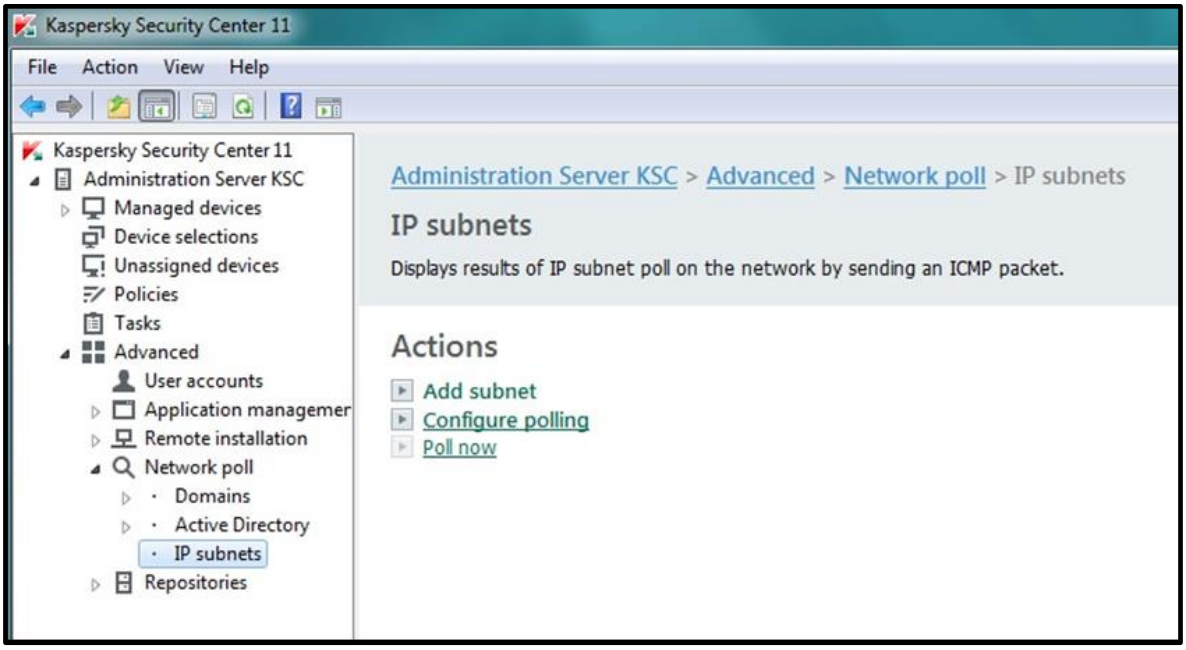


8. Please **Finish** to complete adding your key file.

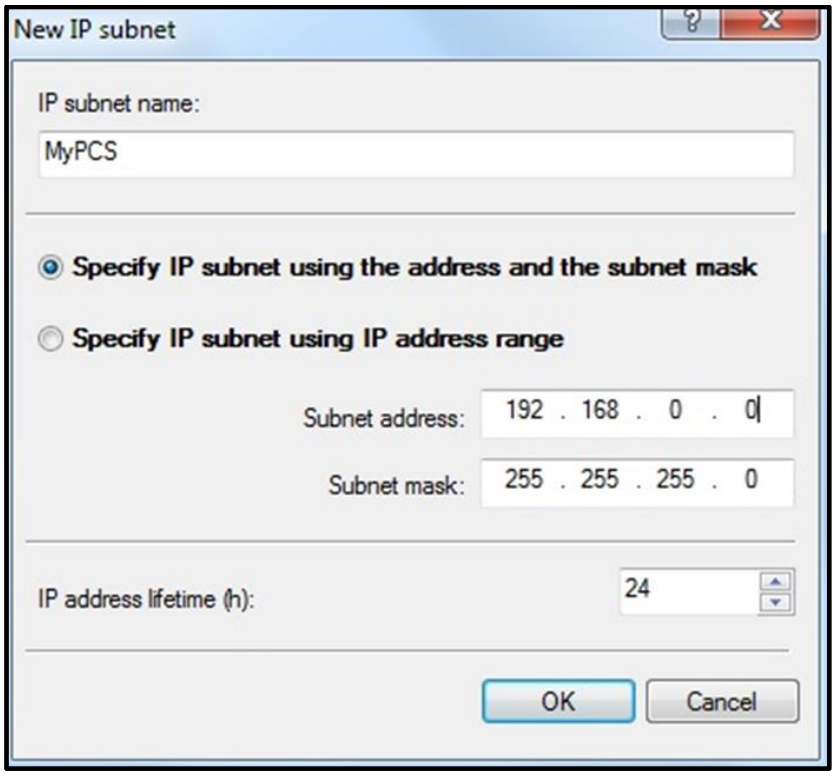


9. If the key file is valid, it should emerge on the list of installed licenses as shown below.

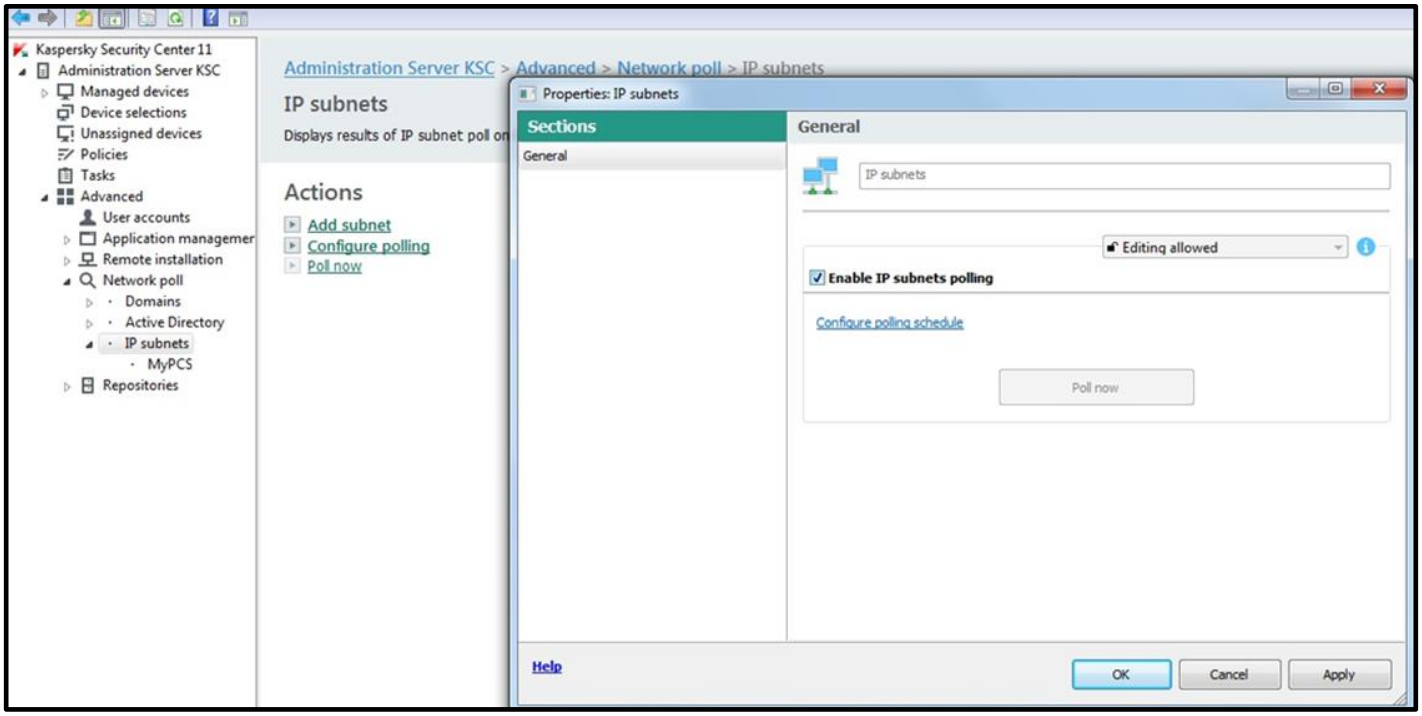
10. Using the navigation tree in the left-hand pane, now we go to the **Administration Server->Advanced->Network Poll->IP subnets** hierarchical node. Click **Add subnet** as shown below.



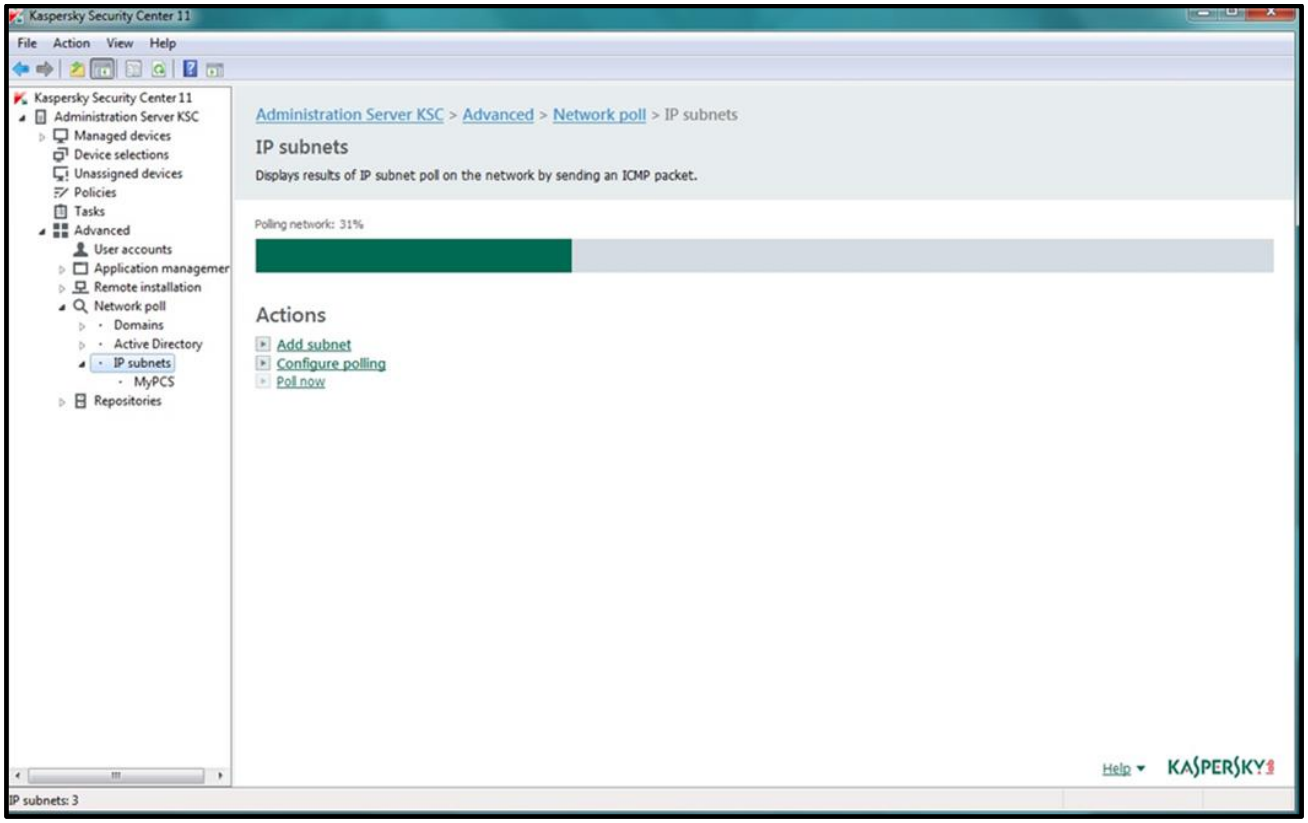
11. In the window that appears, specify the network polling details. In our case, we have named our control system network "**MyPCS**" and specified the IP subnet **(192.168.0.0/24)** that will be polled. Click **OK** when done.



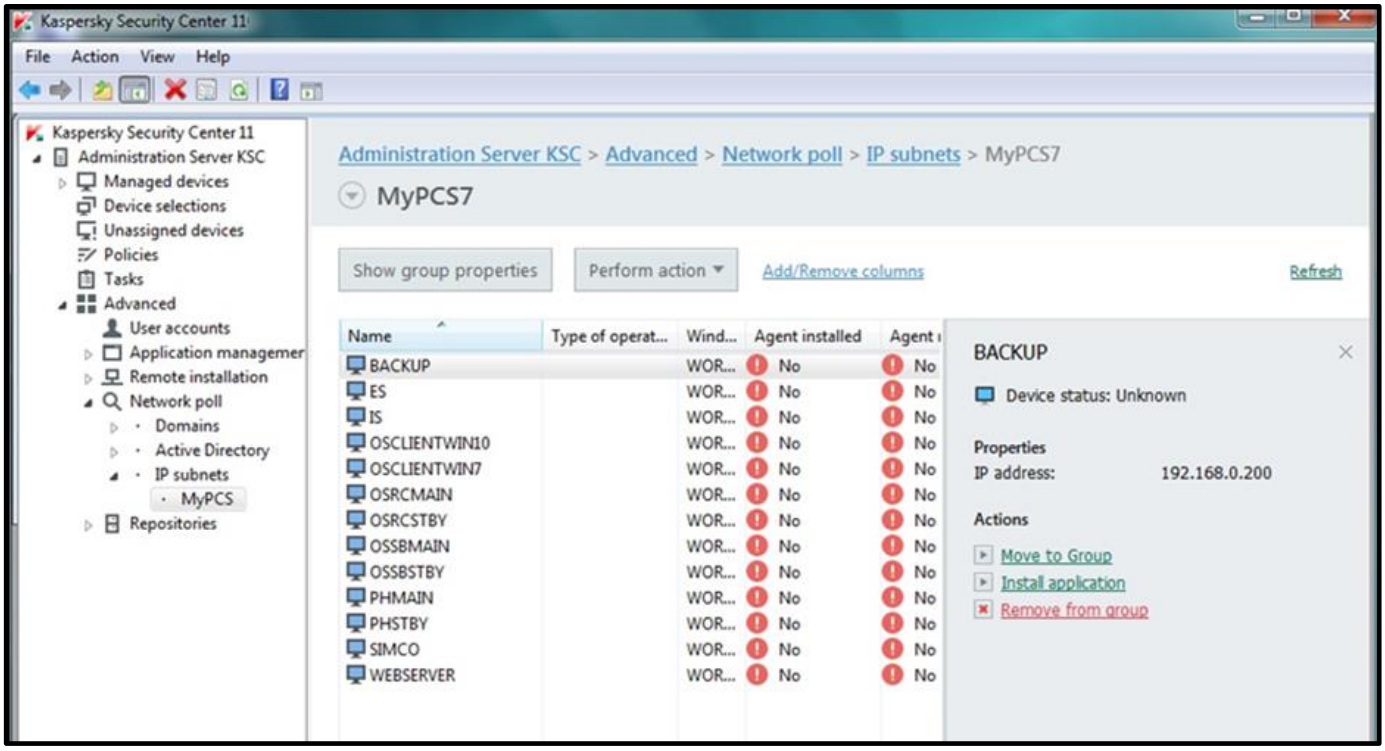
12. Click **Configure Polling** in the right-hand pane. The following window should appear. Check **Enable IP subnets polling** and press the **Poll now** button. Click **OK** to close the popup window.



13. Wait for some time until the polling process is complete. The polling time depends on the scale of your network. You can track percentage of completion by viewing the progress bar as shown below.



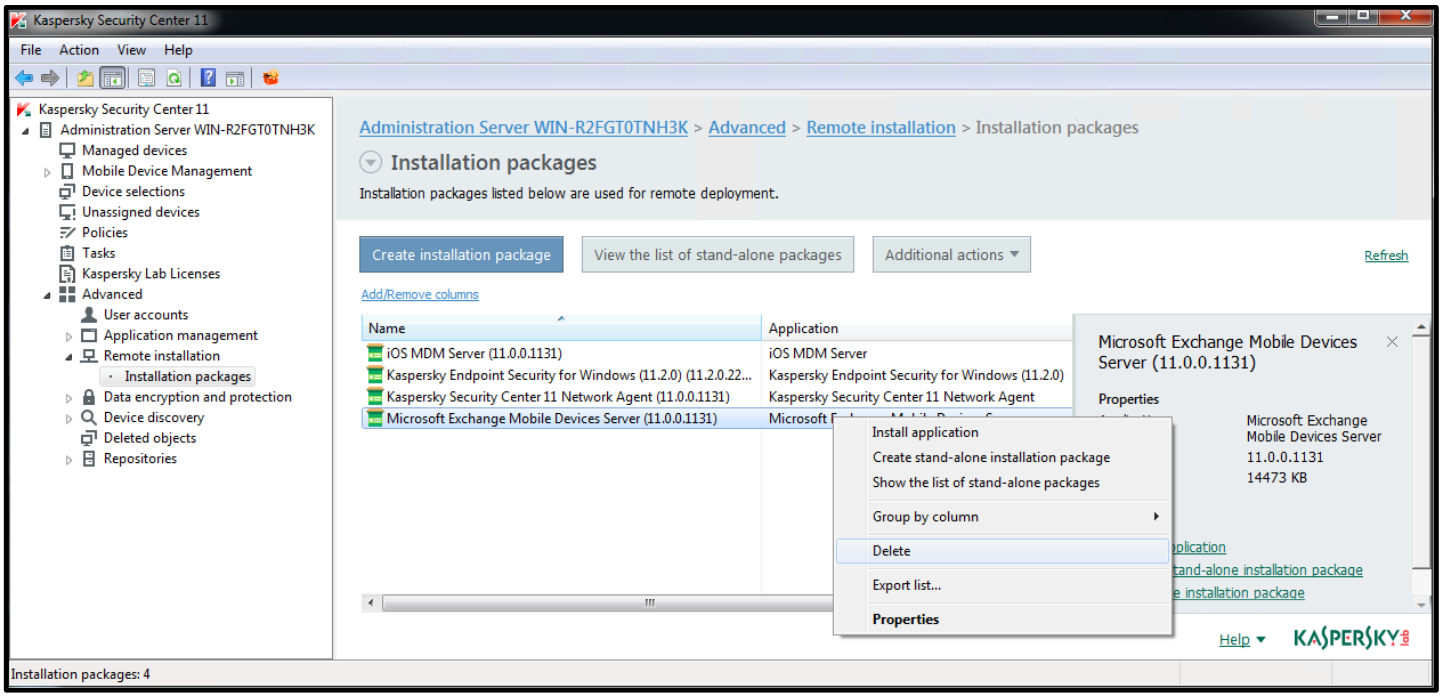
14. After the network polling is 100% complete, go to the newly created network (in our example, **MyPCS**) and view the list of all the hosts discovered on your network.



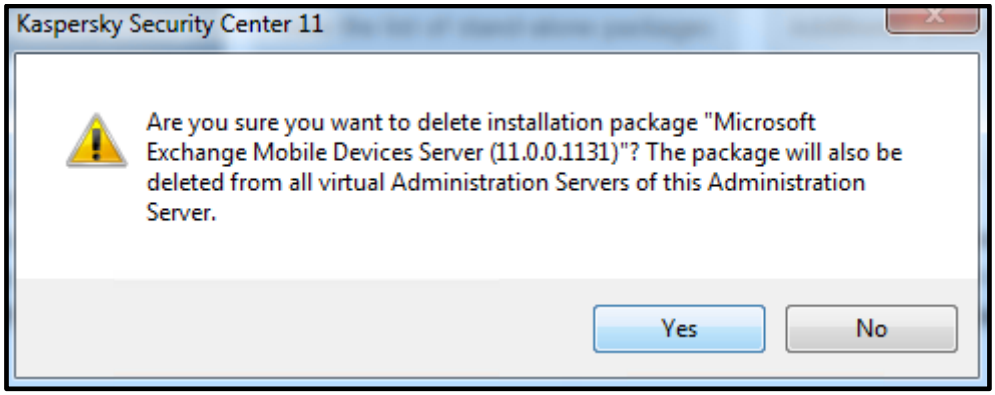
15. In our case, we are going to proceed with the **SIMCO** host only. However, it is easy to replicate the same configuration techniques for multiple hosts[6] by placing them into respective managed devices groups.
16. Using the left-hand pane navigation tree, now we go to the **Administration Server->Advanced->Remote Installation->Installation packages** hierarchical node.

[6] Please note that in this document the terms “device”, “host” and “target computer” have the same meaning and are interchangeable.

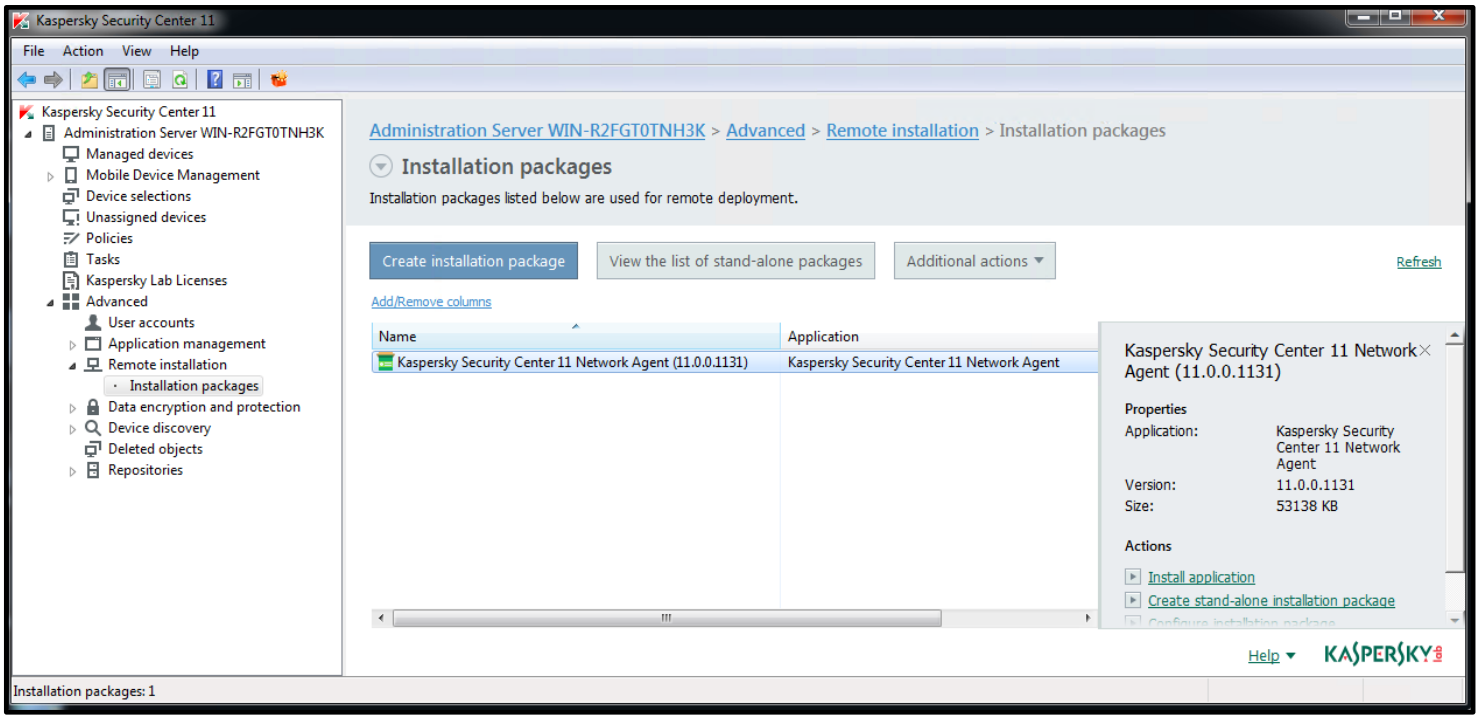
17. It is recommended to remove from the repository all the default packages **apart from Kaspersky Security Center Network Agent.** The latter will be required for the remote installation of **KICS for Nodes**.
18. Select every redundant package and in the context menu choose Delete as shown below.



19. For every software package, that is to be deleted, confirm its removal by pressing **Yes** in the confirmation window.



20. As mentioned before, you should end up with just one software package as shown below.

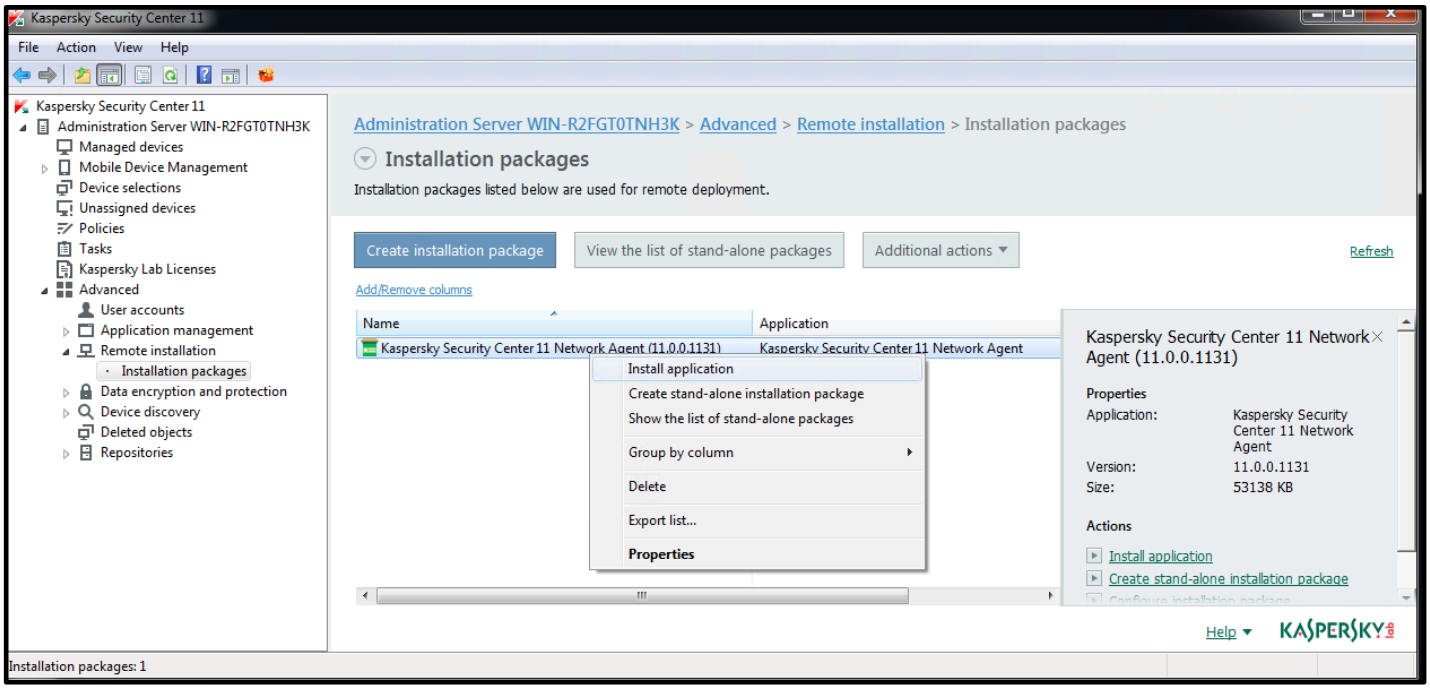


Remote installation of KLnagent onto target computers

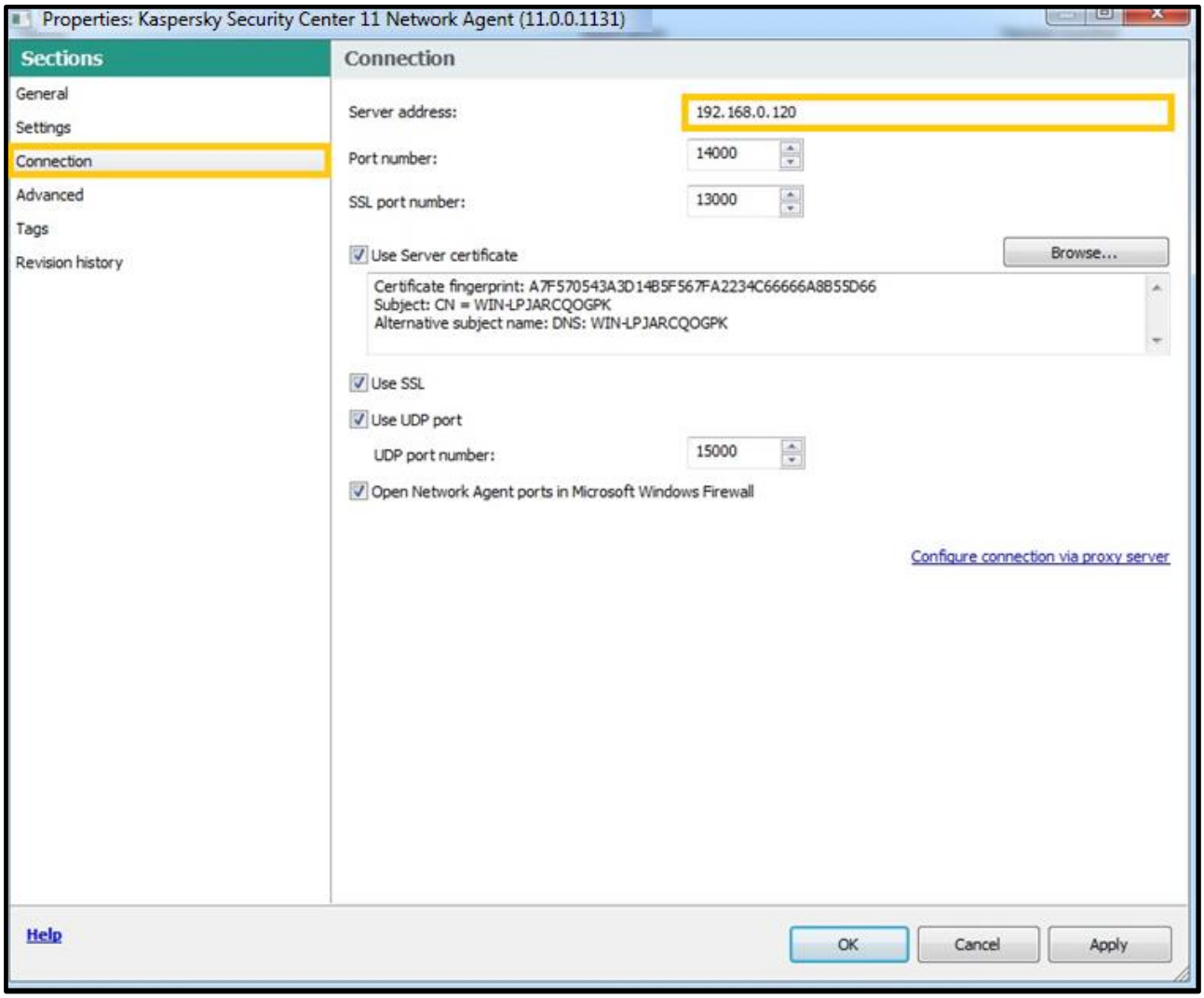
In order to make a host remotely manageable by **KSC**, we need to install the network agent **KLnagent** on that host. However, prior to the **KLnagent** installation, it is important to make sure that the **KSC** computer has network access to the administrative shares located on the **SIMCO** device (such as \\SIMCO\C$ or \\SIMCO\ADMIN$). If not, please set it up first and memorize your administrative credentials.

In order to carry out the remote installation of **KLnagent**, please perform the steps given below. Please also note that steps 1-2 can only be executed as long as your **KSC** server has a static IP-address, otherwise it is recommended skipping to step 3.

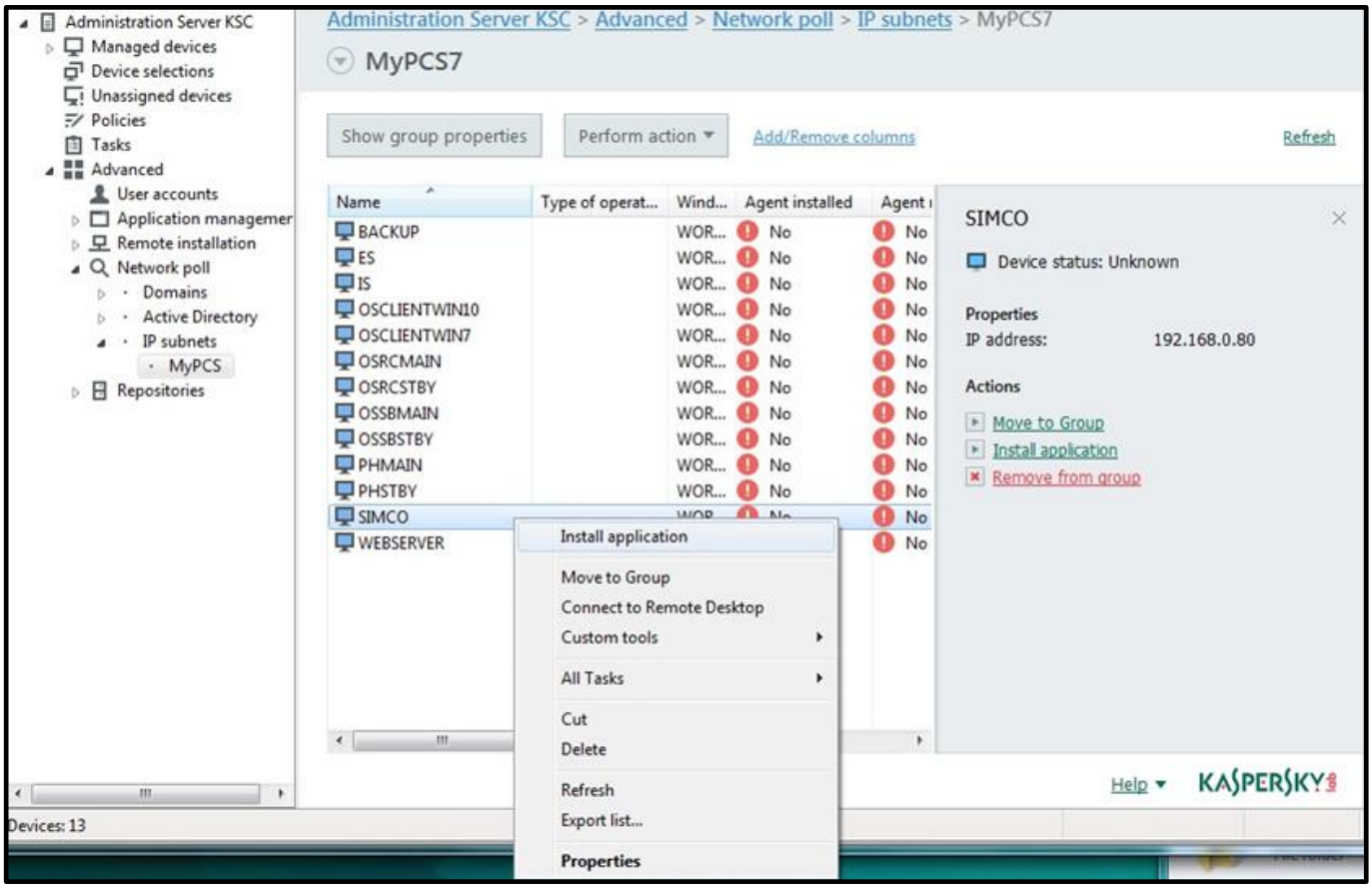
1. Go to the **Advanced->Remote installation->Installation packages** hierarchical node and right-click on the **Kaspersky Security Center 11 Network Agent installation** package. In the context menu, select **Properties**.



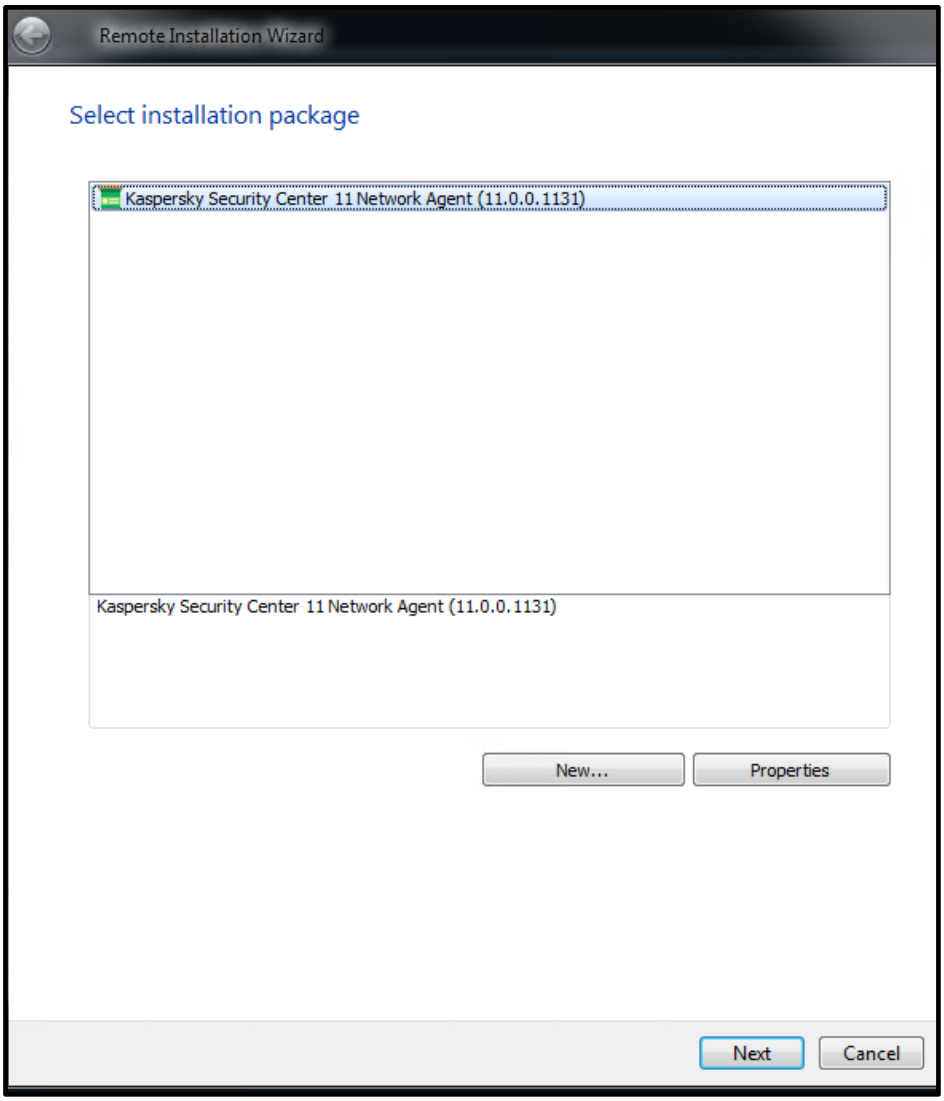
2. In the window that appears, go to **Connection**. Find the **Sever address:** text field and replace the symbolic name of the **Kaspersky Security Center** server with its explicit IP-address. The other settings should look as shown below. Press **Apply** and **OK** to close the window.



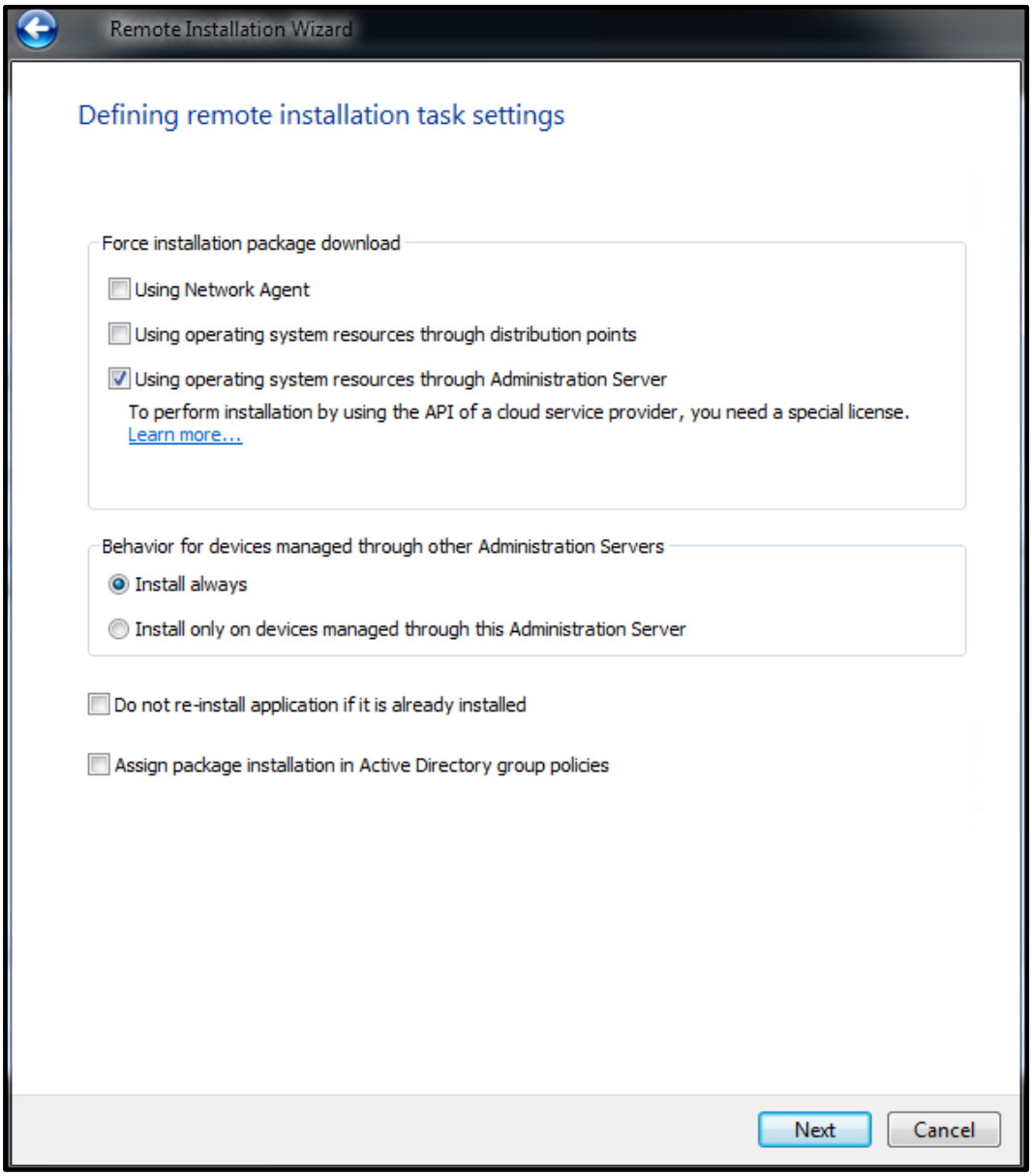
3. Now, proceed to **Advanced->Network Poll->IP subnets**. From the list of discovered devices select the one you want to install **KLnagent** on**.** In our example, it is **SIMCO**. Right-click on it and select **Install Application** in the context menu as shown below.



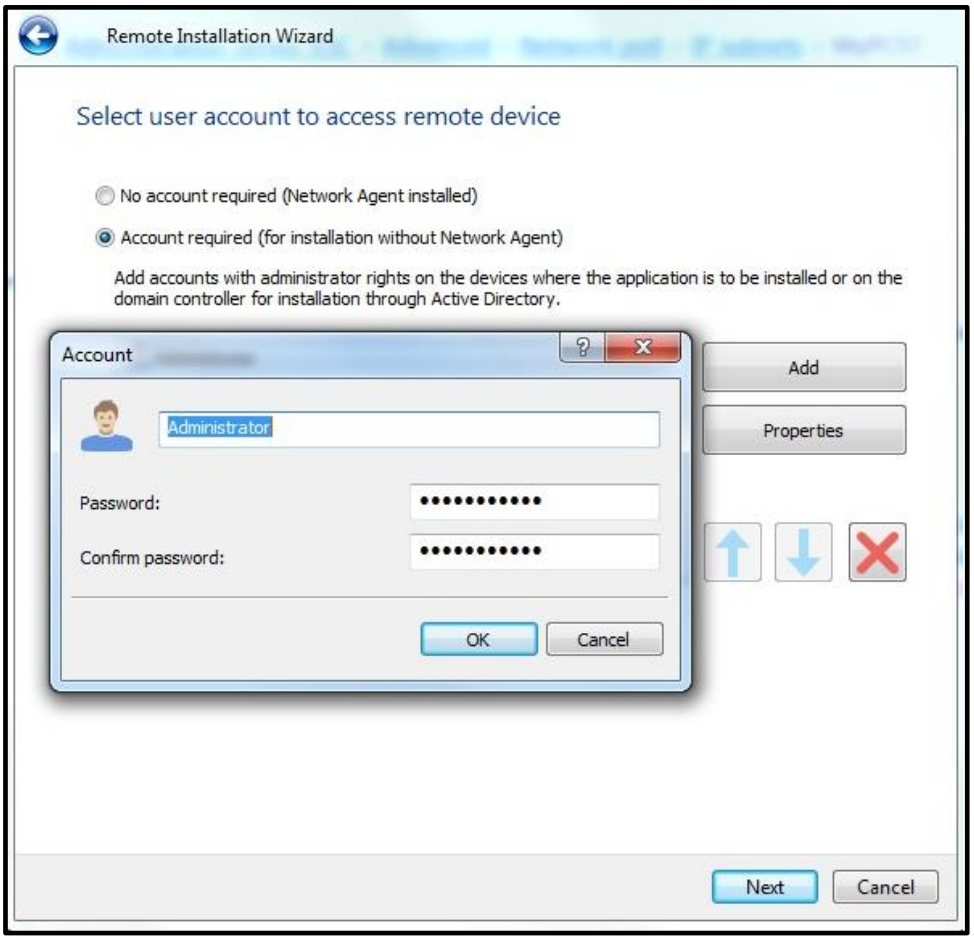
4. In the **Remote Installation Wizard** select **Kaspersky Security Center 11 Network Agent** and click **Next**.



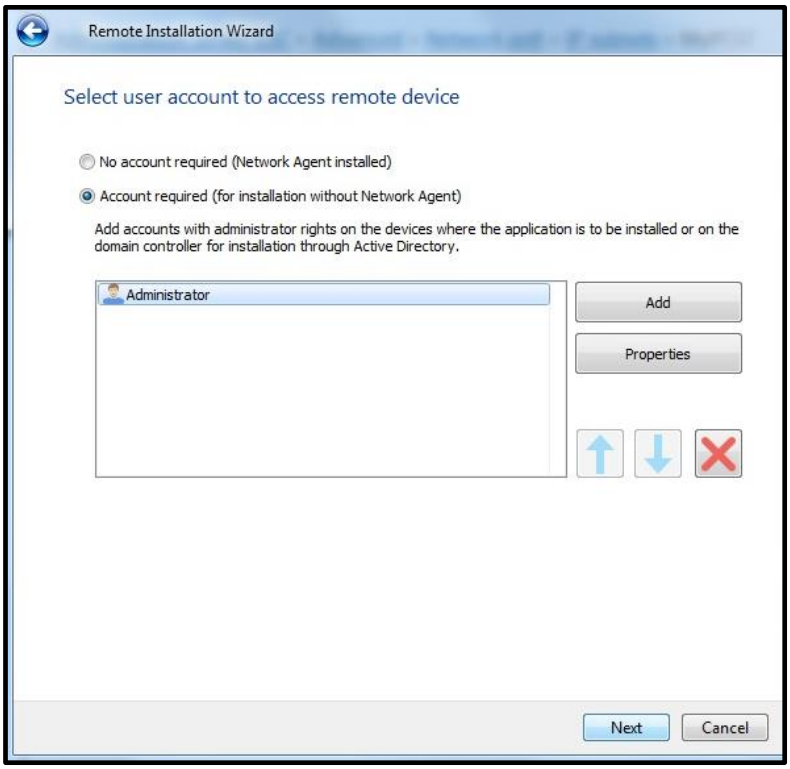
5. Specify the remote installation settings as shown below. Click **Next**.



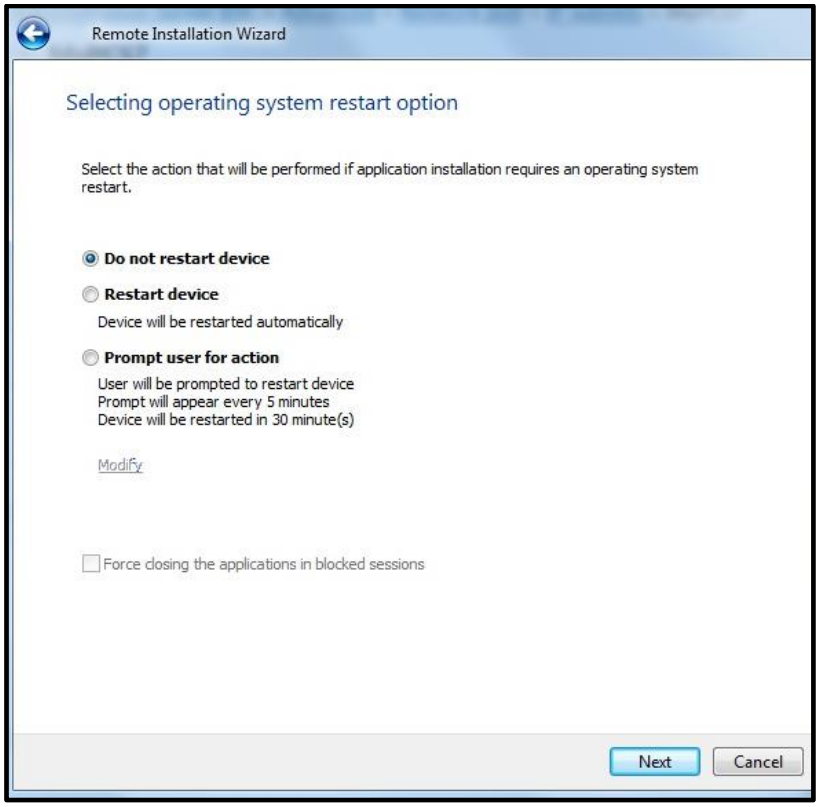
6. Check **Account required (for installation without Network Agent)**, click **Add** and specify your administrator's credentials that enable access to the administrative shares of the remote host (\\SIMCO\ADMIN$, in our case). Click **OK**.



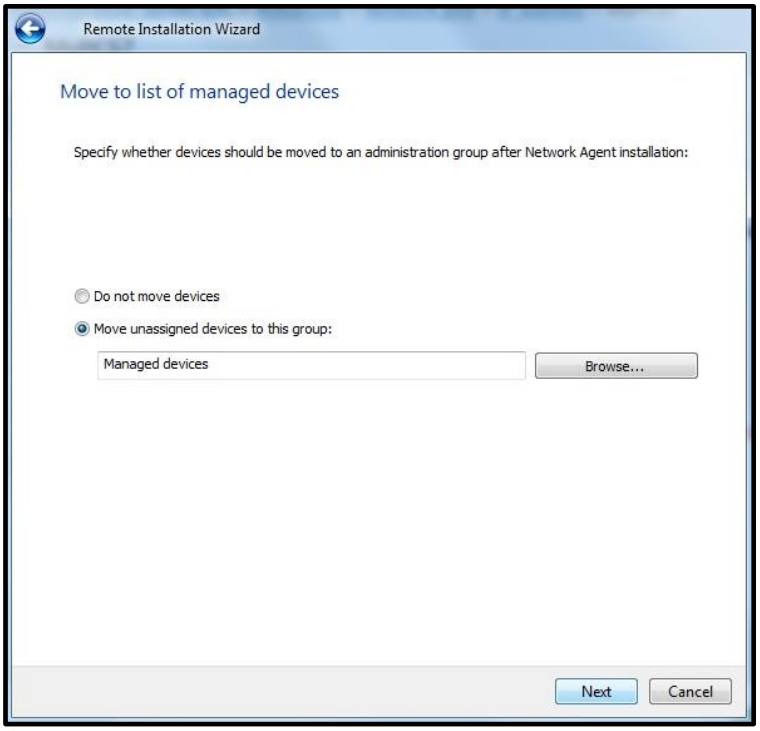
7. When done, click **Next**.



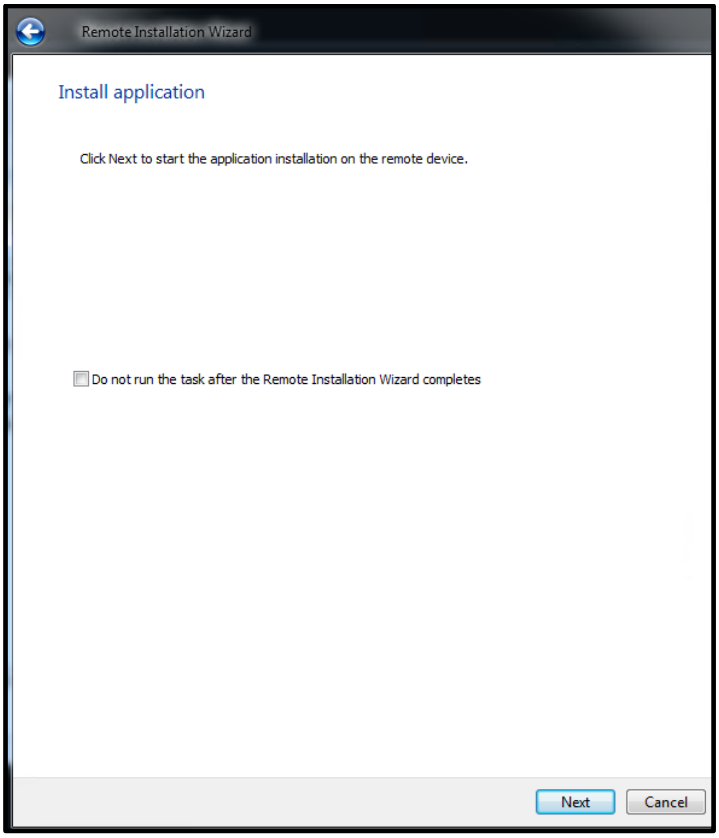
8. In the **Selecting operating system restart option** window, select **Do not restart device** as an operating system restart option. Click **Next**.



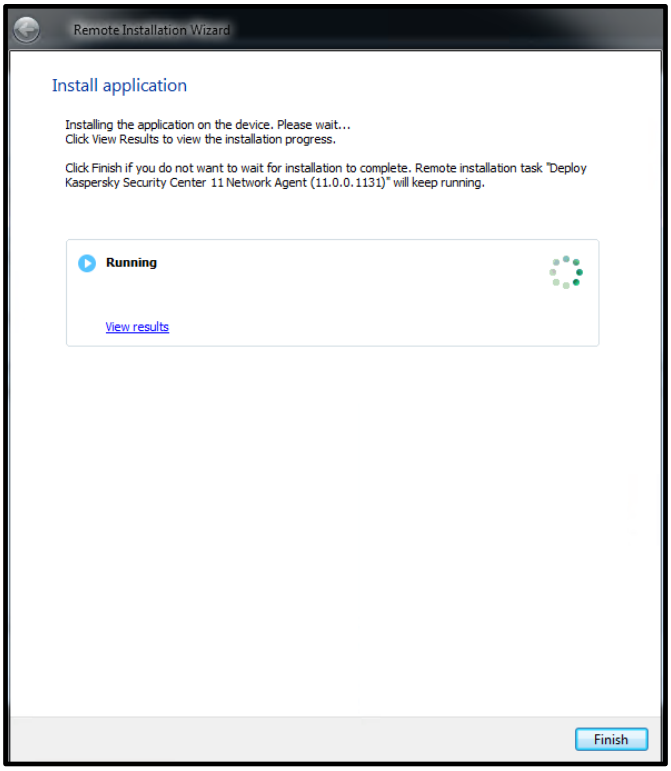
9. Check **Move unassigned devices to this group** and choose **Managed devices** as a destination group. Click **Next**.

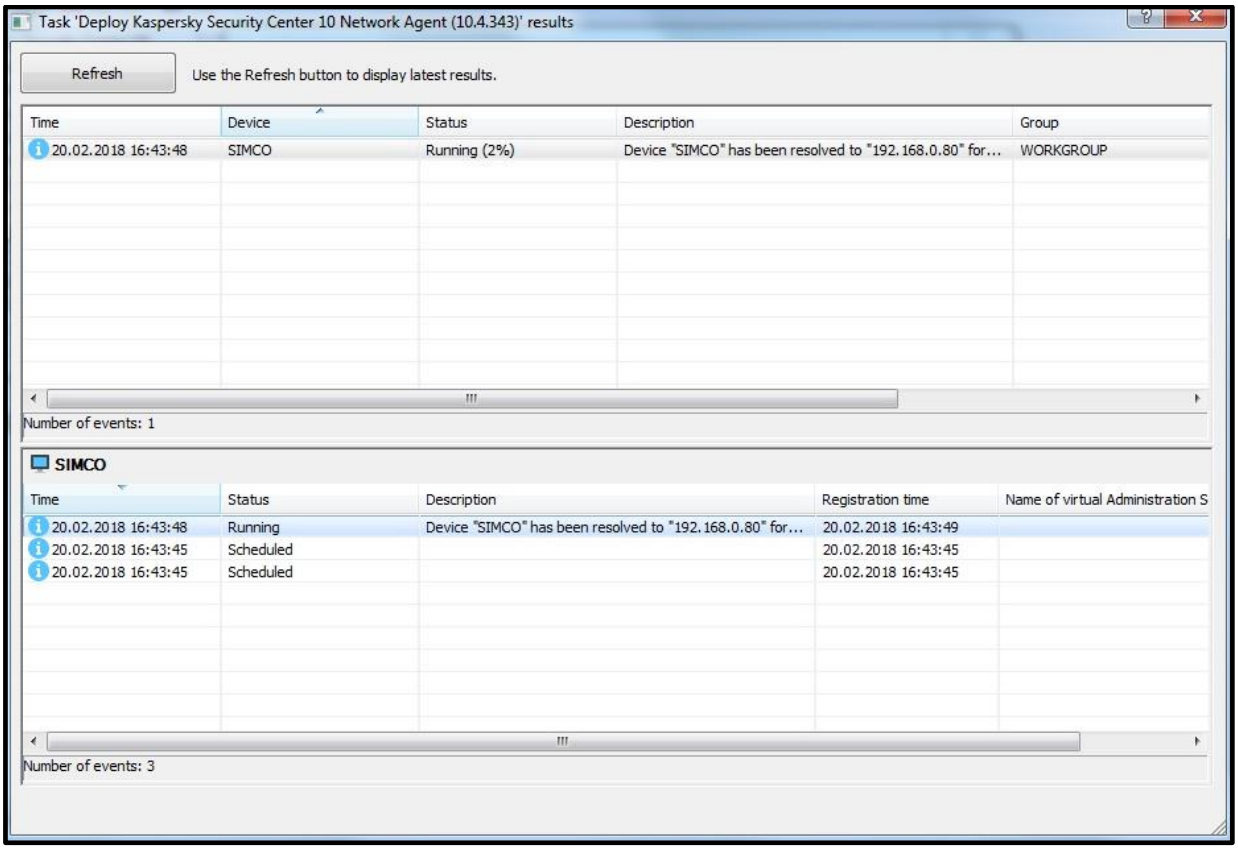


10. Leave the default settings and start the installation by clicking **Next**.

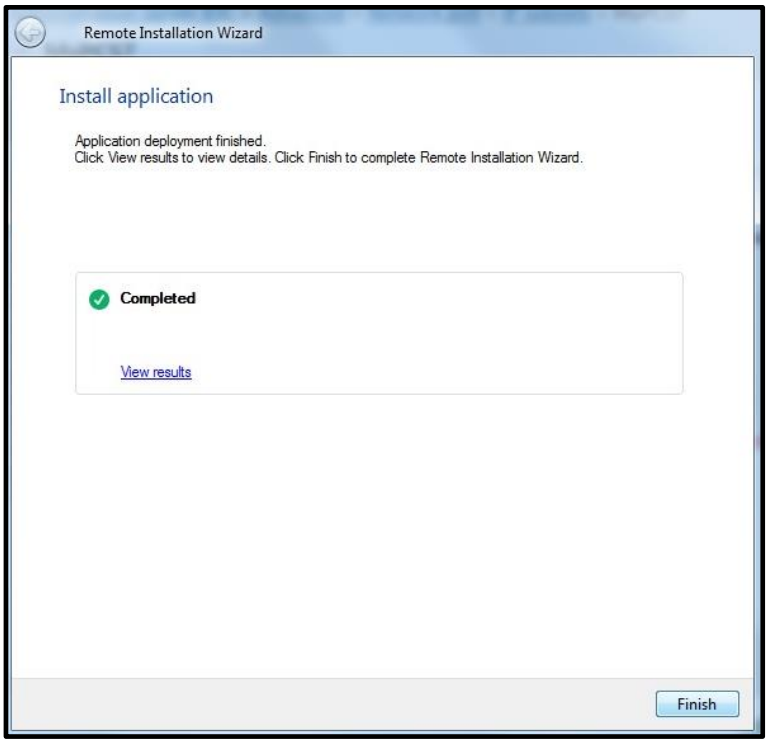


11. Wait until the installation process is complete. It can take up to 10 minutes. You can get more details on the installation progress if you click **View Results**.

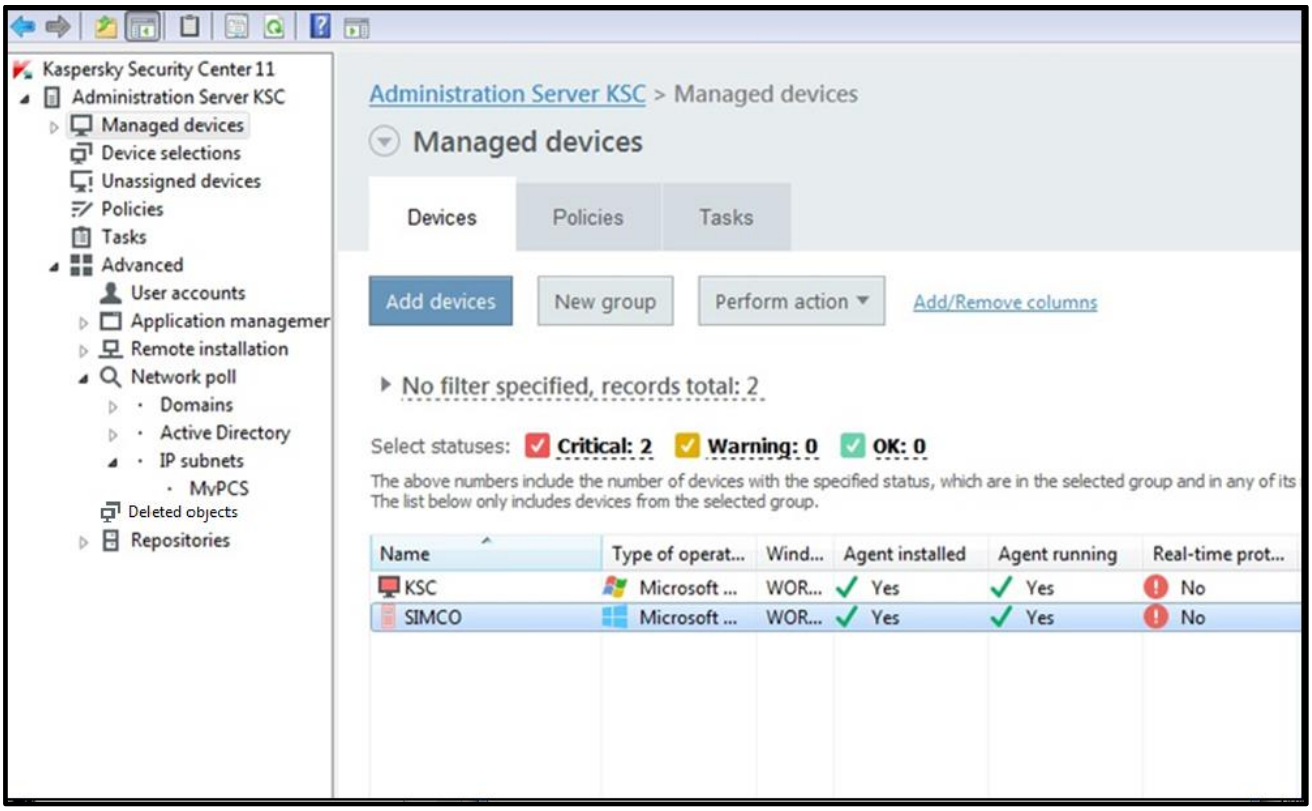




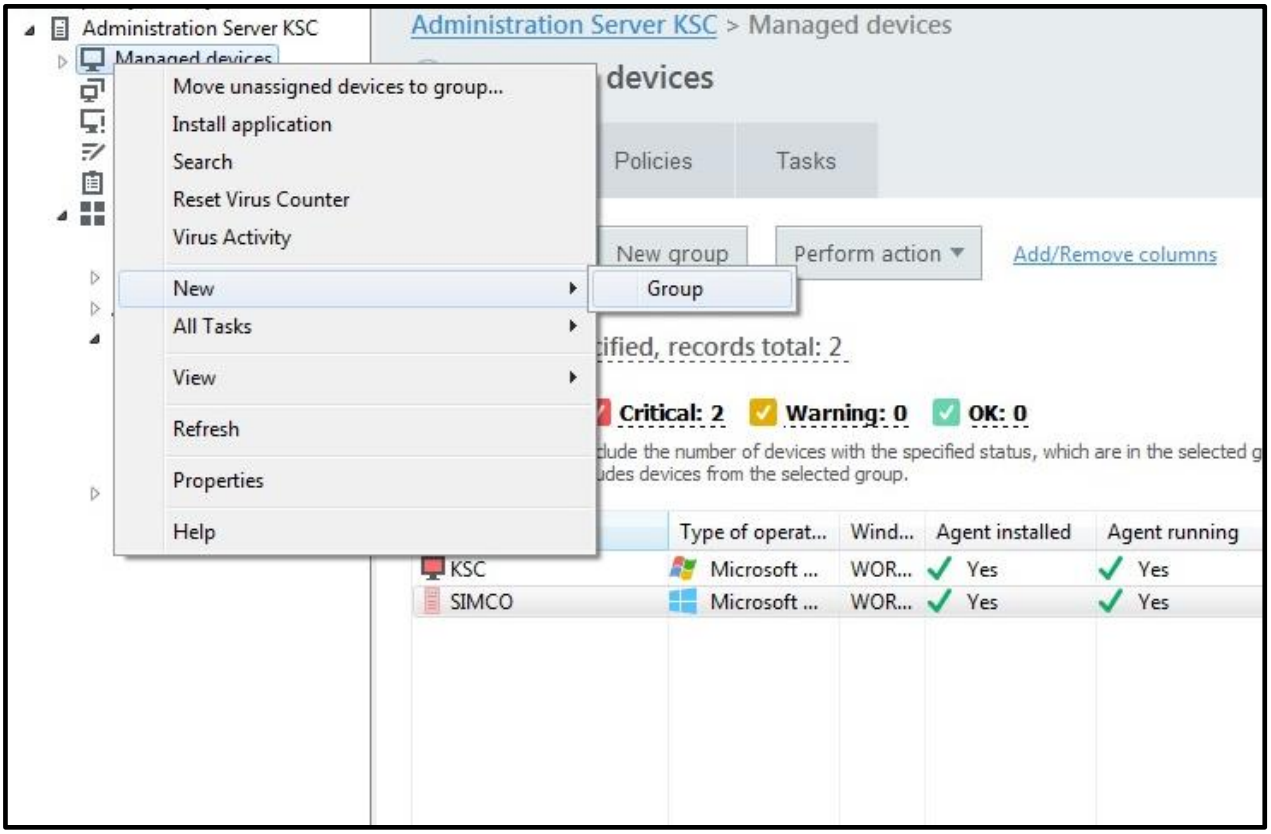
12. When the installation is complete, click **Finish**.



13. Now we go to the **Administration Server->Managed Devices** hierarchical node and switch to the **Devices** tab. Here we should see the host we have recently installed **KLnagent** onto (in our case, **SIMCO**).

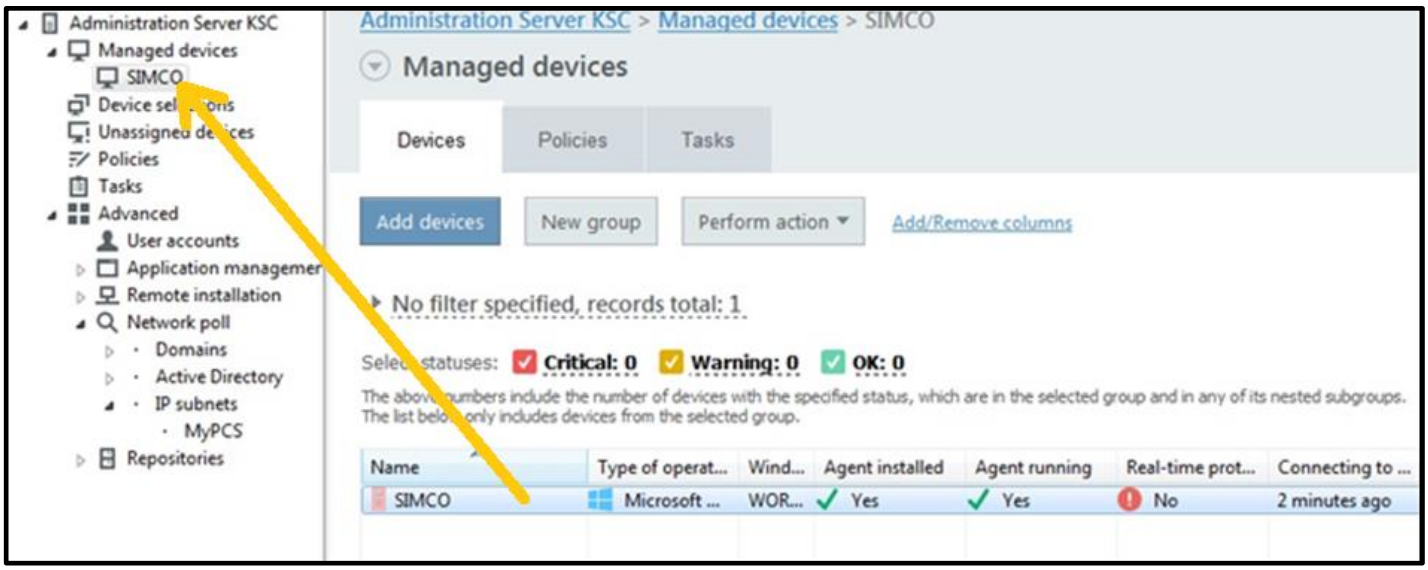


14. Right-click on **Administration Server->Managed Devices** and in the context menu select **New->Group.**



15. Give a name to a new group.

16. Select the device (**SIMCO**, in our case) and drag it to the newly created group, which is now available as a sub-node of the **Managed devices** node. As a result, the device is now assigned to the new group.

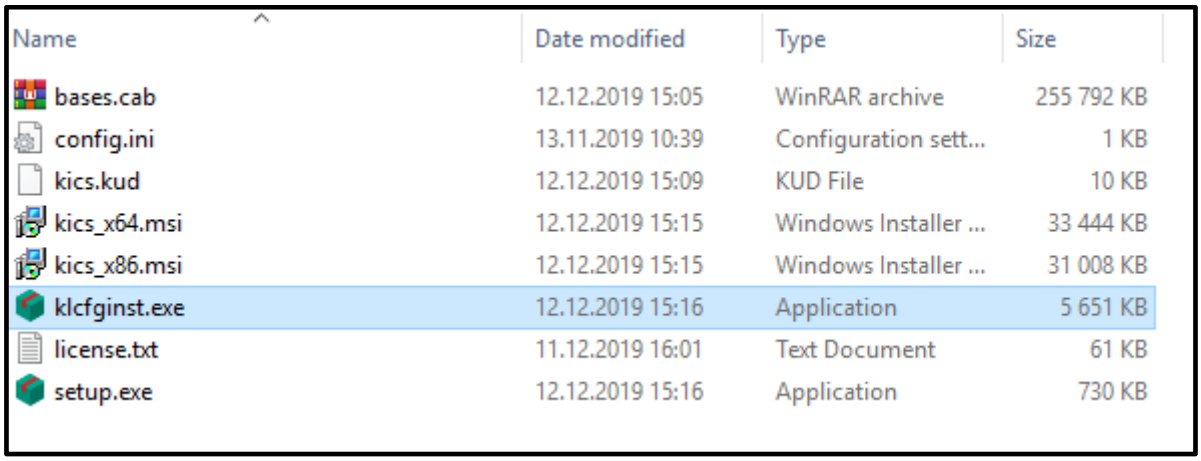


It makes sense to group devices by their functional purpose or by their software composition. For example, if we had a redundant pair of **Process Historians** servers, we would assign both the master and standby units to the same group because redundant devices usually run identical software. The point is that security policies or management tasks placed into a group affect every device belonging to this group.

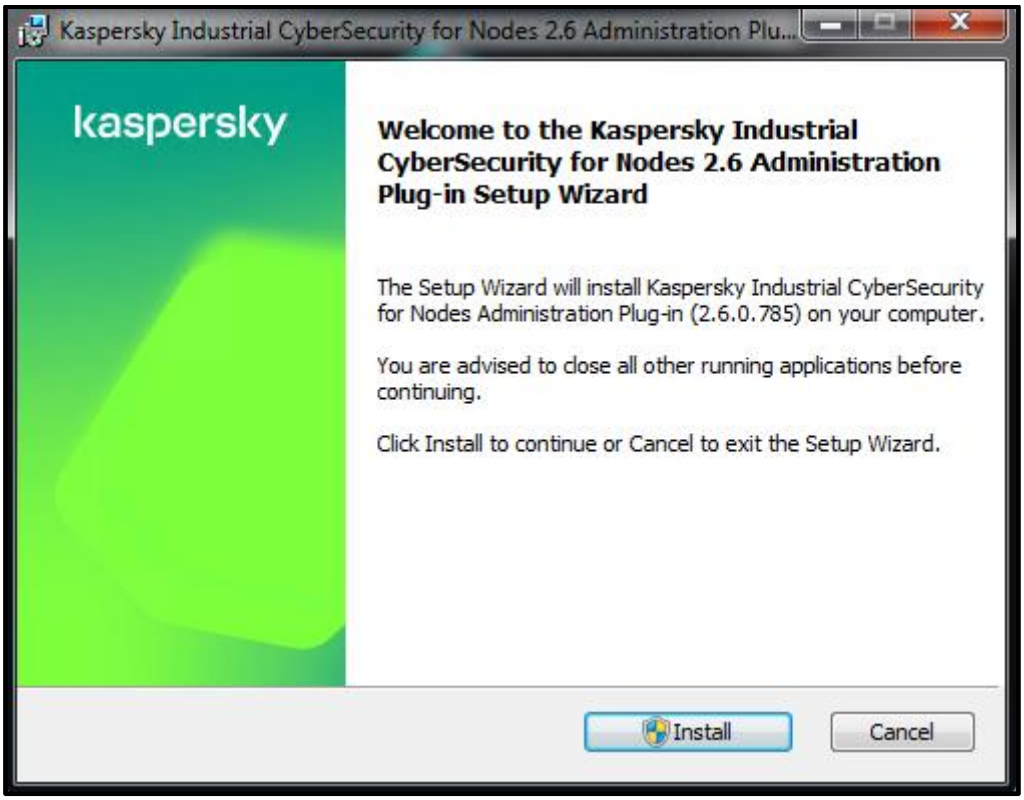
Installation of the KICS for Nodes management plugin

In order to enable remote administration of **KICS for Nodes** instances, we need to supplement **KSC** with **KICS for Nodes management plugin**.

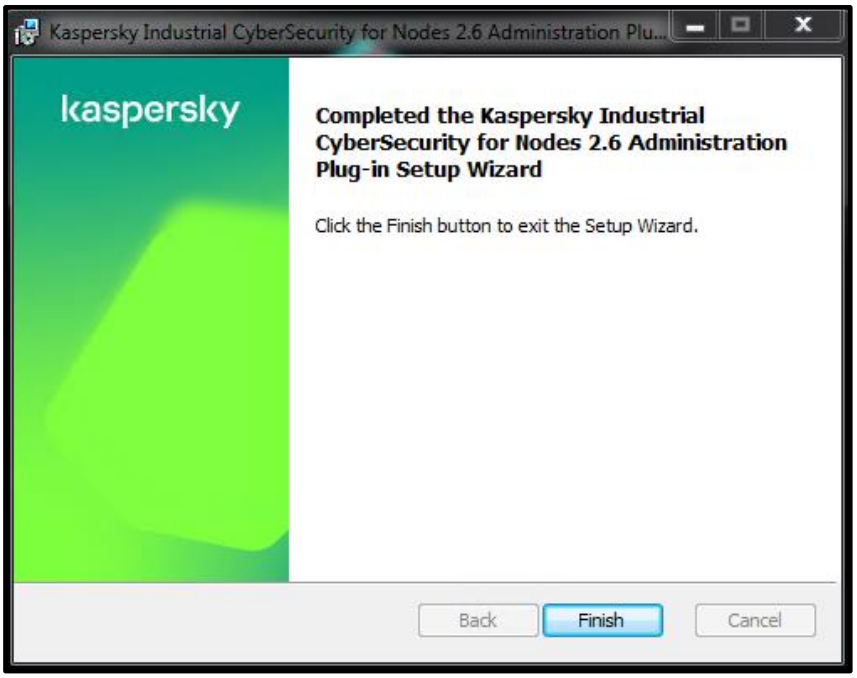
1. Locate **klcfginst.exe** in **server** folder of the distribution package supplied and launch it.



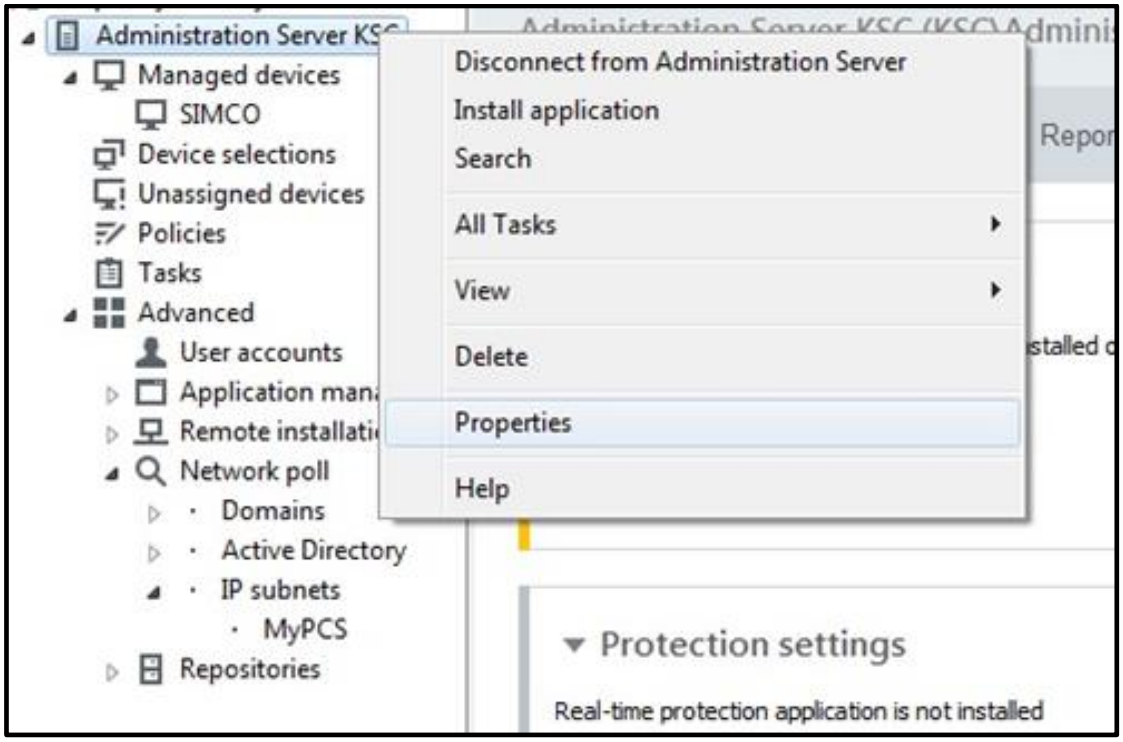
2. In the **Plug-in Setup Wizard** click **Install**.



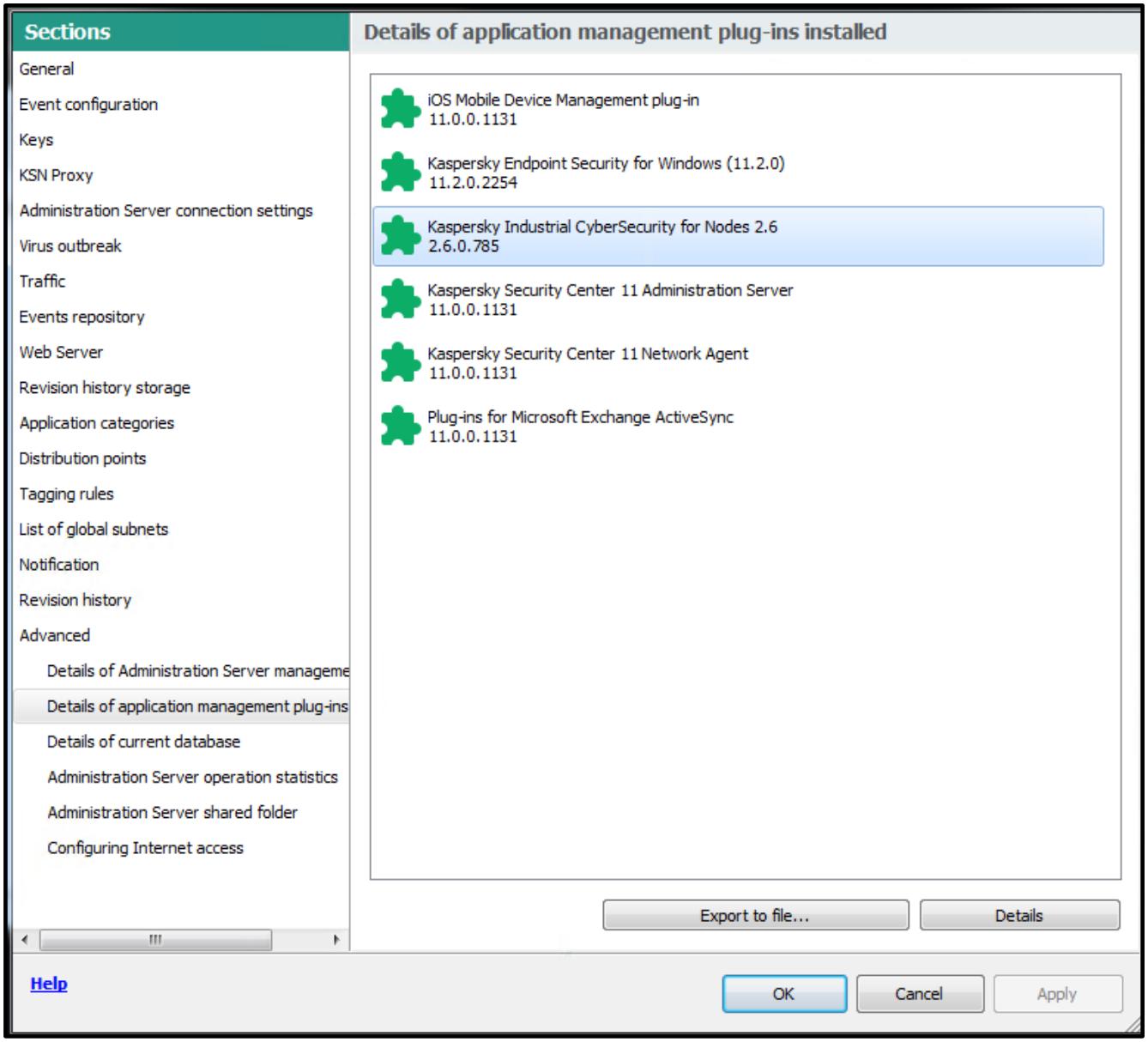
3. Please wait patiently until the installation is completed. During installation the user rights elevation may be requested, you should allow it. The installation process may run in the background. Click **Finish** when the **Installation complete** window appears.



4. In order to make sure that the plugin has been installed correctly, go back to the **KSC Administration Console**, right-click the **Administration Server** node and select **Properties** in the context menu.



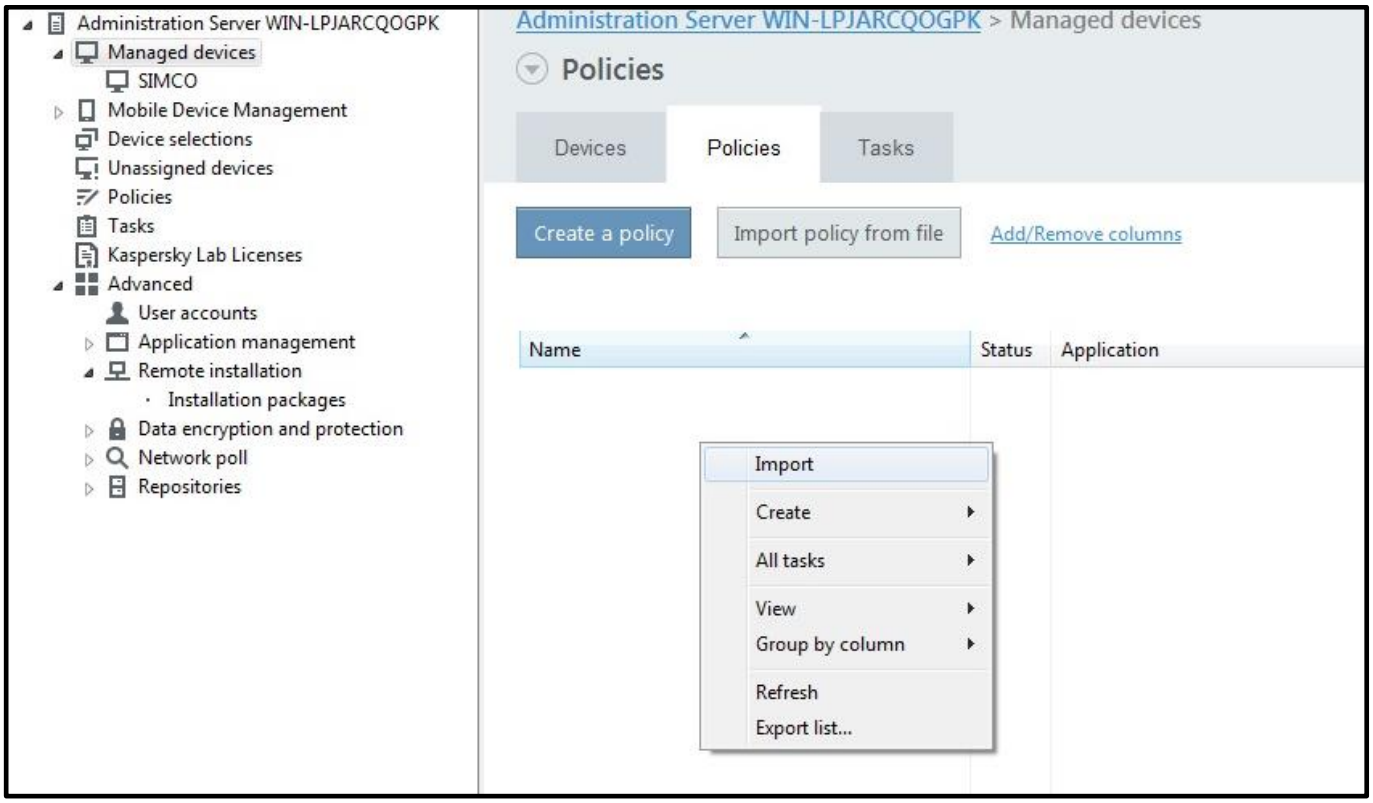
5. In the window that appears, go to **Advanced->Details of the installed application management plug-ins**. Check whether the **Kaspersky Industrial CyberSecurity for Nodes 2.6** plugin is present.



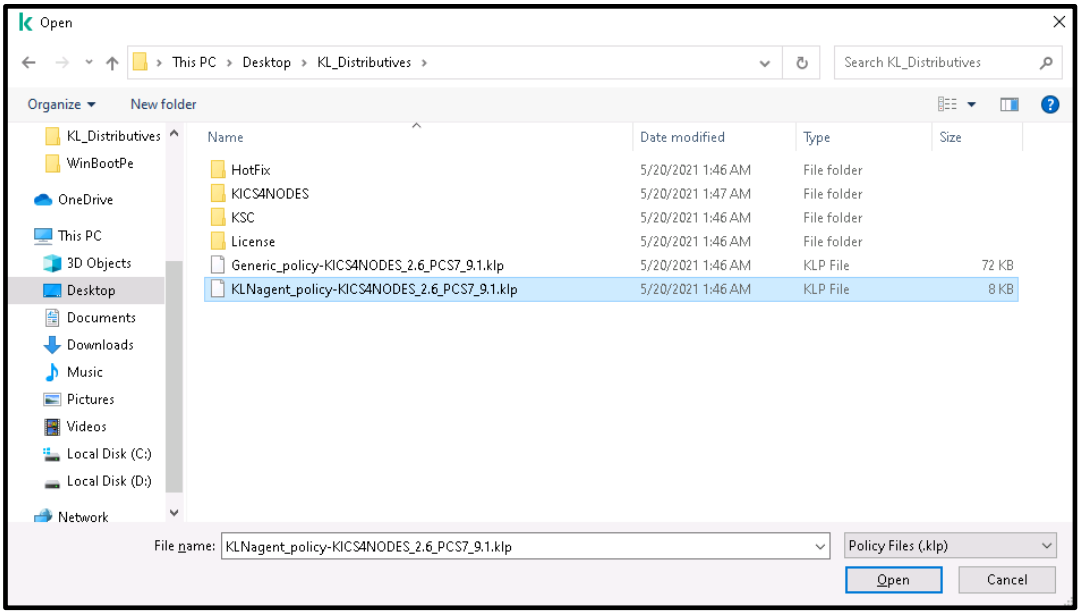
General configuration of the security policy for KLnagent

Now we are ready to import the predefined policy that matches the **KLnagent** most common settings. Once the policy is fully prepared, we will activate (reinforce) it. Please perform the following steps using the **KSC Administration Console**.

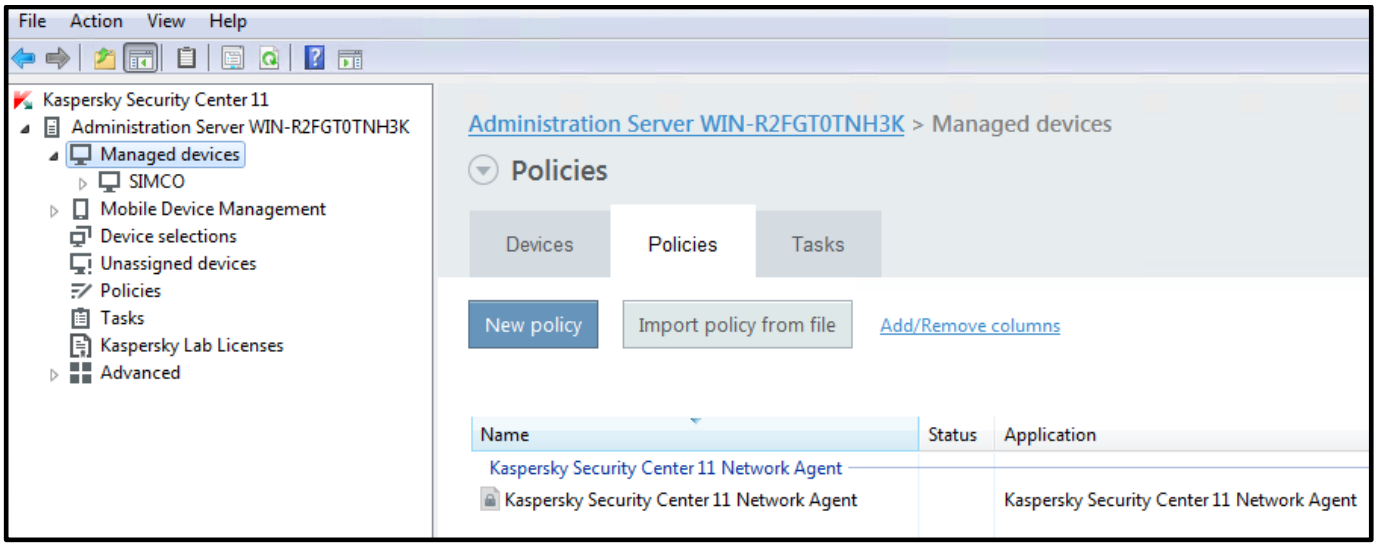
1. Go to **Administration Server->Managed Devices** and switch over to the **Policies** tab. Right-click on the **Policies** list and in the context menu select **Import**.



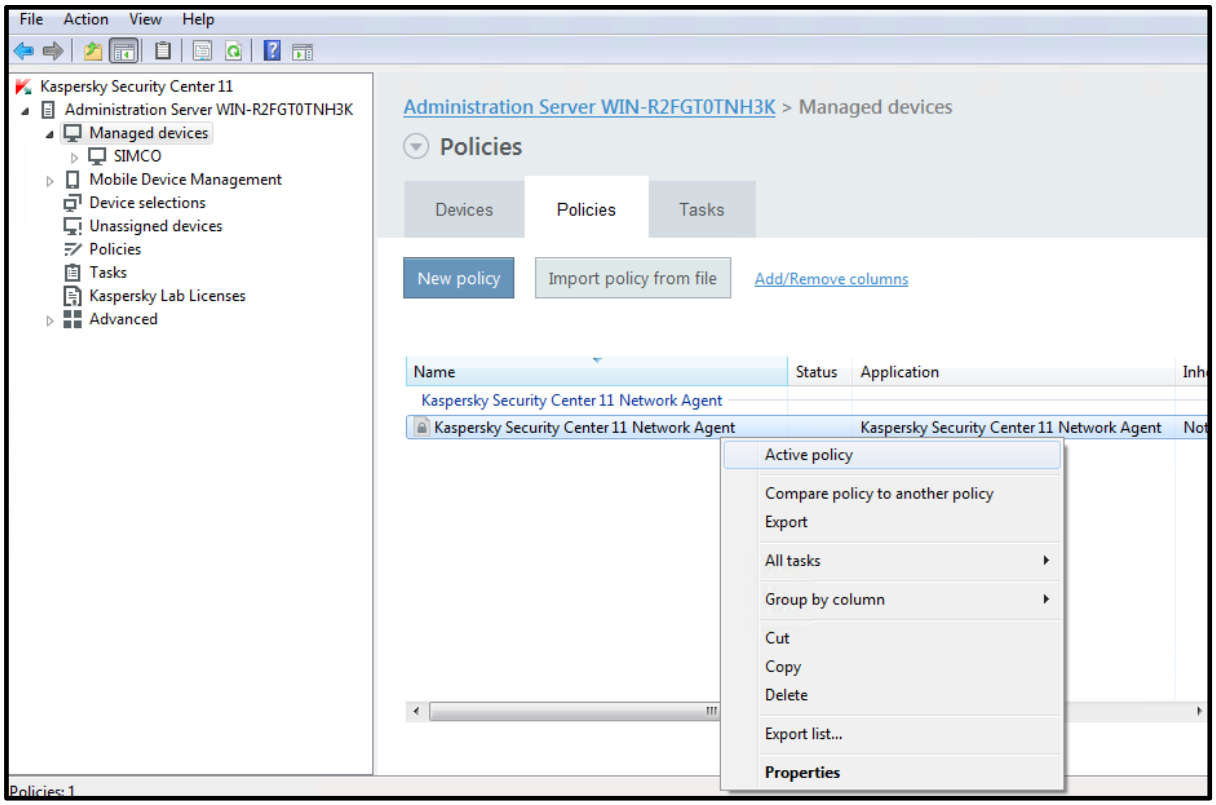
2. Using the file browser, go to the distribution package and locate the **KLNagent_policy-KICS4NODES_2.6_PCS7_9.1.klp** file as shown below. Click **Open**.



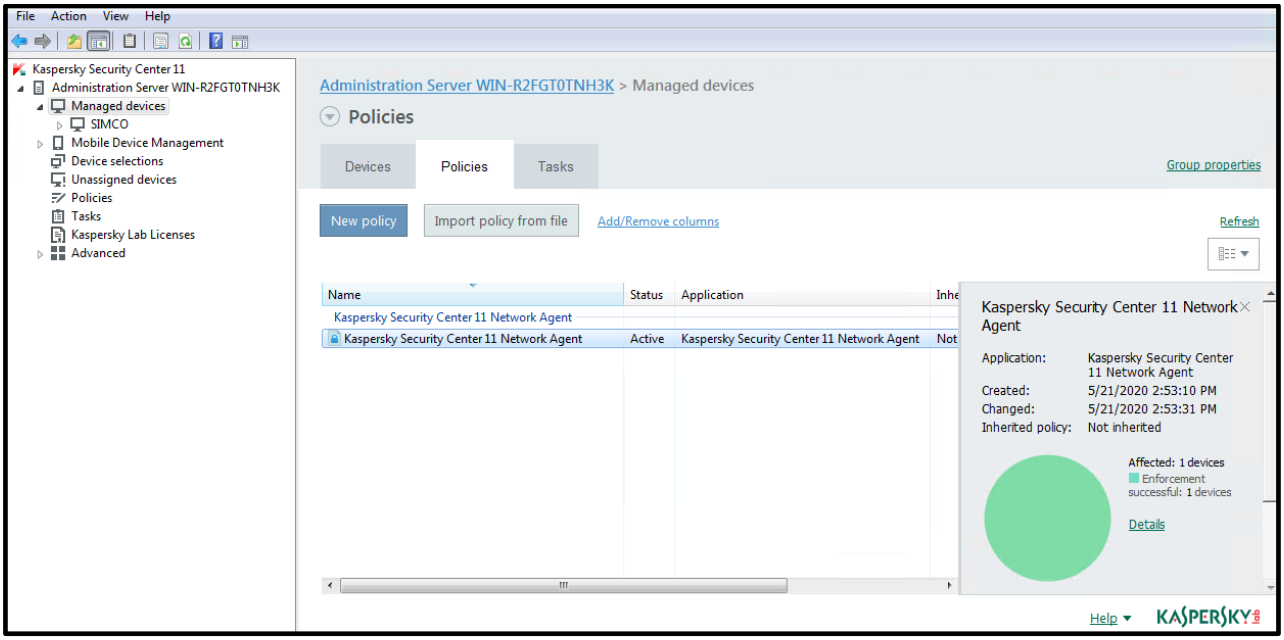
3. The new **KLnagent** policy should immediately appear. It applies to every host assigned to the top-level **Managed devices** group and to the derivative groups. By default, the newly created policy remains inactive until you put into force manually.



4. Right-click on the just created policy and in the context menu choose **Active policy**.



5. Wait for some minutes until the right-hand pane chart turns fully green, which means that the policy has been successfully applied to the **SIMCO** host.



As a result, we have created and activated the **KLnagent** policy, which is now visible on the **Policies** list. Similar to tasks, this policy affects every device assigned to the top-level **Managed devices** group as well as every subsidiary group. It is reasonable because the **KLnagent** policy is likely to be the same for every existing or newly added device.

kaspersky

Configuring KICS for Nodes instances

The configuration of **KICS for Nodes** is carried out by creating appropriate security policies via **Kaspersky Security Center** and applying them to the target hosts. In case of a multi-node installation, this centralized deployment technique helps to reduce implementation time and minimizes efforts because there is no need to switch from one computer to another.

We recommend creating some generic **KICS for Nodes** policy and applying it to the target hosts even before the **KICS for Nodes** software is actually installed on those hosts. This approach ensures that the safe and compatible "backbone" security policy will be automatically distributed to the target hosts right after the subsequent **KICS for Nodes** installation is done. In fact, this generic ("backbone") policy of **KICS for Nodes** remains the same for every control system host because it excludes any device-specific fine tunings and white lists. Later on, we will have to "personalize" our generic policy for the **SIMCO** station by supplementing specific white lists for **Application launch control** and **Device Control**.

When it comes to **Application launch control** and **Device Control,** some preparation tasks should be executed prior to switching on these features. These tasks enable automatic creation of application and device white lists essential for **Application launch control** and **Device Control** operation**.**

From this point on, the **KICS for Nodes 2.6** configuration routine will comprise the following sequential steps:

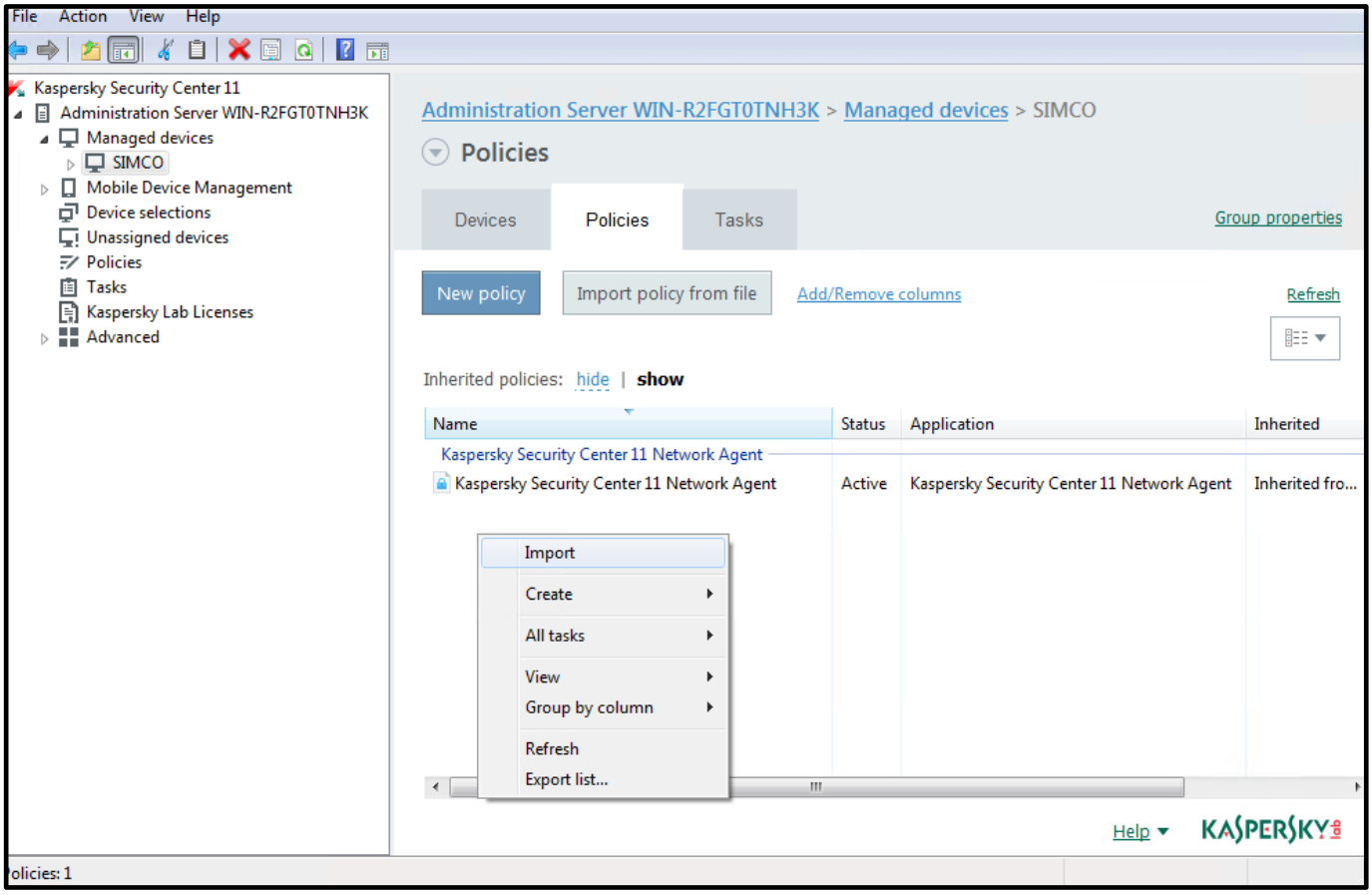
- Import of the generic ("backbone") policy for **KICS for Nodes** from the **Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp** file supplied as a part the distribution package.
- Remote installation of **KICS for Nodes 2.6** onto the target hosts.
- Remote installation of **Hotfix** onto the target hosts[7].
- Initial update of antivirus databases.
- Performing the **On-Demand** scanning on the target hosts.
- Execution of the **Generate Rules for Application Launch Control** task.
- Setting up **Application Launch Control** whitelisting.
- Setting up **Device Control** whitelisting.
- Setting up **PLC Integrity Checker** (if applicable).

[7] Please note that in some specific cases no **Hotfix** should be installed and this deployment step should be omitted. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section for details.

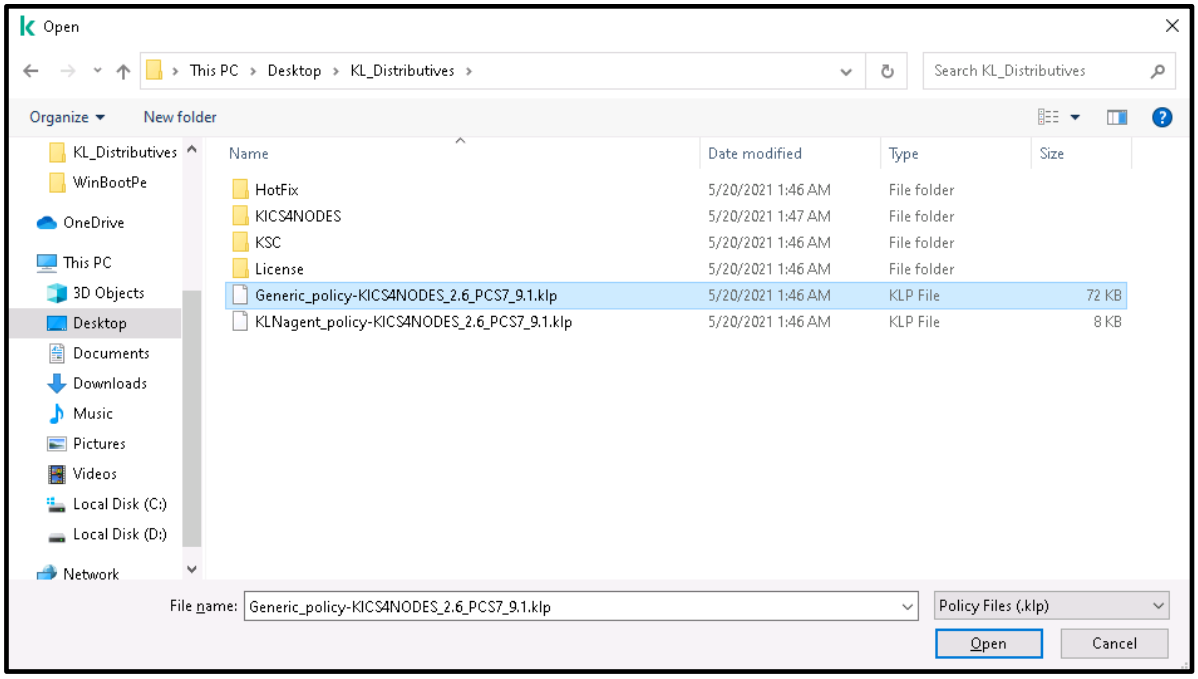
Creation of the generic policy for KICS for Nodes

KICS for Nodes configuration should be carried out in strict accordance with operational and security requirements of your control system. It is crucial to consider DCS operational characteristics to be a top priority!
In order to facilitate the **KICS for Nodes** deployment, we are going to make use of the predefined generic policy that contains the **KICS for Nodes** unified settings appropriate for most of the control systems. Once the policy is fully prepared, we will activate (reinforce) it. Please perform the following steps using the **KSC Administration Console**:
Please follow the following steps to create the generic policy for **KICS for Nodes**.

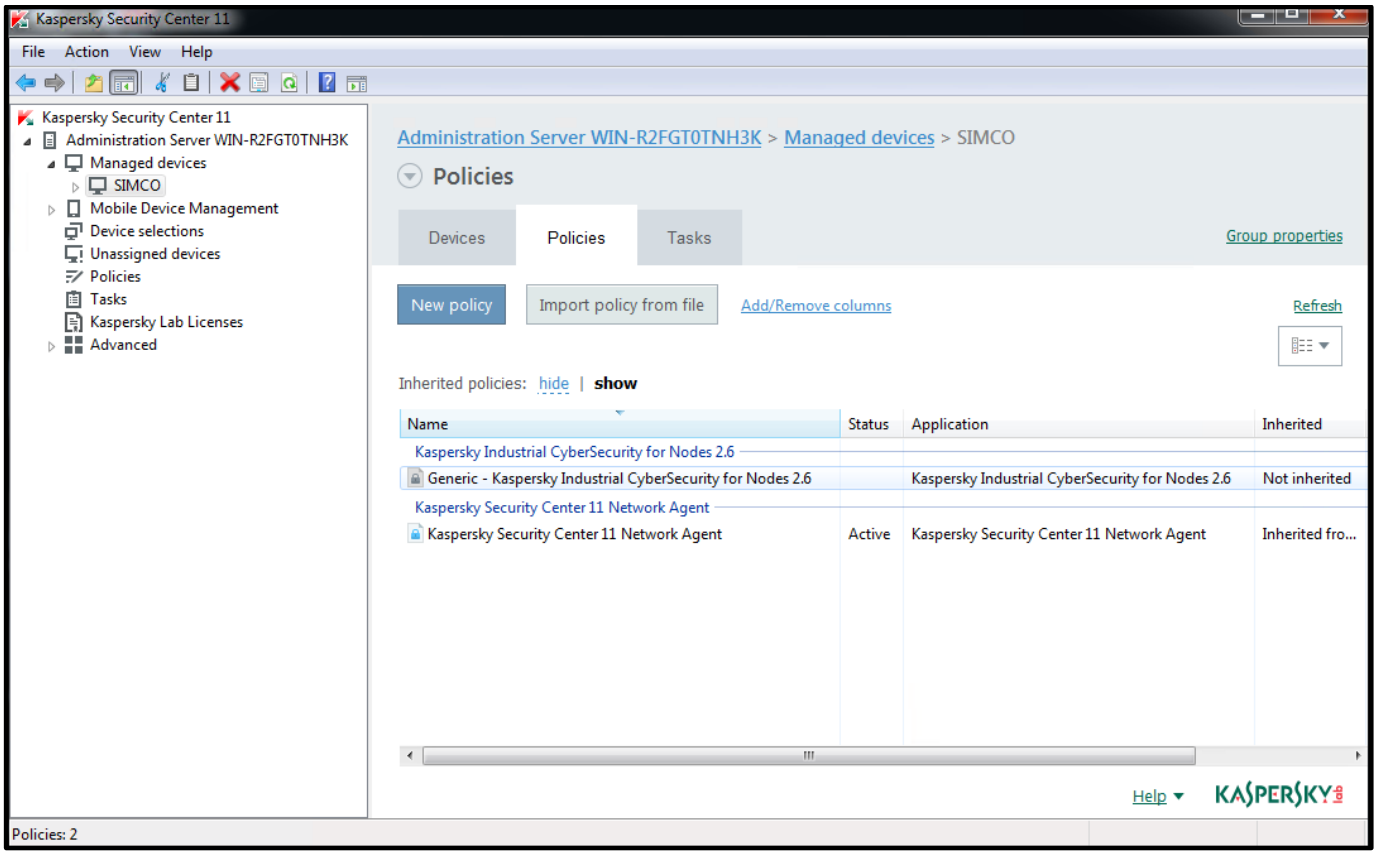
1. Go to the subsidiary device group, which contains our target host (in our case, **SIMCO**). Switch to the **Policies** tab. Start importing a new policy in the same manner as we did before with **KLnagent**.



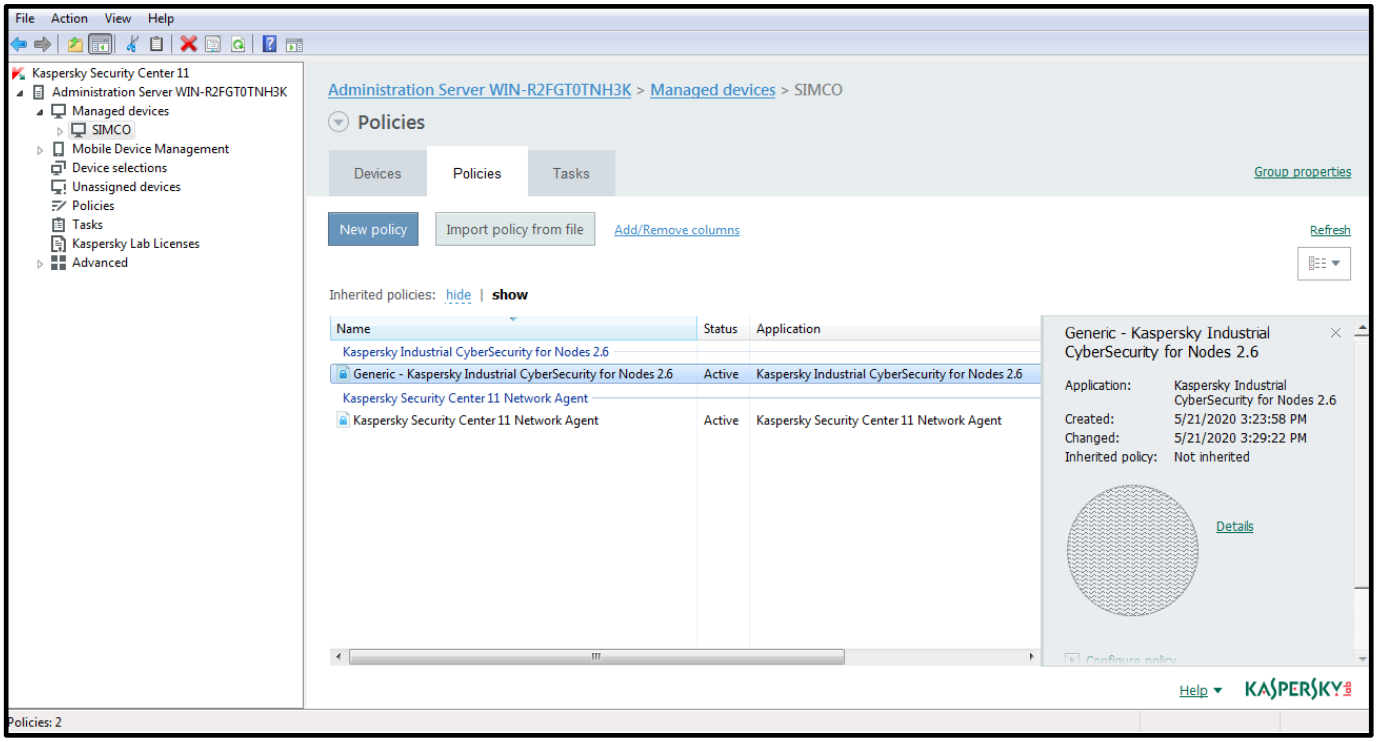
2. Using the file browser, go to the distribution package and locate the **Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp** file as shown below. Click **Open**.



3. The new **KICS for Nodes** policy should immediately appear. It solely applies to the hosts assigned to the **SIMCO** subgroup. By default, the newly created policy remains inactive until you put into force manually.



4. Right-click on the just created policy and using the context menu activate it in the same way as you did for the **KLnagent** policy.
5. This time the right-hand pane chart will not turn green, because no **KICS for Nodes** application is installed on the **SIMCO** host yet.

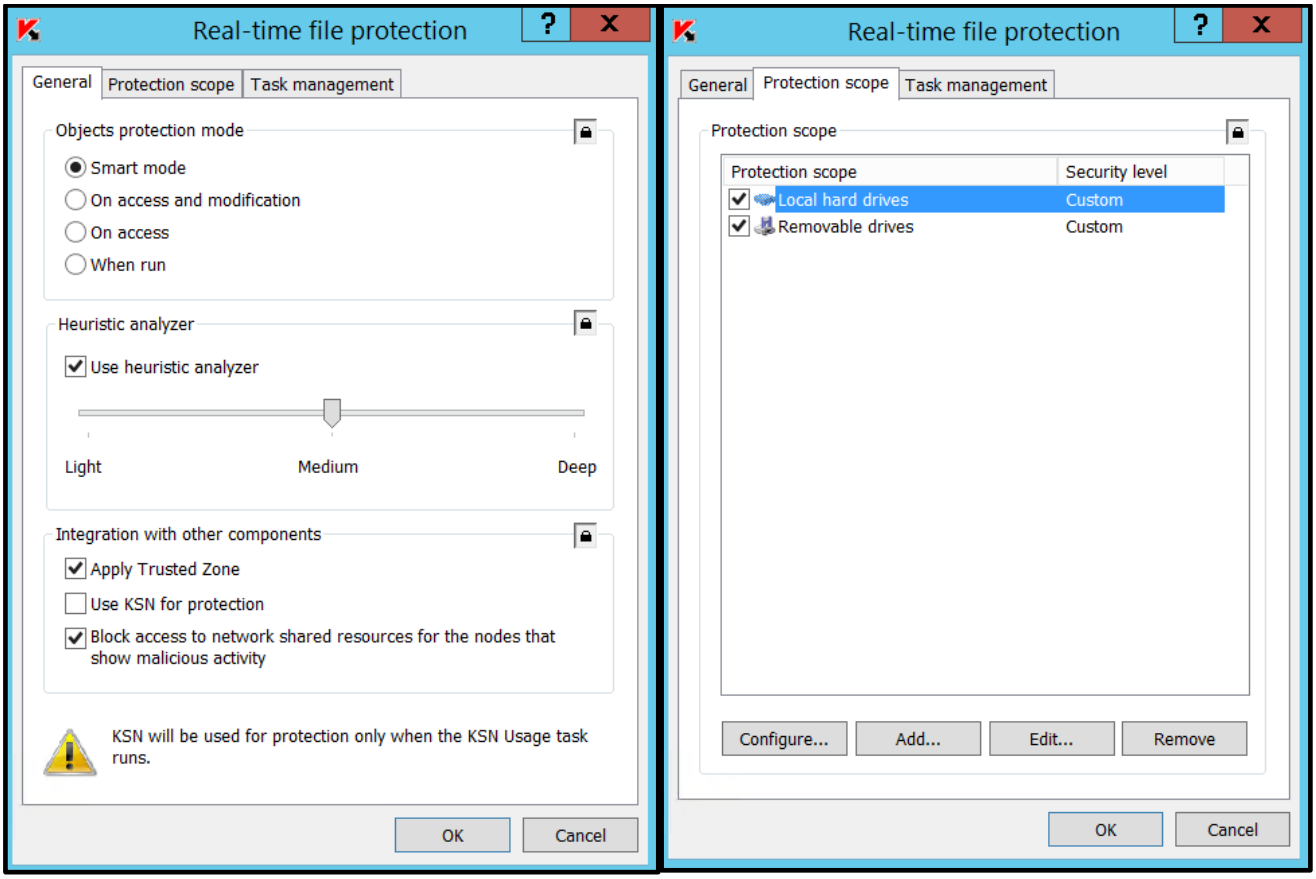


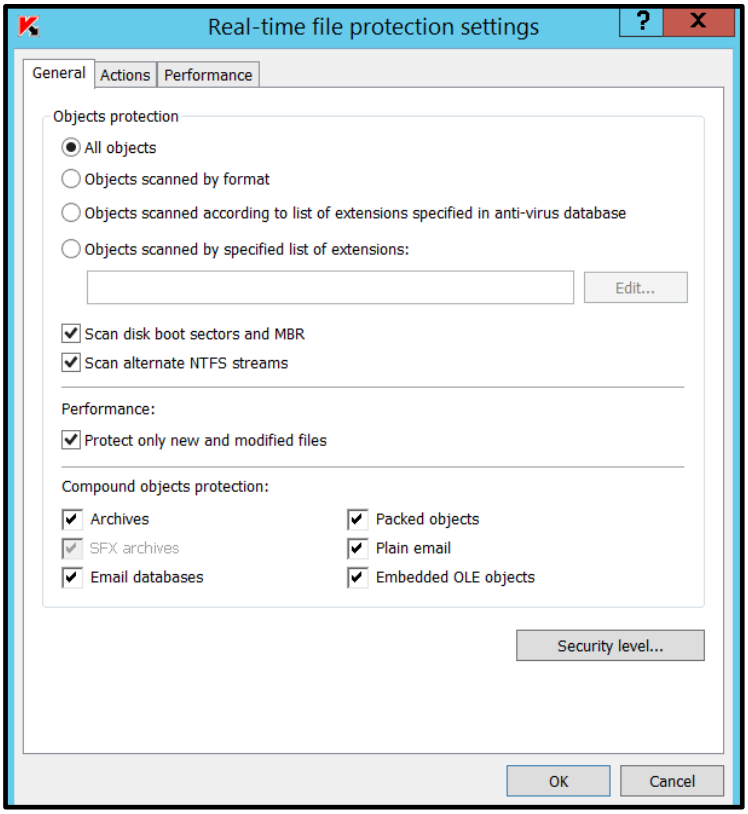
So far, the **KICS for Nodes** policy has incorporated only general security settings. Later, we will revert to this policy in order to make it more specific to the **SIMCO** host.

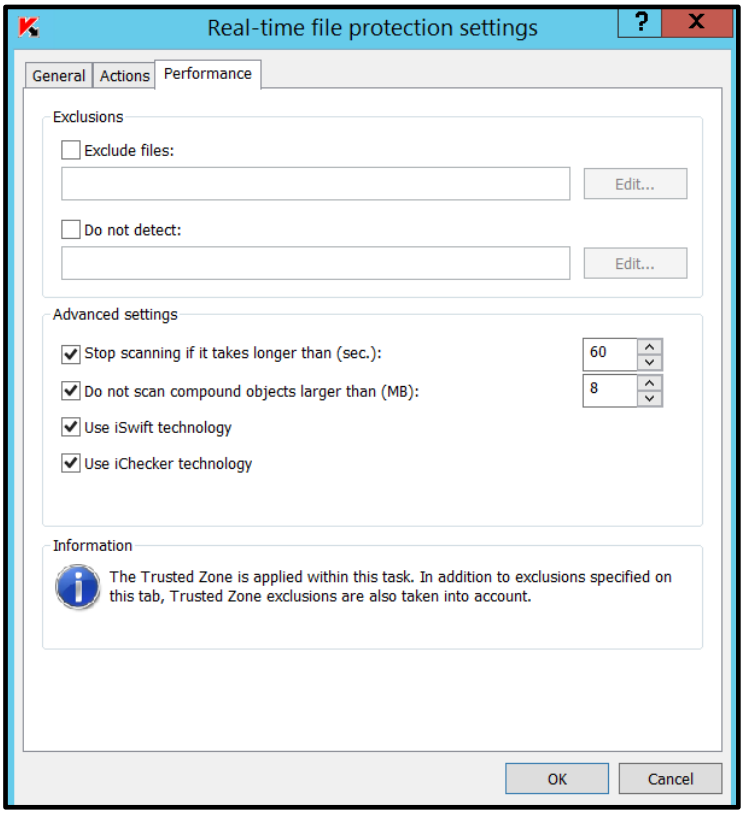
Settings of KICS for Nodes generic policy

This chapter highlights some important settings of the **Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp** policy that deviate from the default policy configuration. In general, the following features have been modified so that their settings are different from those of a newly created **KICS for Nodes** policy:

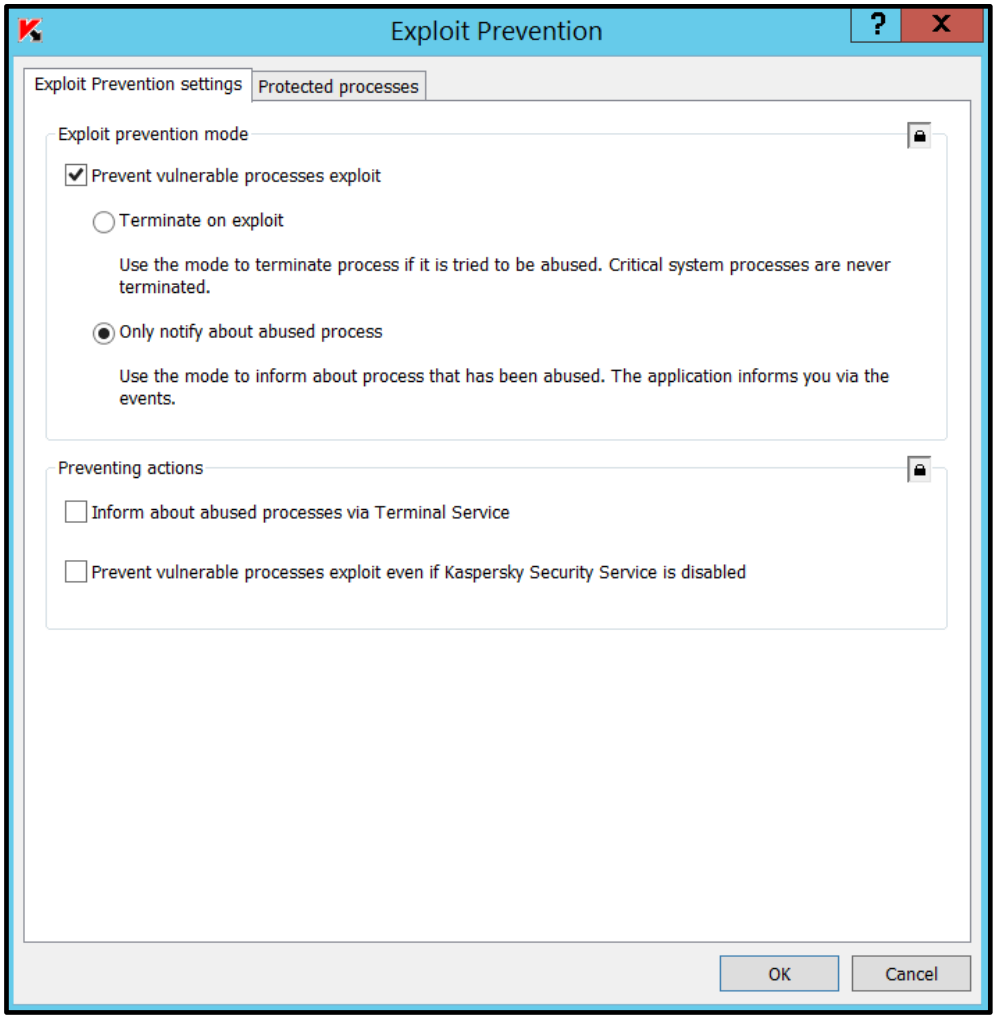
1. **Real time file protection** settings are as shown in the screenshots below (please note that we do not use **KSN**):



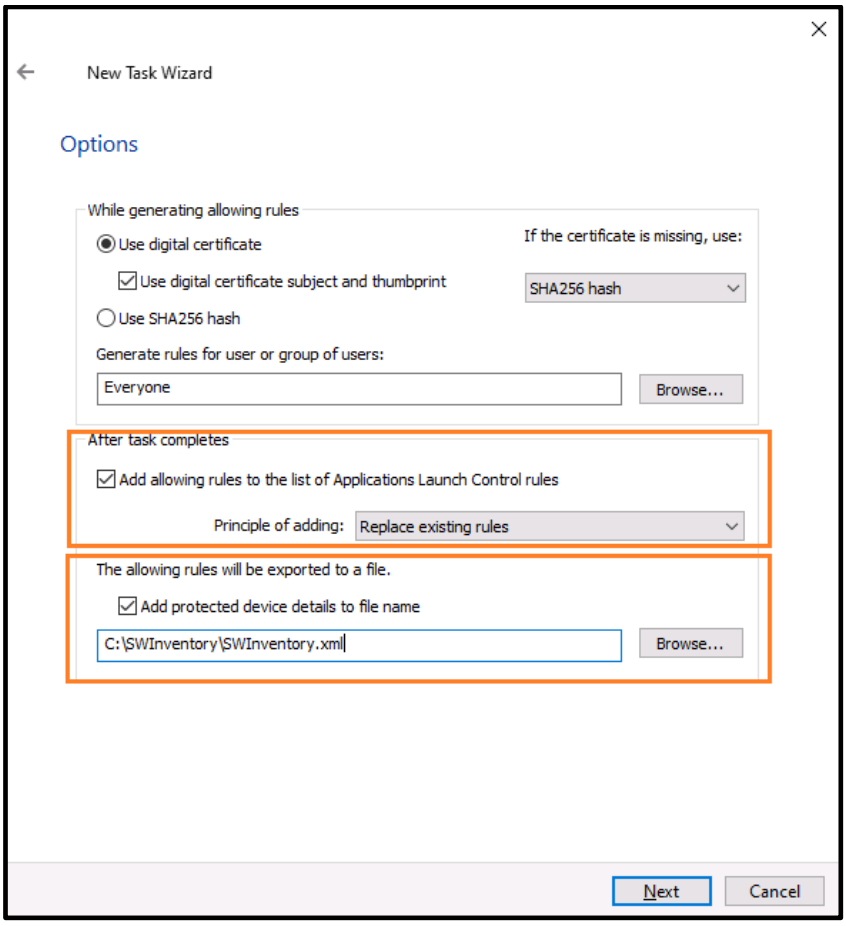

Real-time file protection settings
General
Actions
Performance
Objects protection
All objects
Objects scanned by format
Objects scanned according to list of extensions specified in anti-virus database
Objects scanned by specified list of extensions:
Edit...
Scan disk boot sectors and MBR
Scan alternate NTFS streams
Performance:
Protect only new and modified files
Compound objects protection:
Archives
Packed objects
SFX archives
Plain email
Email databases
Embedded OLE objects
Security level...
OK
Cancel

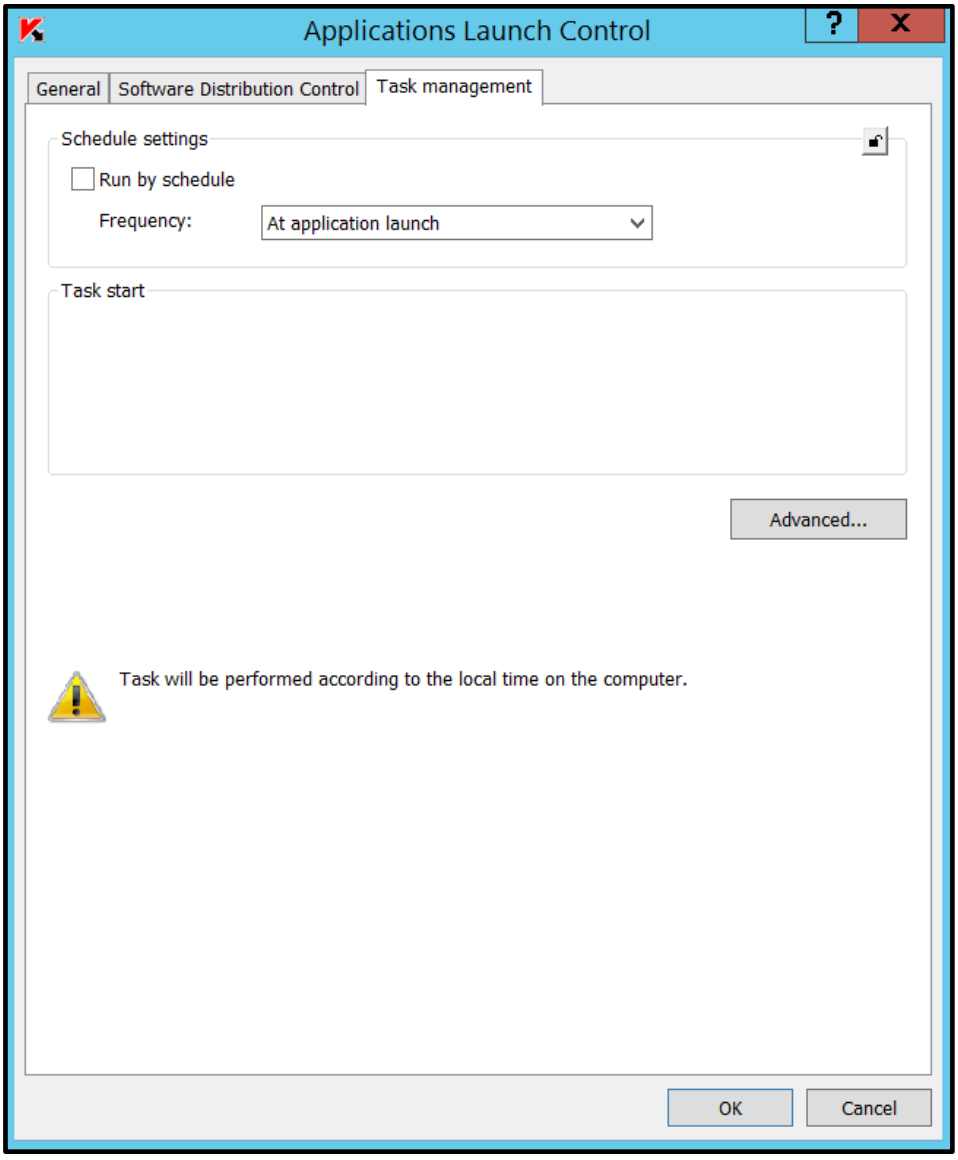

Real-time file protection settings
General
Actions
Performance
Exclusions
Exclude files:
Edit...
Do not detect:
Edit...
Advanced settings
Stop scanning if it takes longer than (sec.):
60
Do not scan compound objects larger than (MB):
8
Use iSwift technology
Use iChecker technology
Information
The Trusted Zone is applied within this task. In addition to exclusions specified on this tab, Trusted Zone exclusions are also taken into account.
OK
Cancel

2. **Kaspersky Security Network (KSN)** is disabled.
3. **Exploit Prevention** settings are as shown in the screenshot below:

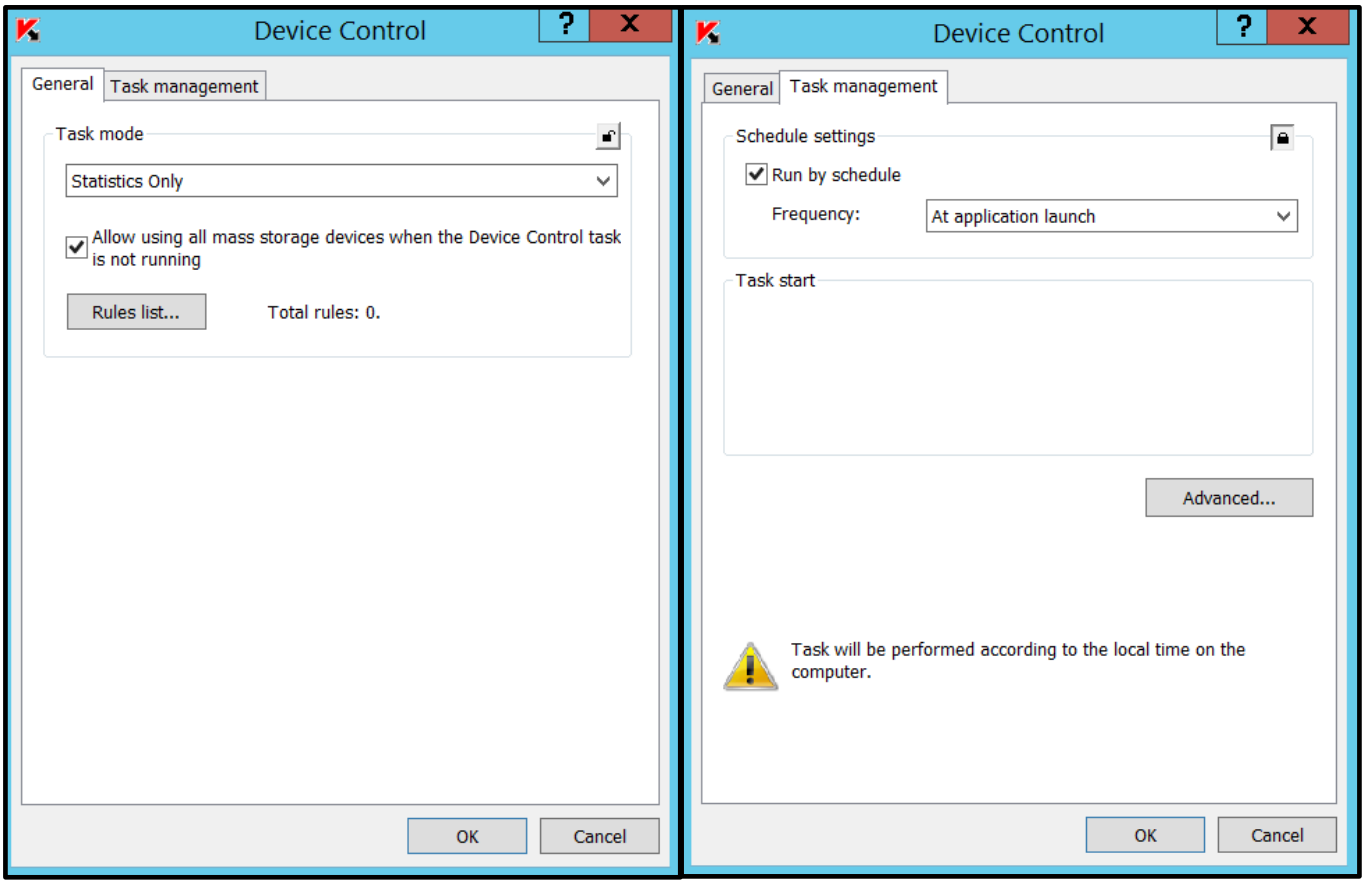


4. **Application Launch Control** settings are as shown in the screenshots below. Please note that the rule list lock is released because we will be filling up white lists later (individual for each device). At this stage the task itself should not be launched yet.



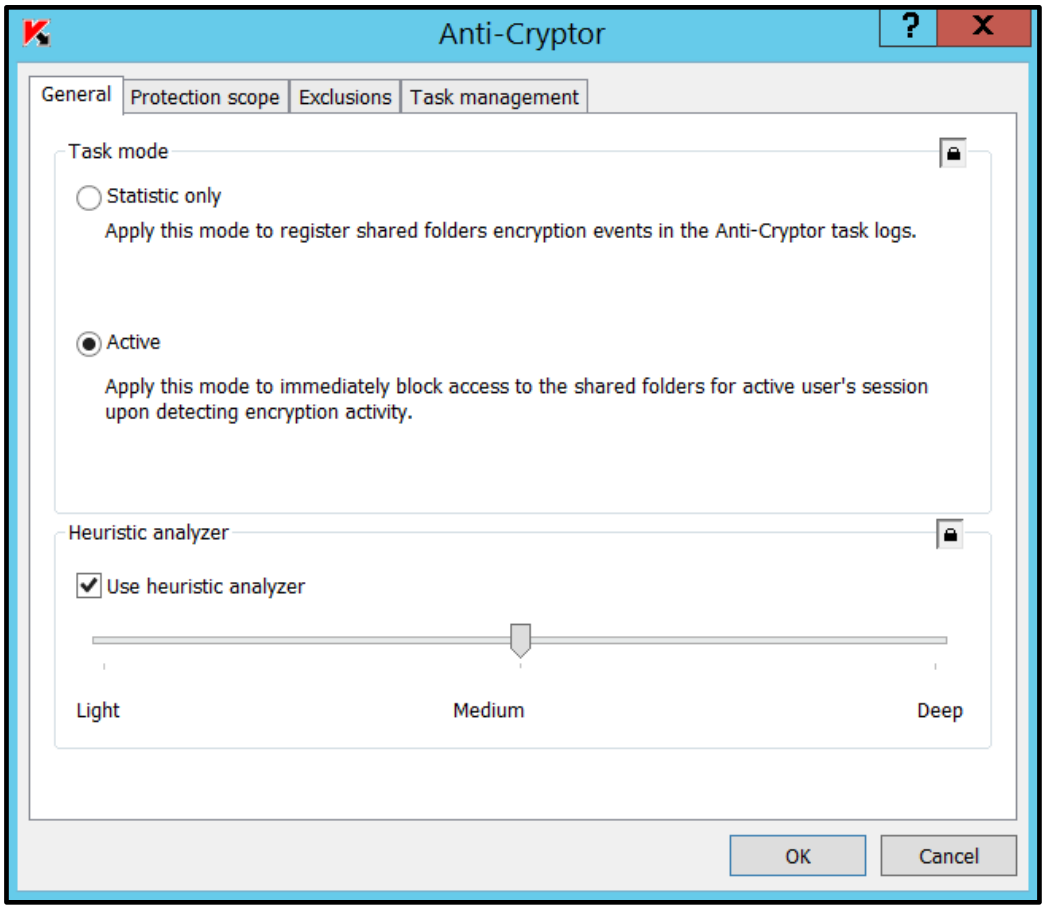

Applications Launch Control
General
Software Distribution Control
Task management
Schedule settings
Run by schedule
Frequency:
At application launch
Task start
Advanced...
Task will be performed according to the local time on the computer.
OK
Cancel

5. **Device Control** settings are as shown in the screenshots below. Please note that the task is already activated with a blank white list, which implies alerting on any USB storage device detected. The white list may be filled later for individual hosts if necessary.

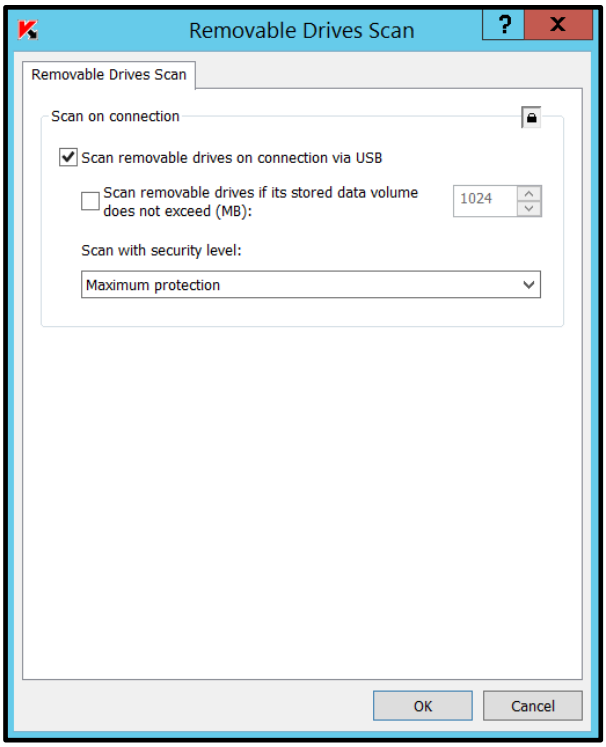


6. **Wi-Fi Control** is disabled.
7. **Firewall Management** is disabled.

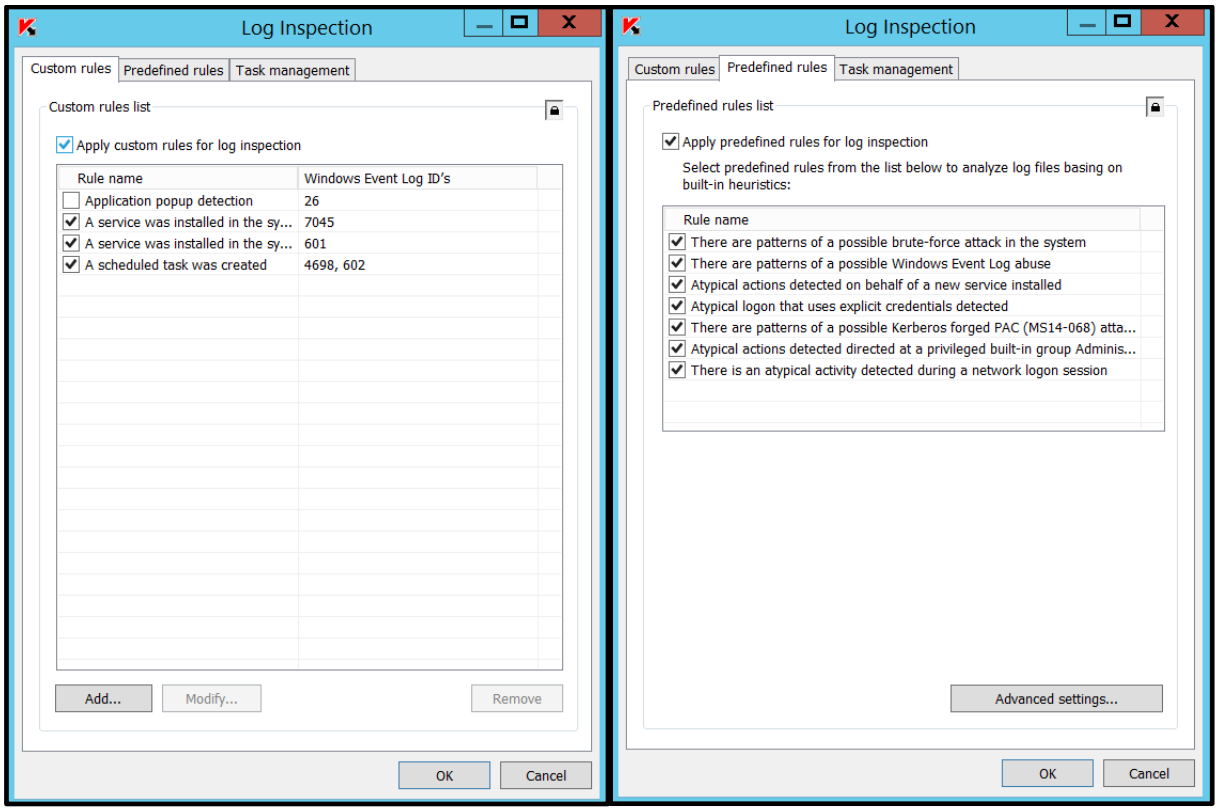
8. **Anti-Cryptor** settings are as shown in the screenshot below:



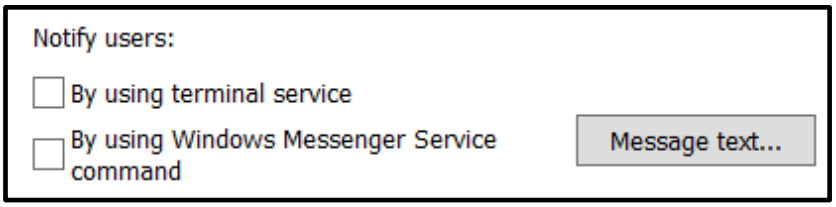
9. **Removable Drives Scan** settings are as shown in the screenshot below:



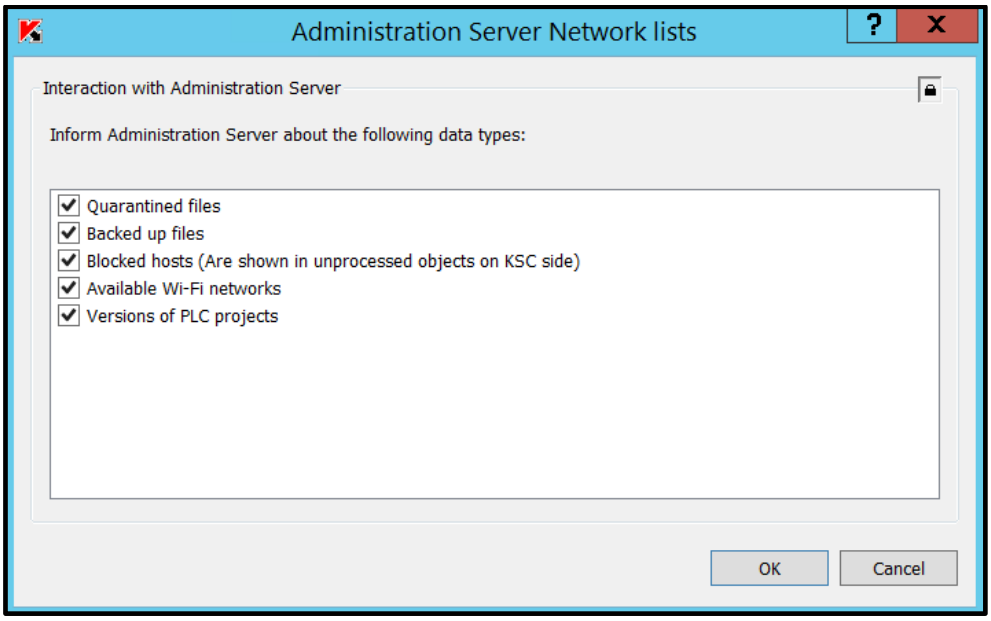
10. **File Integrity Monitor** is disabled.
11. **Log Inspection** settings are as shown in the screenshot below:



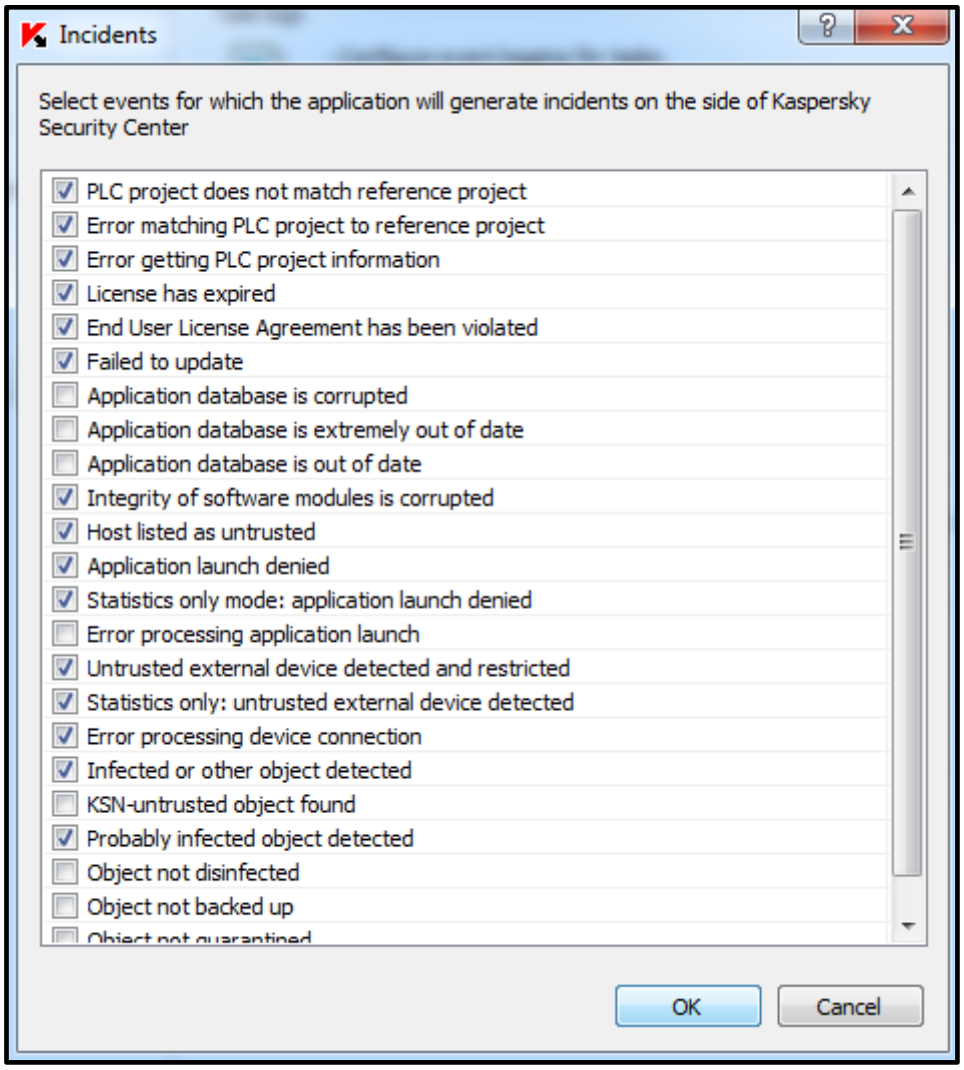
12. **In Logs and notifications->Event notifications** for each event type the following options are unchecked:



13. **Interaction with Administration Server** settings are as shown in the screenshot below:



14. **Incidents** settings are as shown in the screenshot below:



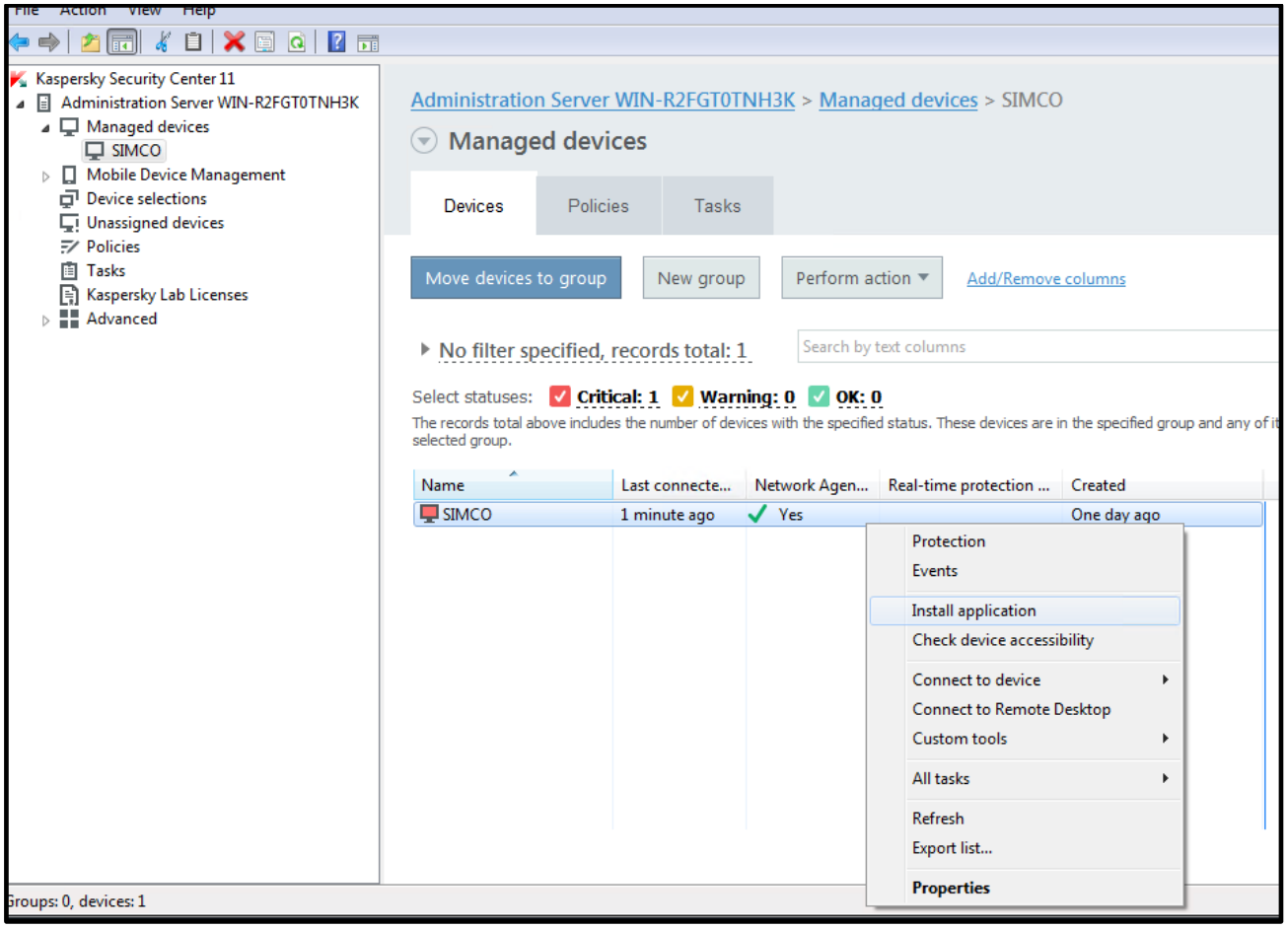
If specific antivirus exclusions are provided by an automation vendor, it is recommended to configure **Supplementary->Trusted Zone->Exclusions** and **Supplementary->Trusted Zone->Trusted Processes** accordingly. This may improve overall performance significantly.

Prior to proceeding to the next steps, please go through all the policy settings (mentioned above) very carefully and, if necessary, adjust them to your particular requirements that may differ.

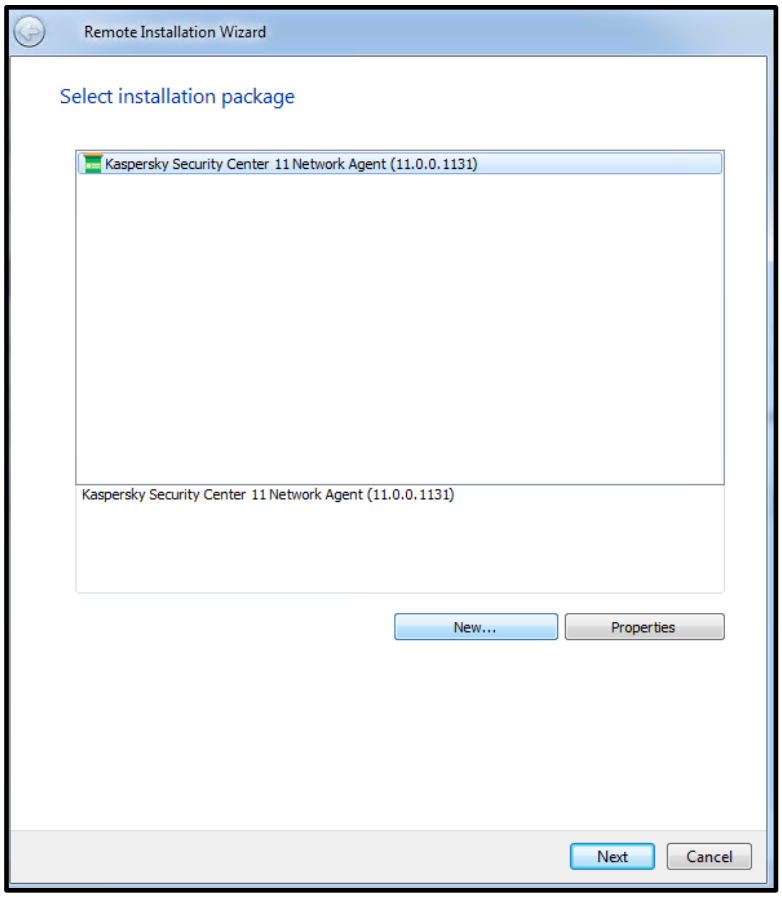
Remote installation of KICS for Nodes onto target computers via KLnagent

In order to get **KICS for Nodes** installed on a remote device please go through the following steps.

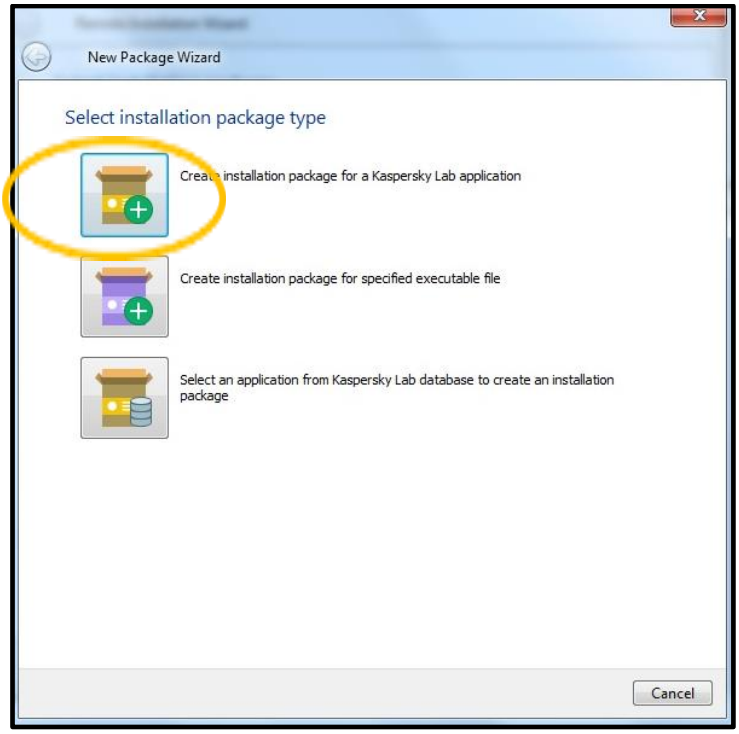
1. Go to the newly created device group (**SIMCO**, in our case) and locate the managed device we have installed **KLnagent** onto (if the **SIMCO** host does not show up automatically, click **Refresh** in the upper-right corner). Right-click on the device and choose **Install Application** in the context menu.



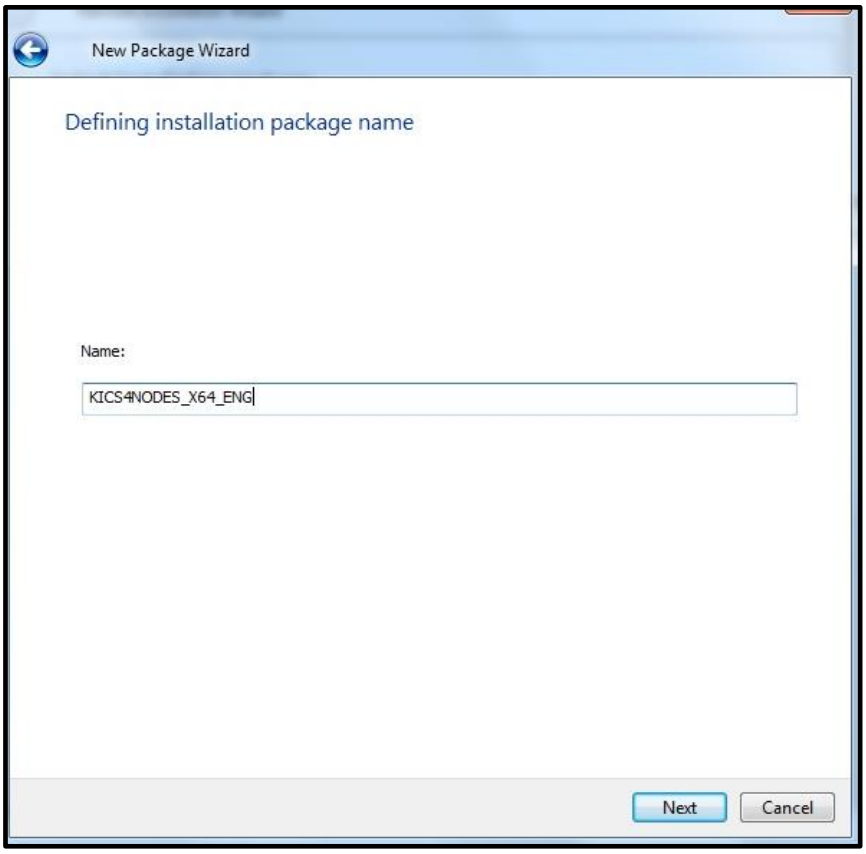
2. In the **Remote Installation Wizard** press the **New**… button.



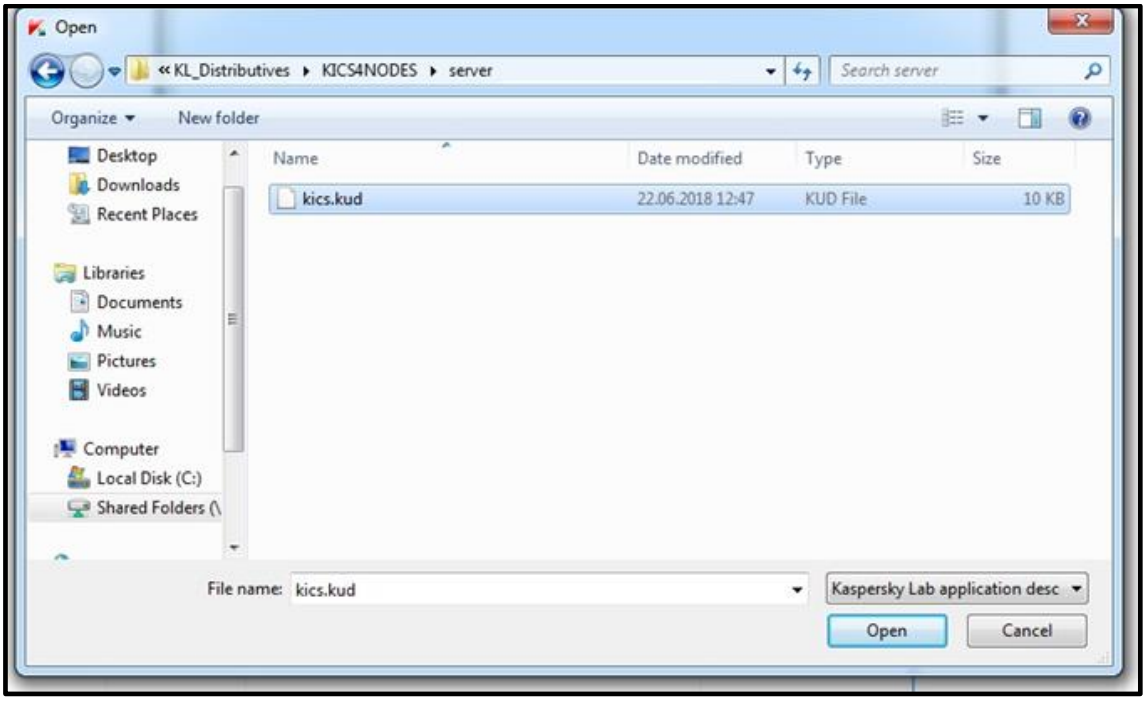
3. Click the **Create Installation package for a Kaspersky Lab application** button.

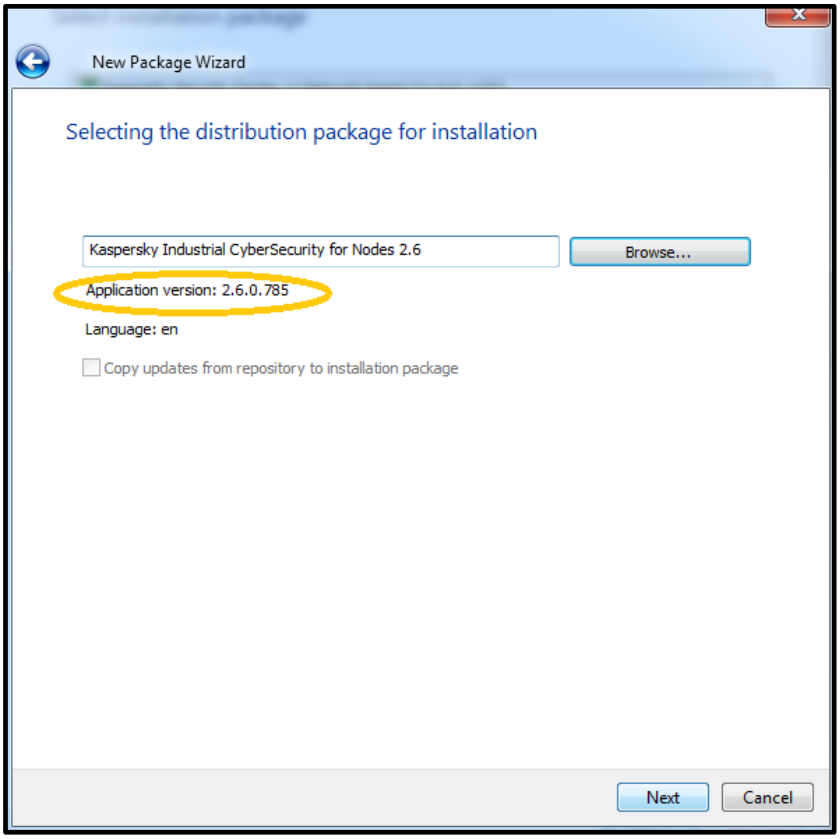


4. Give a name to the newly created installation package (**KICS4NODES_X64_ENG**, in our case). Click **Next**.

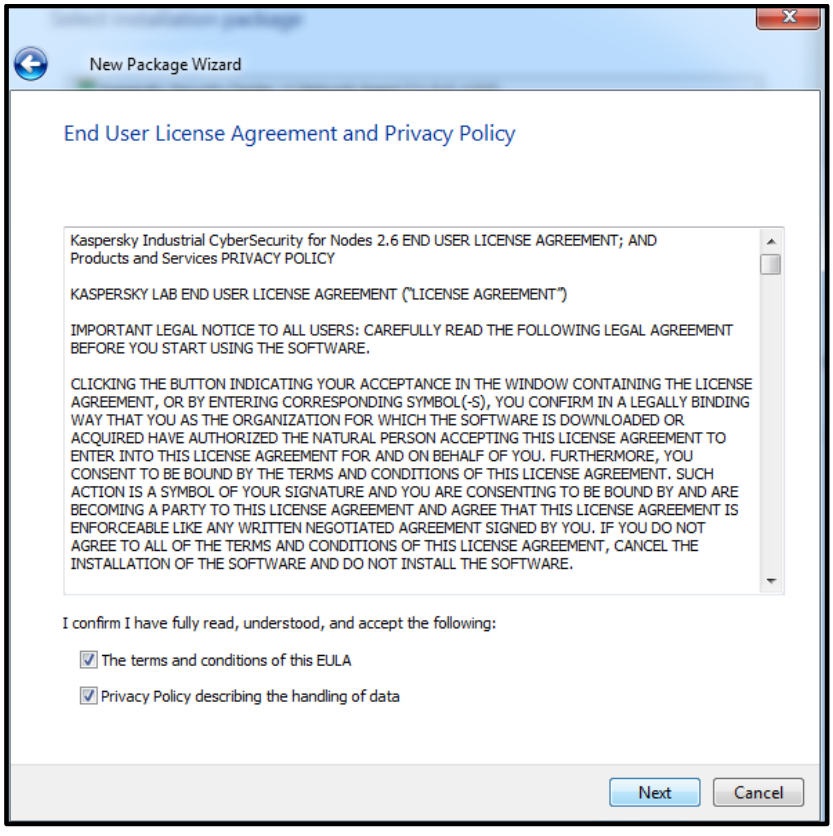


5. In the **Selecting the distribution package for installation** window click **Browse** to locate the **kics.kud** file, which is a part of the distribution package (**KL_Distributives\KICS4NODES\server**). After you open it, make sure that the application version is displayed as **2.6.0.785**. Click **Next**.

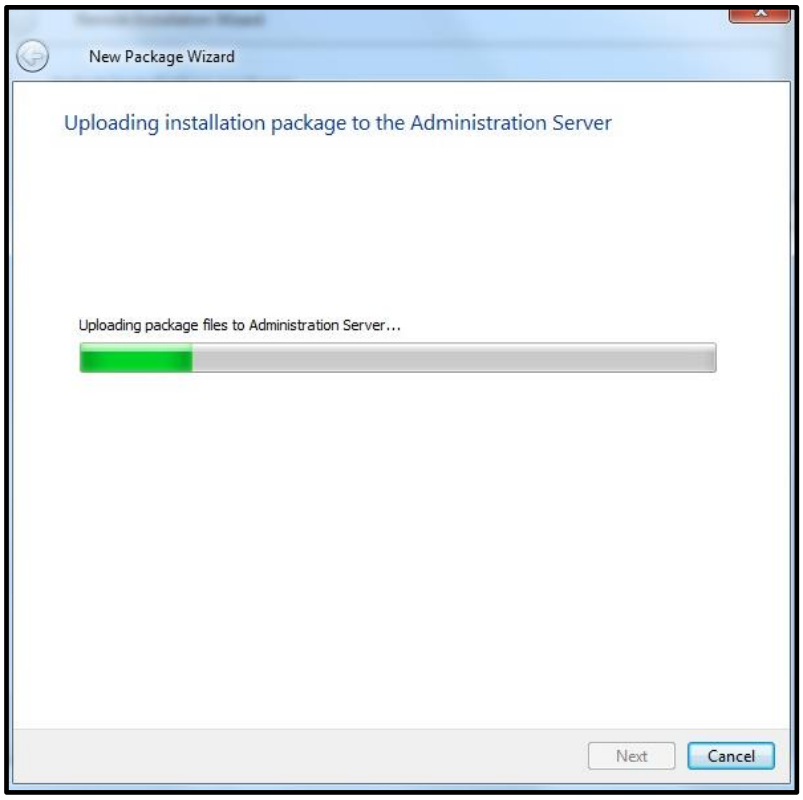




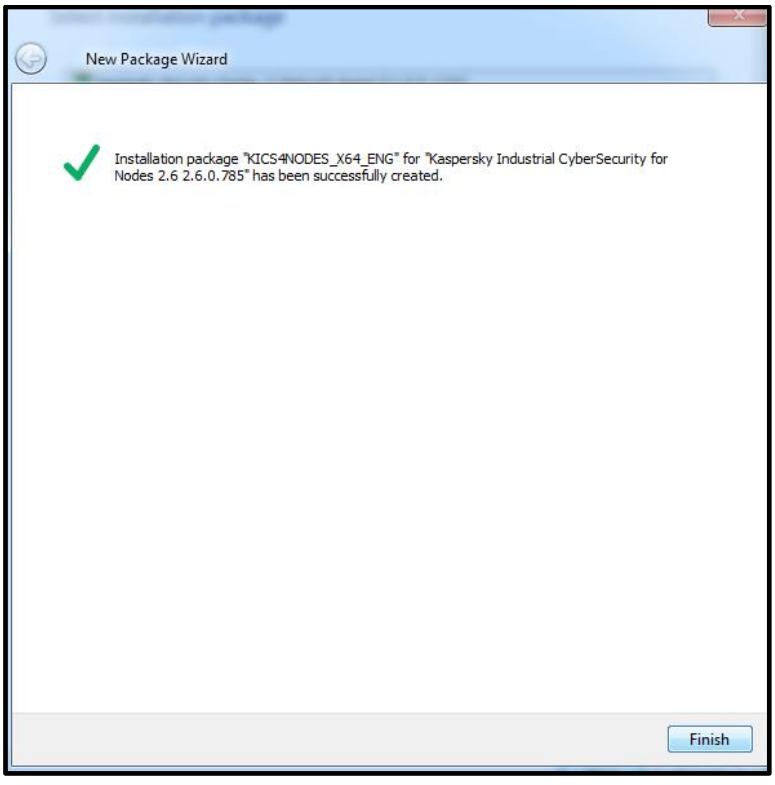
6. Accept the license agreement and privacy policy. Click **Next**.



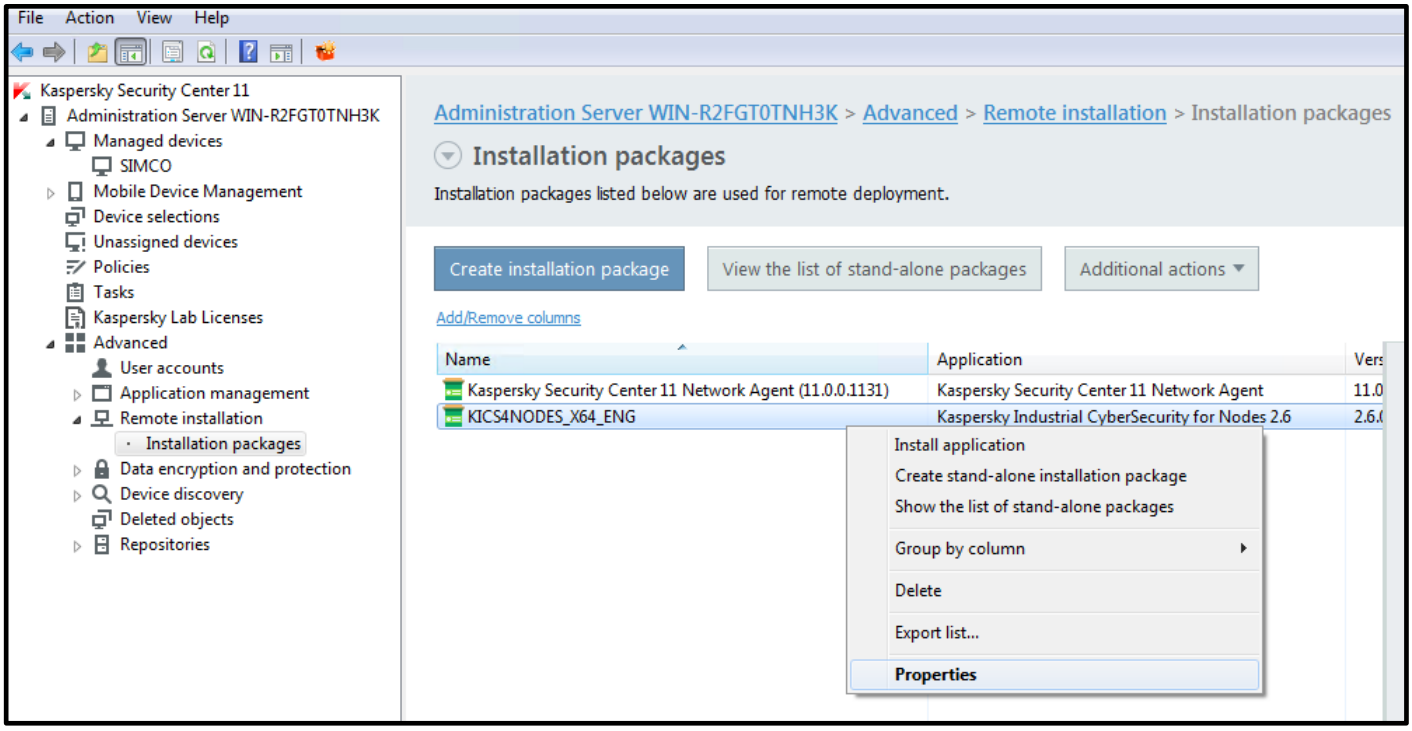
7. Wait while the installation package is being added to the **KSC** software repository.



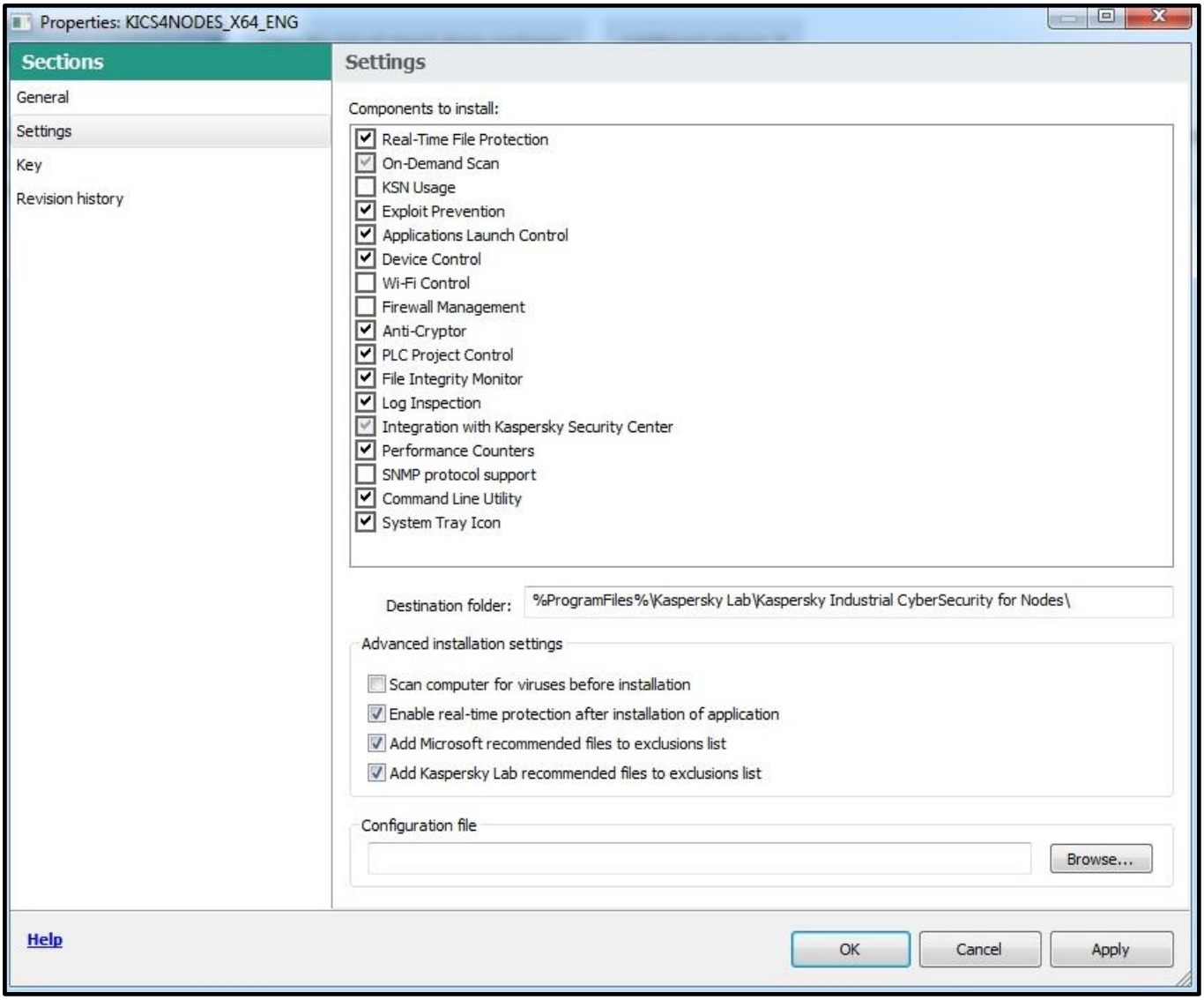
8. Press Finish upon installation completion to exit **New Package Wizard**. Click **Cancel** in the parent window to close **Remote Installation Wizard**.



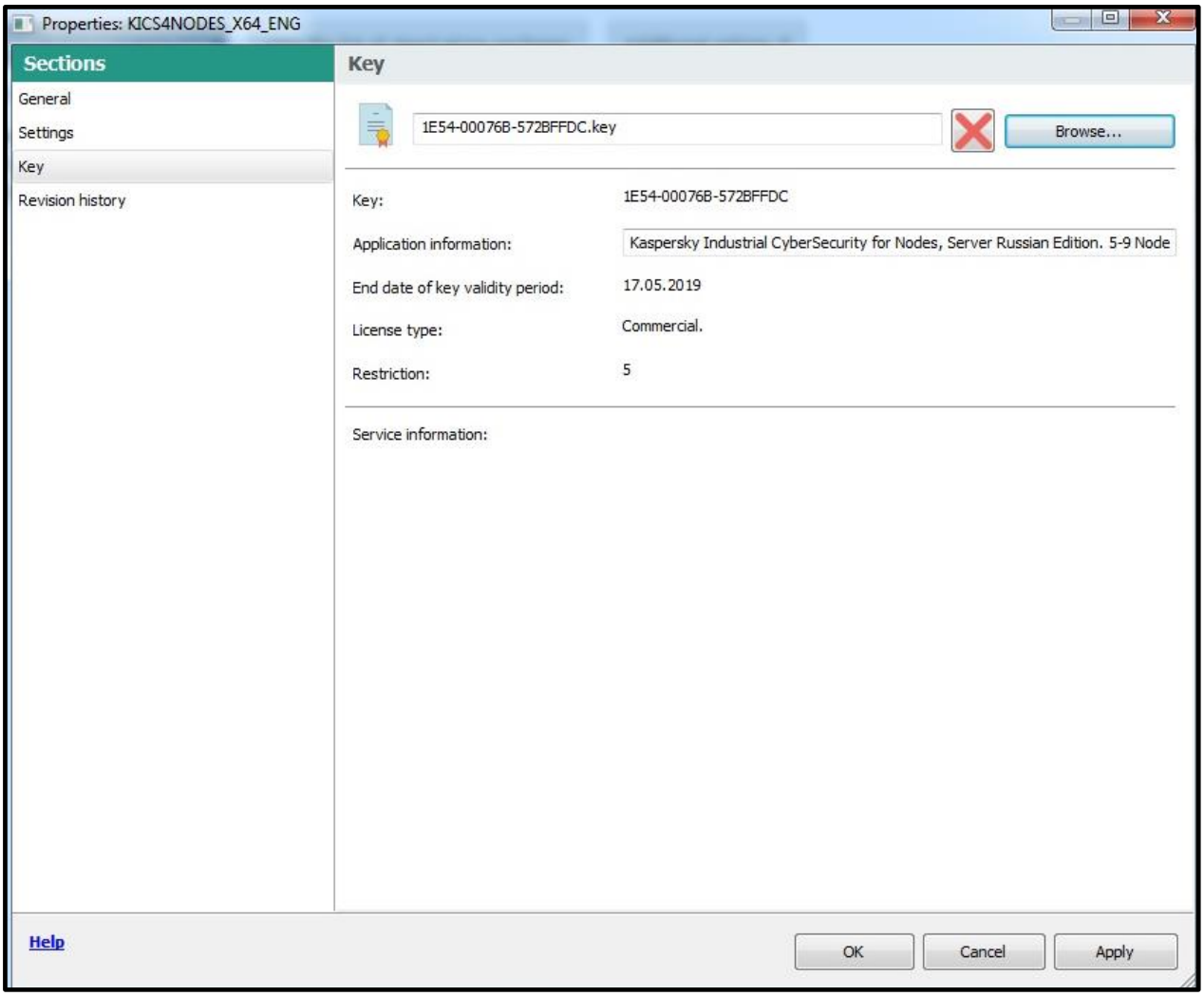
9. Go to **Administration Server->Advanced->Remote installation->Installation packages**. Select the just created installation package, right-click on it and choose **Properties** in the context menu.



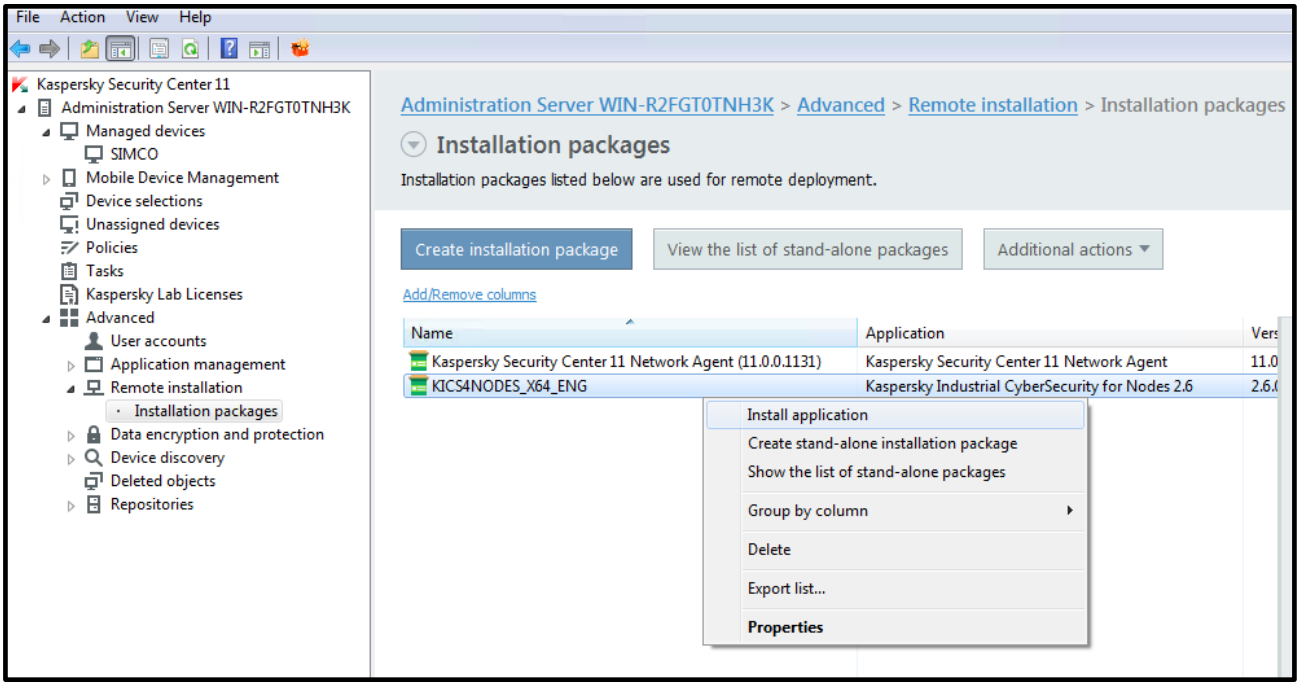
10. In the window that pops up, go to **Settings.** In the **Settings** pane, select **Components to install** strictly as shown below. Then specify **Advanced installation settings** as shown below.



11. Go to Key and, using the **Browse** button, locate the very same key-file (*.key) as was shown in “Initial configuration of KSC”. Follow the instructions of the familiar **Add key** wizard. Make sure that the license term is valid. Click **OK** to finalize fine-tuning the **KICS for Nodes** installation package.

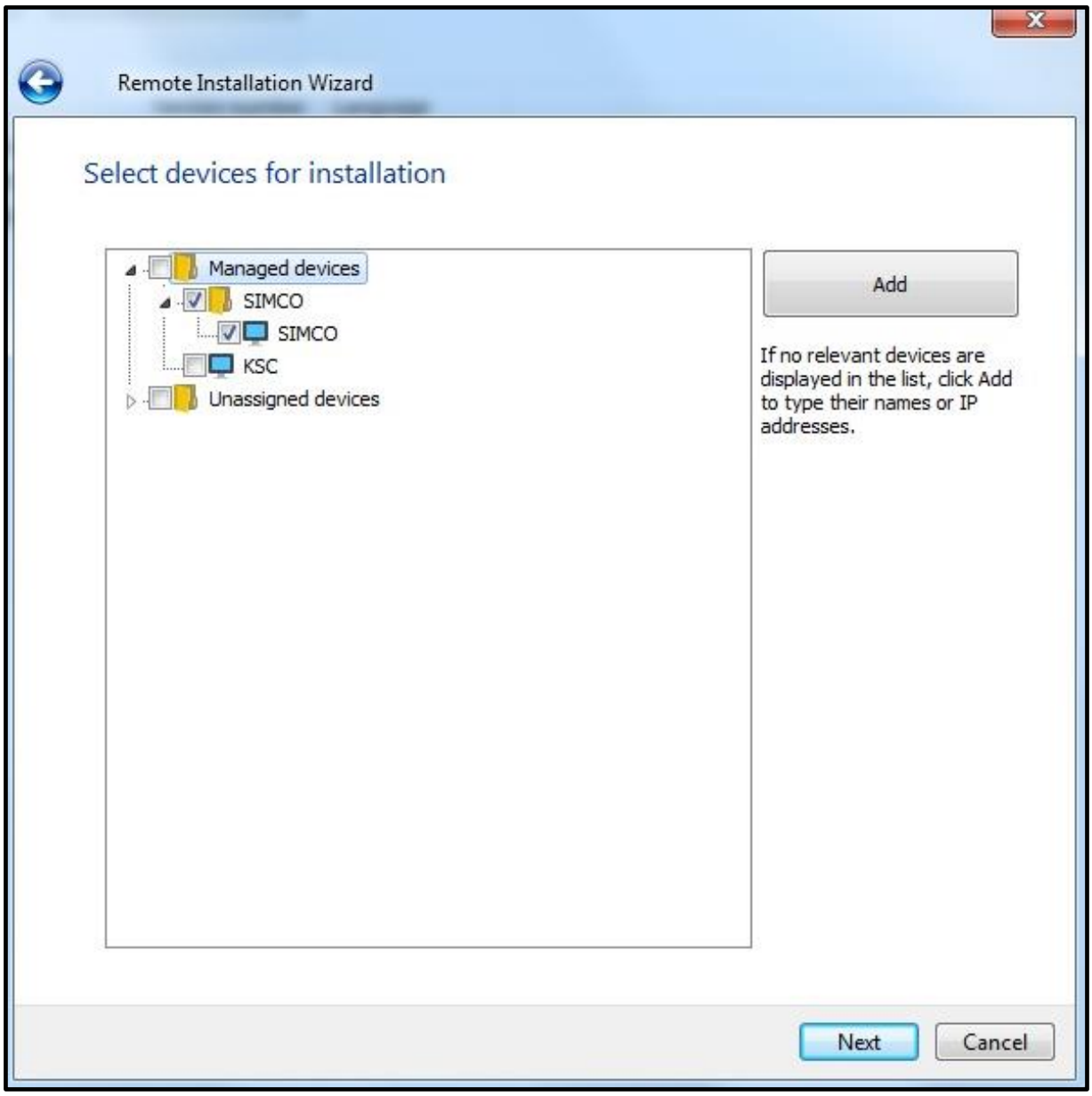


12. After you have created and tuned up the **KICS for Nodes** installation package, select it again, right-click on it and in the context menu choose **Install application**.

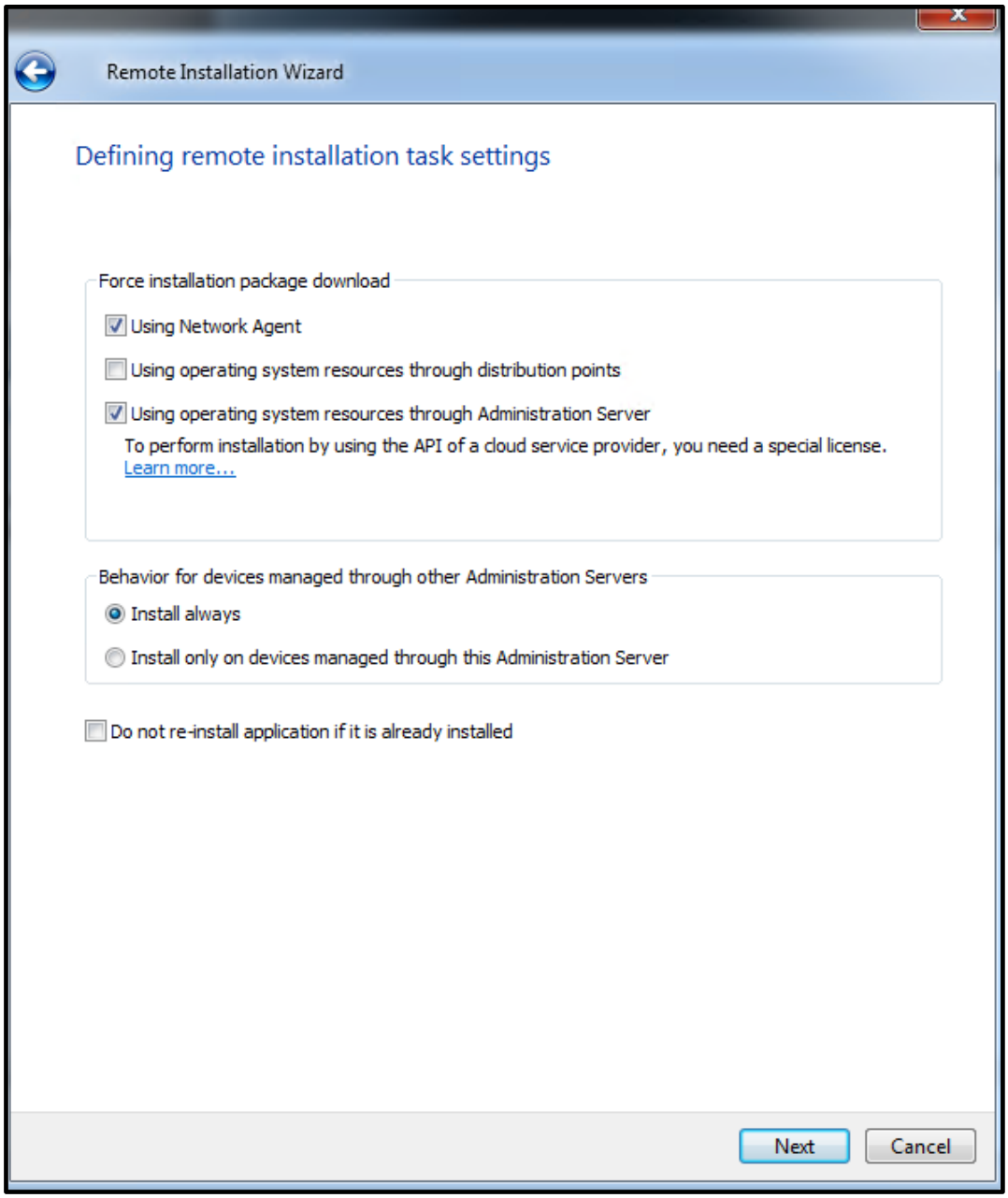


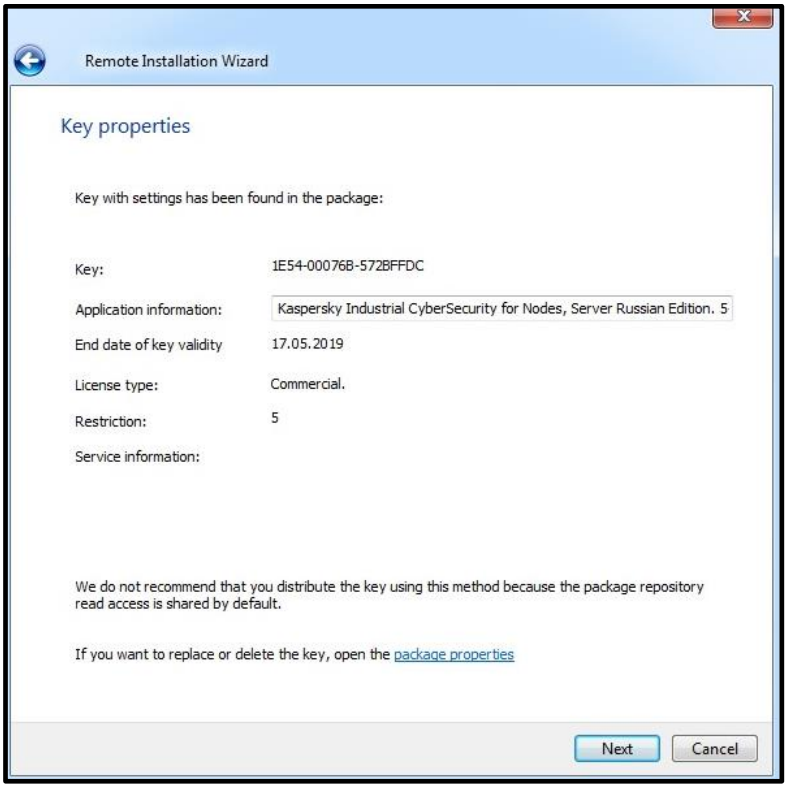
13. In the **Remote Installation Wizard** click **Select devices for installation**.

14. In the **Select devices for installation** tree view select the recently added device running **KLnagent** (in our case, **SIMCO**). Select it and press **Next**.

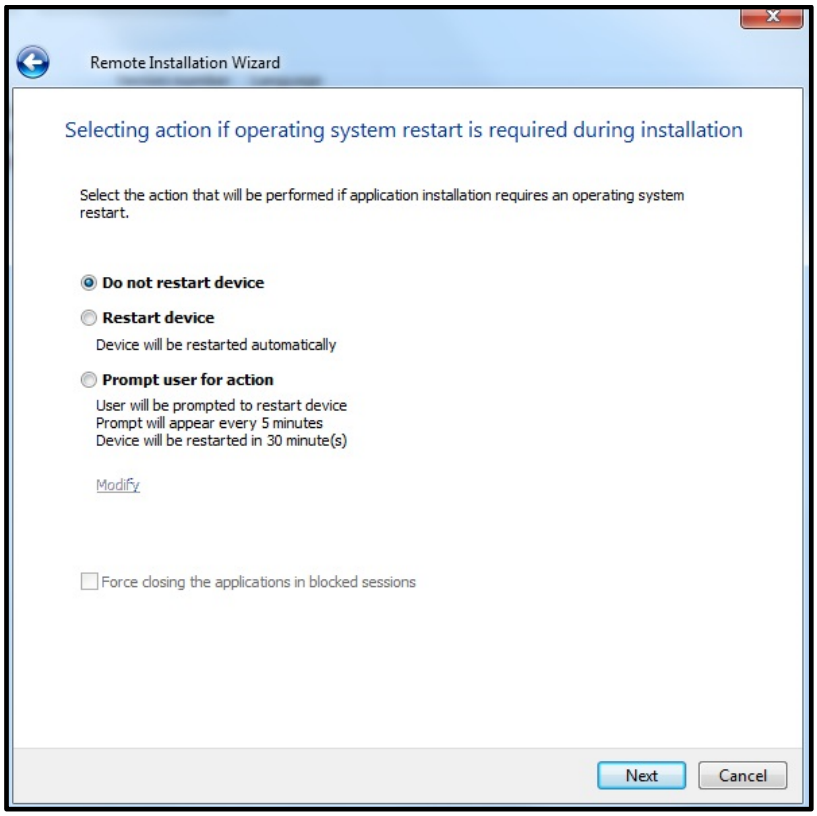


15. In the **Defining remote installation task settings** window, apply the settings as shown below. Click **Next**.

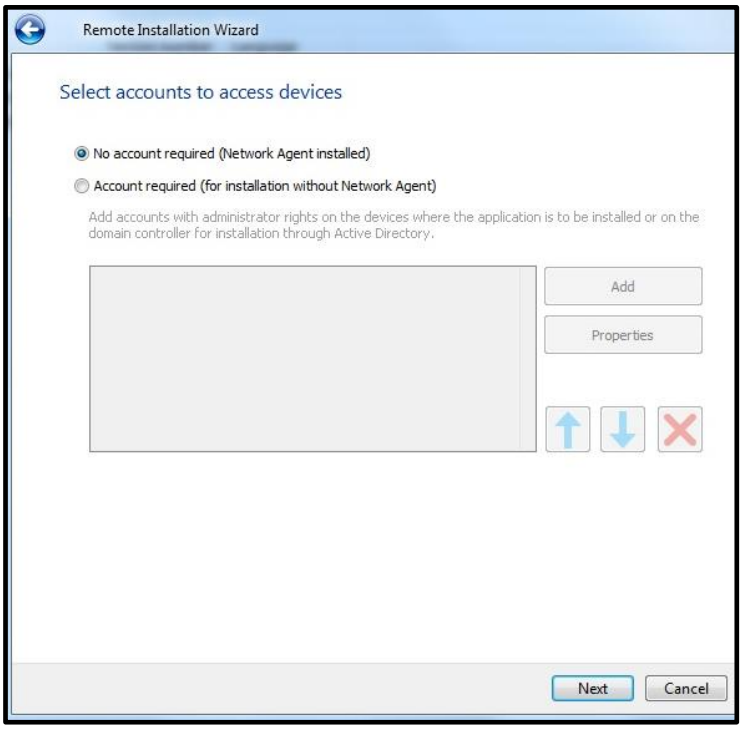




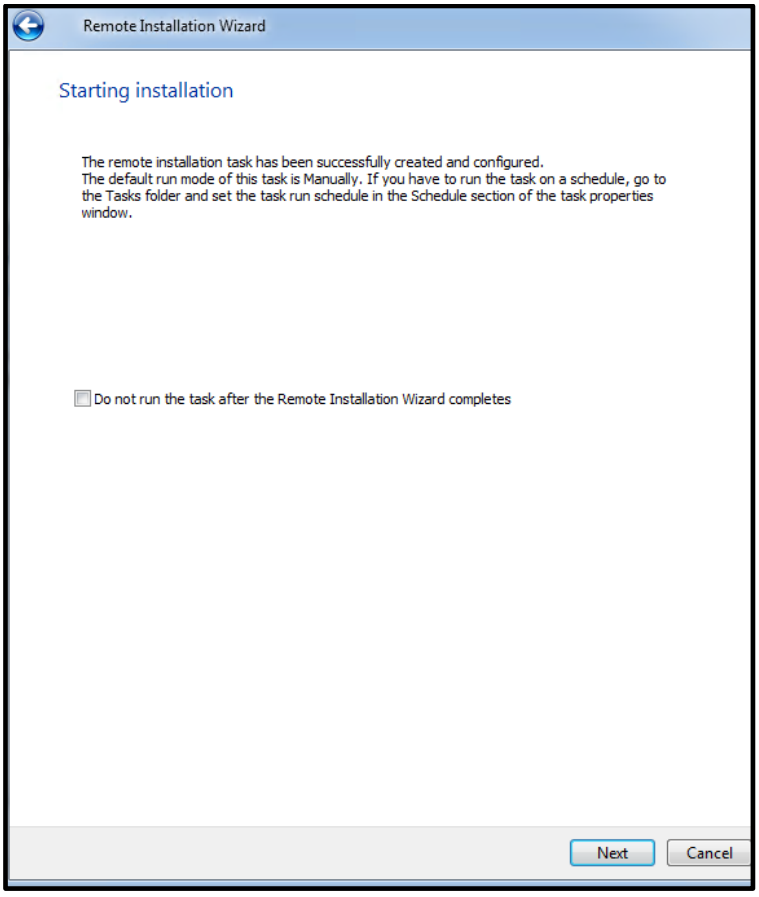
16. We have picked the license file before. Verify the terms once again and, if you agree, click **Next**.
17. In the windows that appears, apply the settings as shown below. Click **Next**.



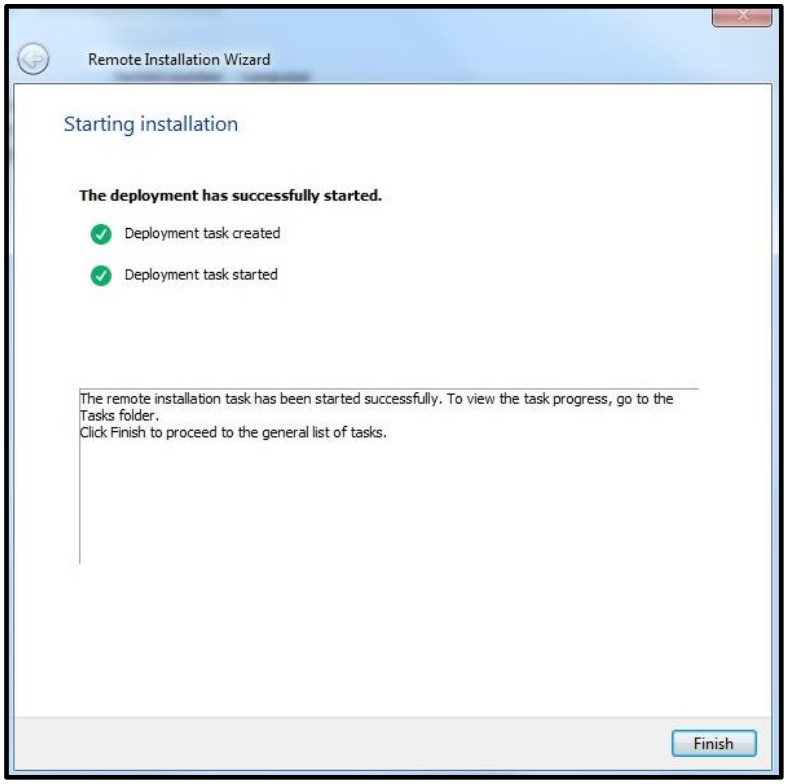
18. In the window that comes next, leave the default account settings as shown below. Click **Next**.



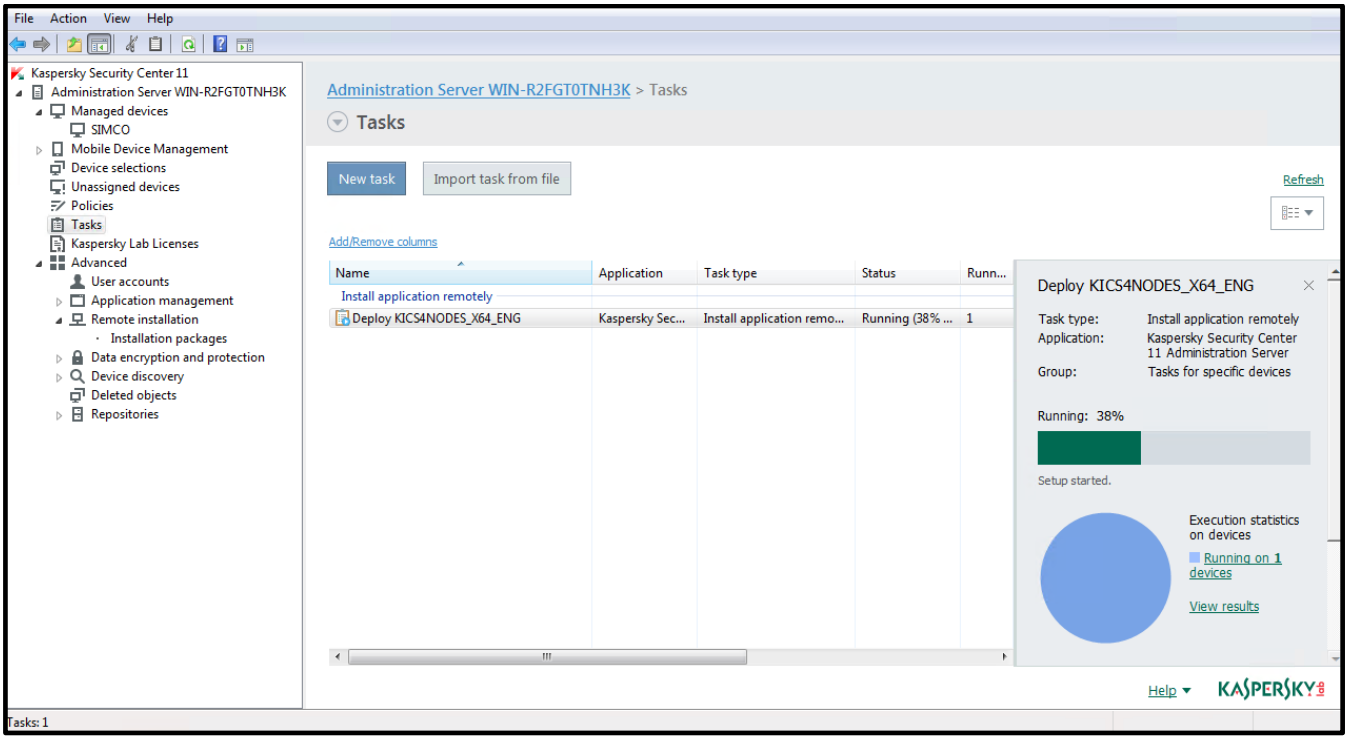
19. In the **Starting installation** window just click **Next**.



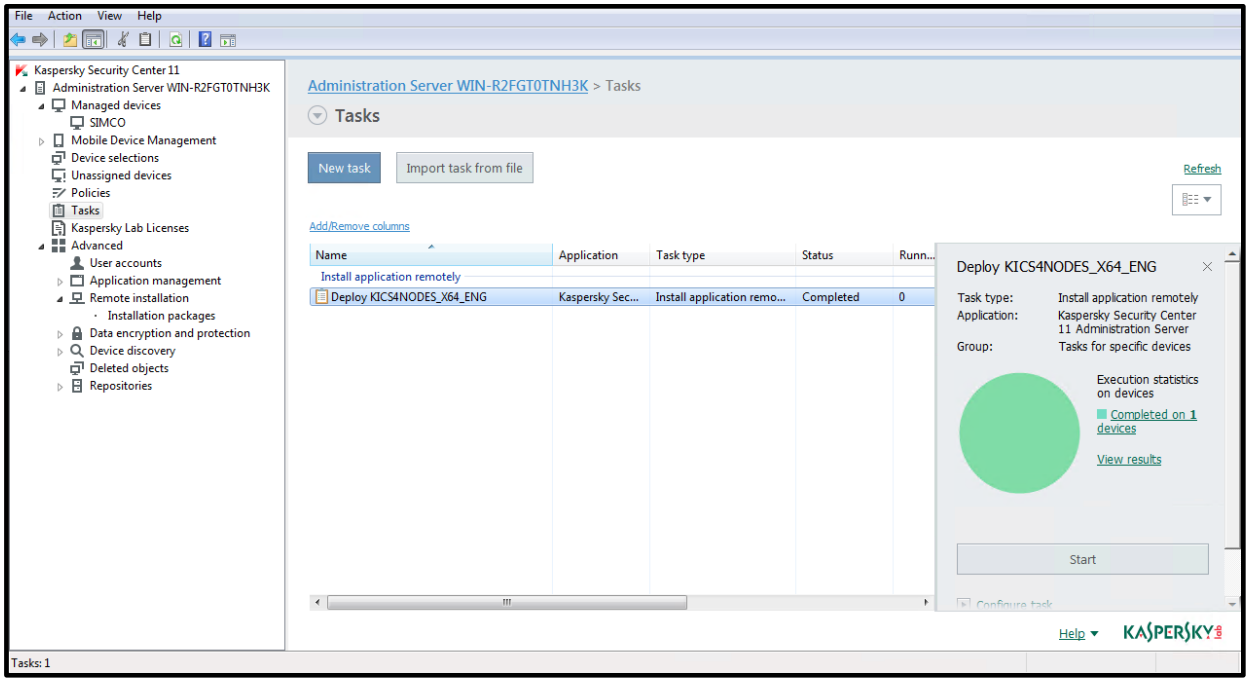
20. In the window that appears, just click **Finish**. Now we have created and launched the **KICS for Nodes** remote installation task.



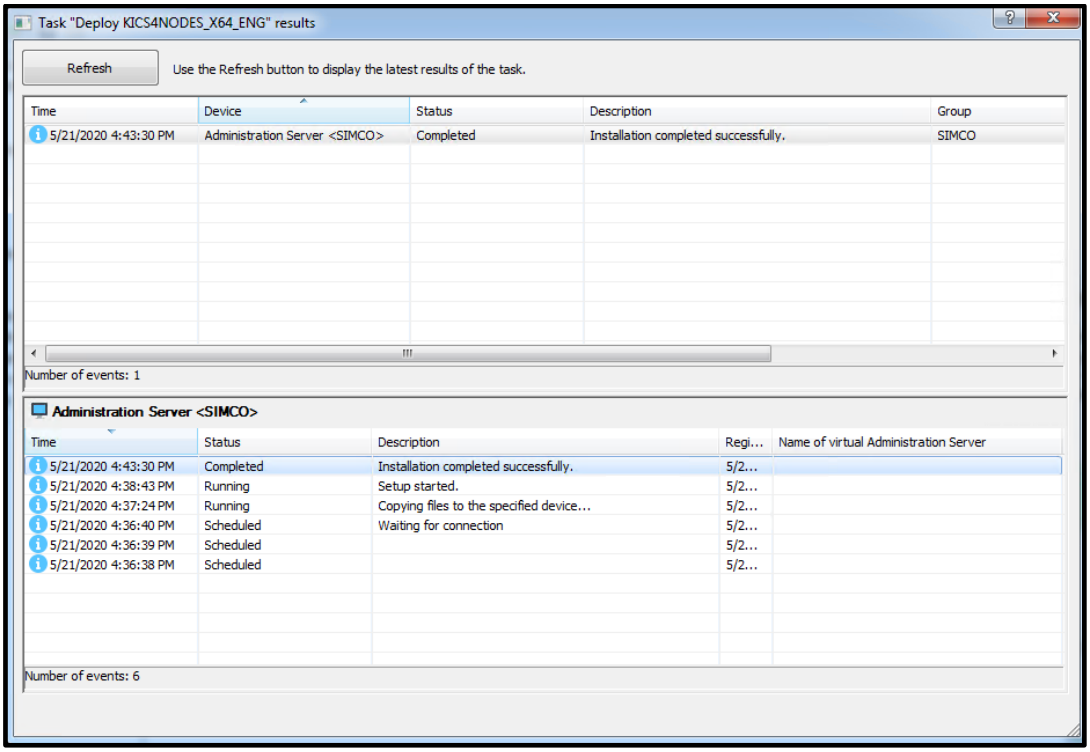
21. By going to **Administration Server->Tasks** and selecting the recently created remote installation task (**KICS for Nodes** deployment task), you can track its execution progress as shown below.



22. Wait until the installation task is completed[8]. Make sure that the task **execution statistics** are displayed as **Completed on … devices** and the chart has turned green.



23. You can learn details on the task execution by clicking **View results** in the right-hand pane. The task status window will pop up. Periodically click the **Refresh** button to update the displayed progress.



[8]A remote installation task may take up to 15 minutes depending on the performance of the target PC.

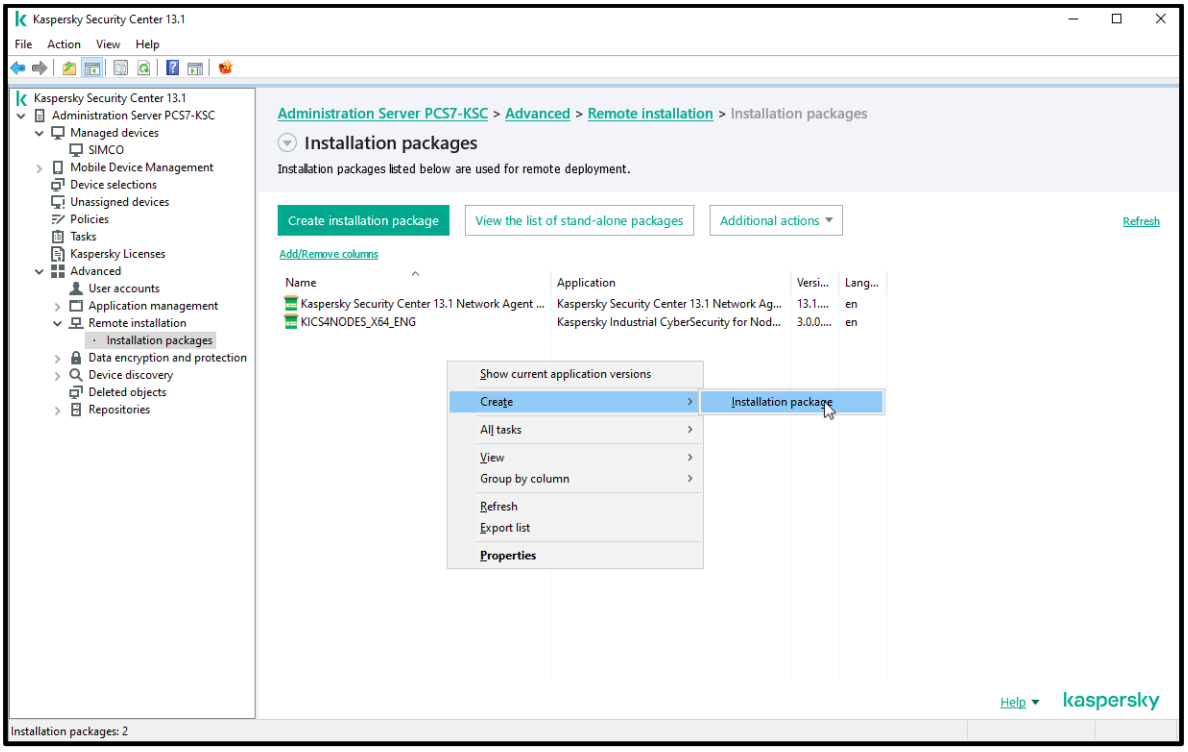
Remote installation of Hotfix onto target computers via KLnagent

At the time, we are writing this installation and deployment guide; the actual **Hotfix** version is **critical_fix_core_12**[9]**.** However, you are likely to receive the installation package with a newer **Hotfix**. Since the **Hotfix** installation procedure remains the same regardless of the version, we recommend that you always follow the steps described below. Every **Hotfix** is cumulative as it incorporates all the previous patches and improvements. Conversely, there is no need to uninstall the previous **Hotfixes** (if already installed) before installing the newest one.

The following note applies only to Russia: due to the industry-specific regulations of Russia, the installation of patches and Hotfixes relative to KICS for Nodes may be restricted so that this deployment step is sometimes skipped. Please refer to the section "FSTEK certification for KICS for Nodes installations within the territory of Russia" for details.

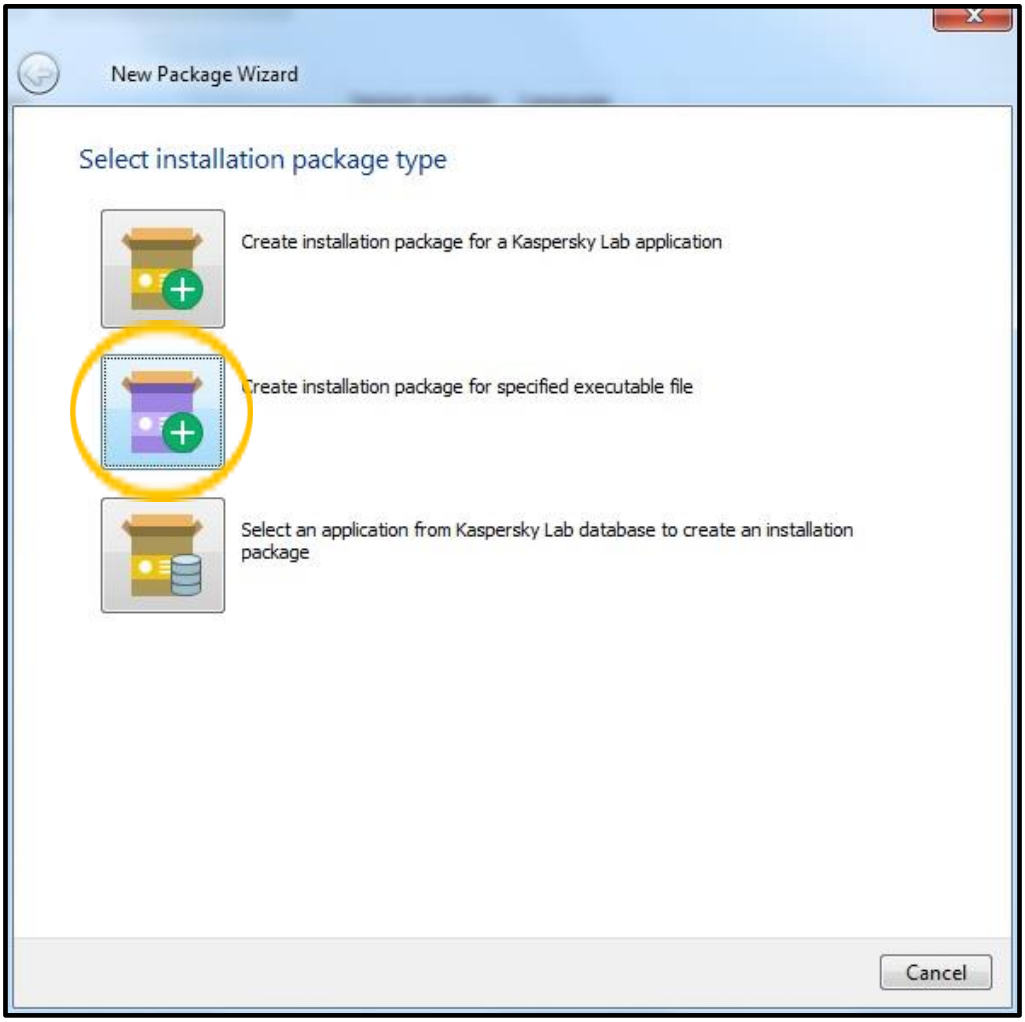
As before, we need to create an installation package for distributing our **Hotfix**.

1. Go to **Administration Server->Advanced->Remote Installation**. Right-click on any spare area of the installation packages list. In the context menu choose **Create->Installation package**.

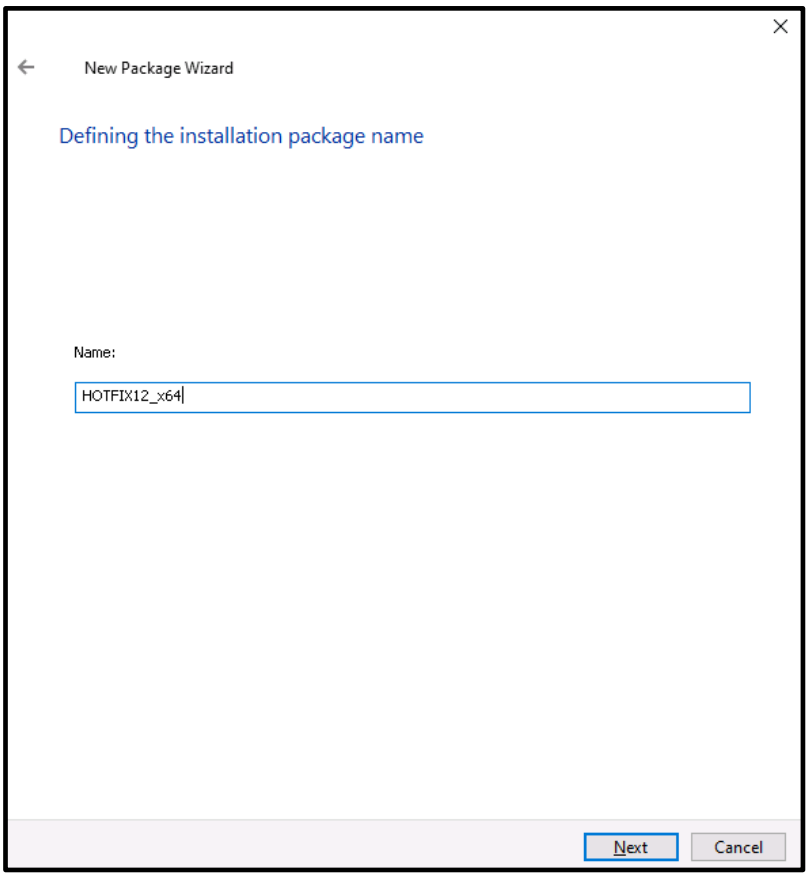


[9] As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a subsequent version has become available.

2. In the **Select installation package type** window, click **Create installation package for specified executable file**.

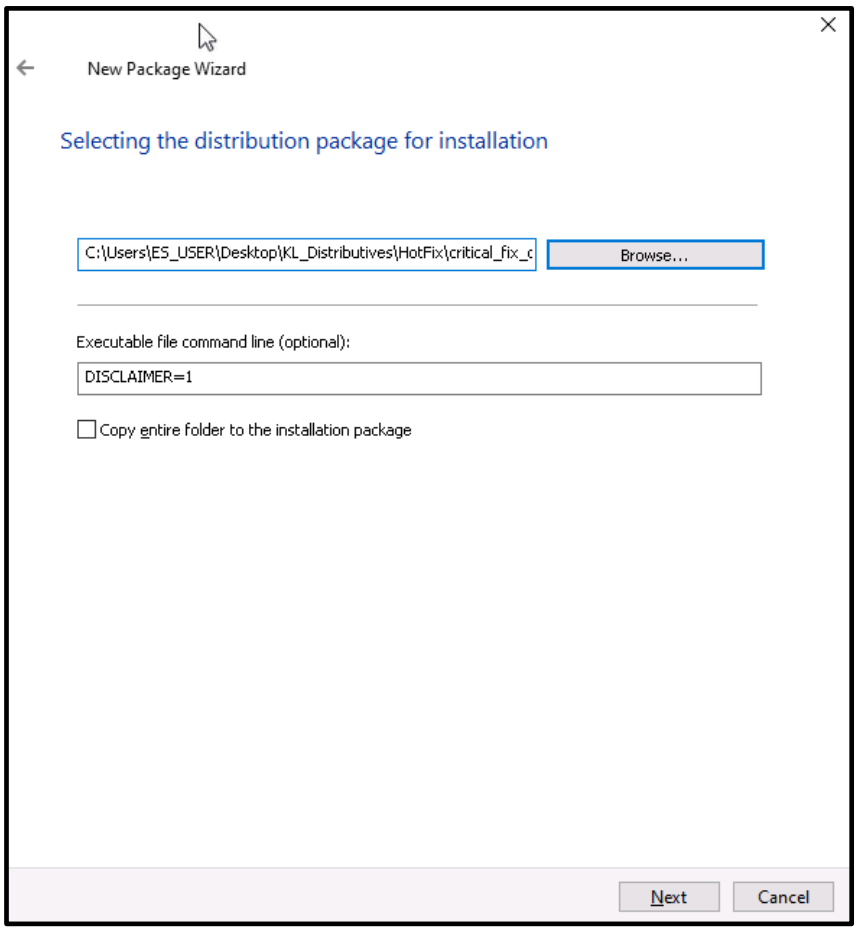


3. In the window that appears, give the **Hotfix** package a name (in our case, we are about to install **Hotfix 12**[10]). Click **Next**.



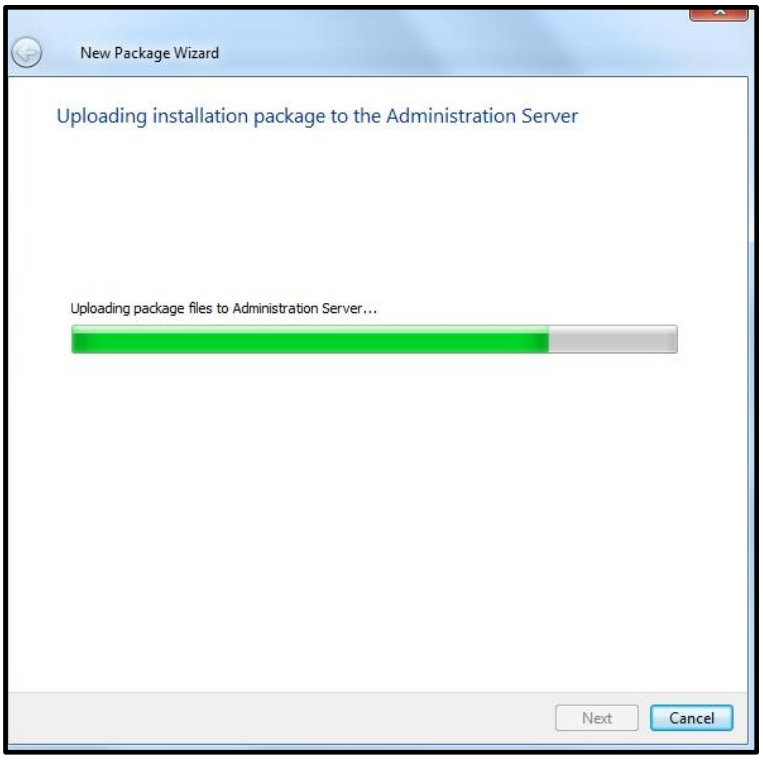
[10] Most likely, you have received a newer version of the **KICS for Nodes Hotfix**.

4. In the **Selecting the distribution package for installation** window, browse to the **Hotfix**[11] file supplied as a part of the distribution package (the **Hotfix** file has the *.**msp** extension). Specify the **DISCLAIMER=1** attribute in the **Executable file command line** field and uncheck **Copy entire folder to the installation package**. Click **Next**.

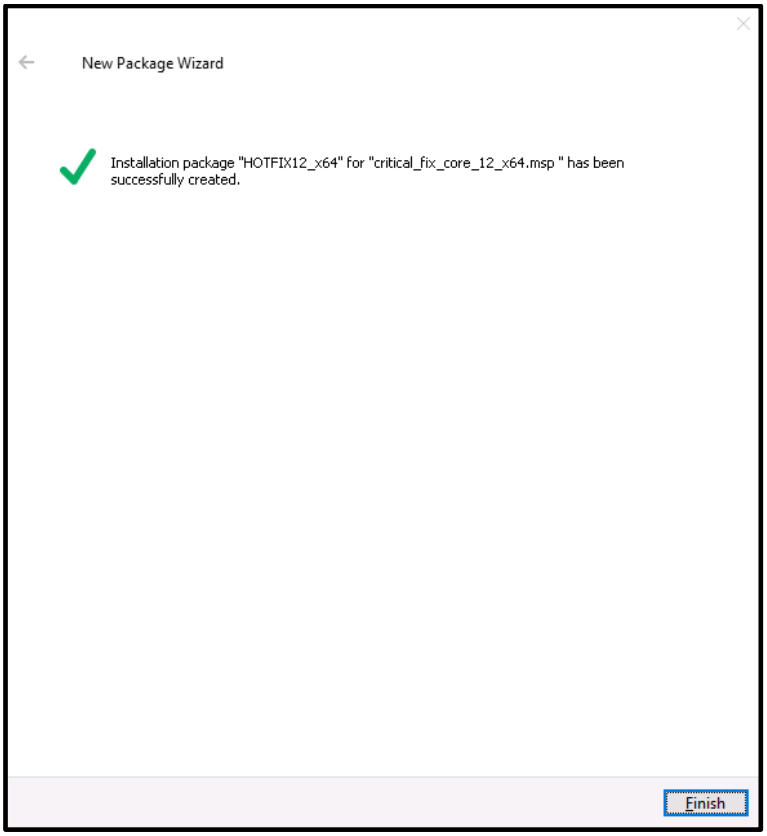


[11] You should mind suffixes **X64** and **X86** in the names of **Hotfix** installation files. The installation file must match the target operating system you are planning to install **Hotfix** onto.

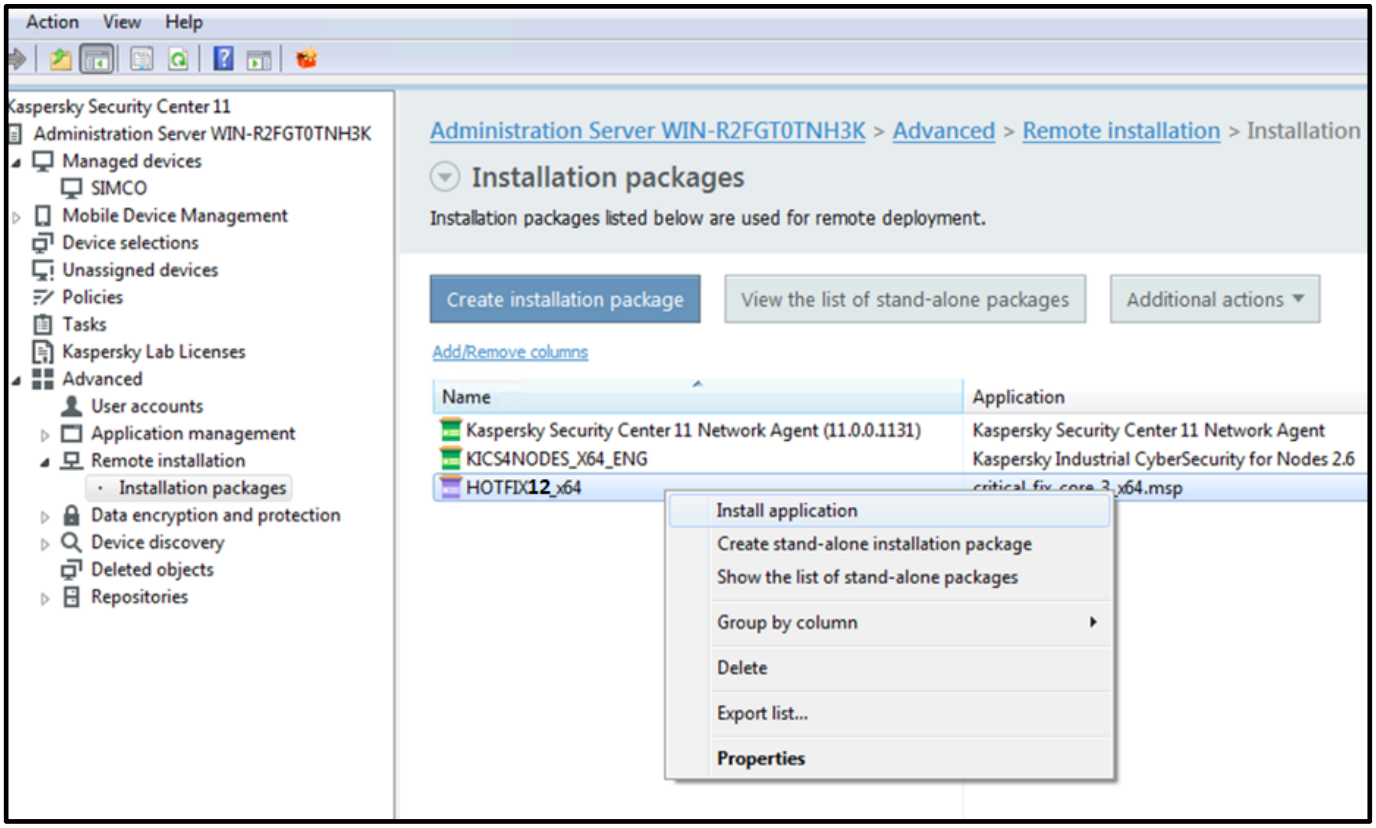
5. Wait while the **Hotfix** is being uploaded to the **Administration Server** repository.



6. Make sure that the **Hotfix** installation package has been successfully created and click **Finish**.

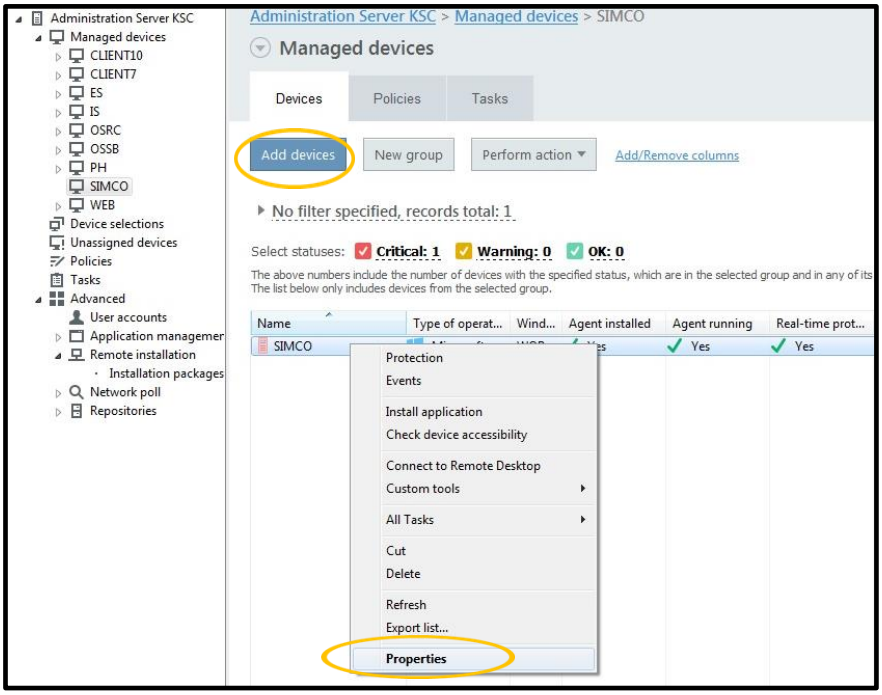


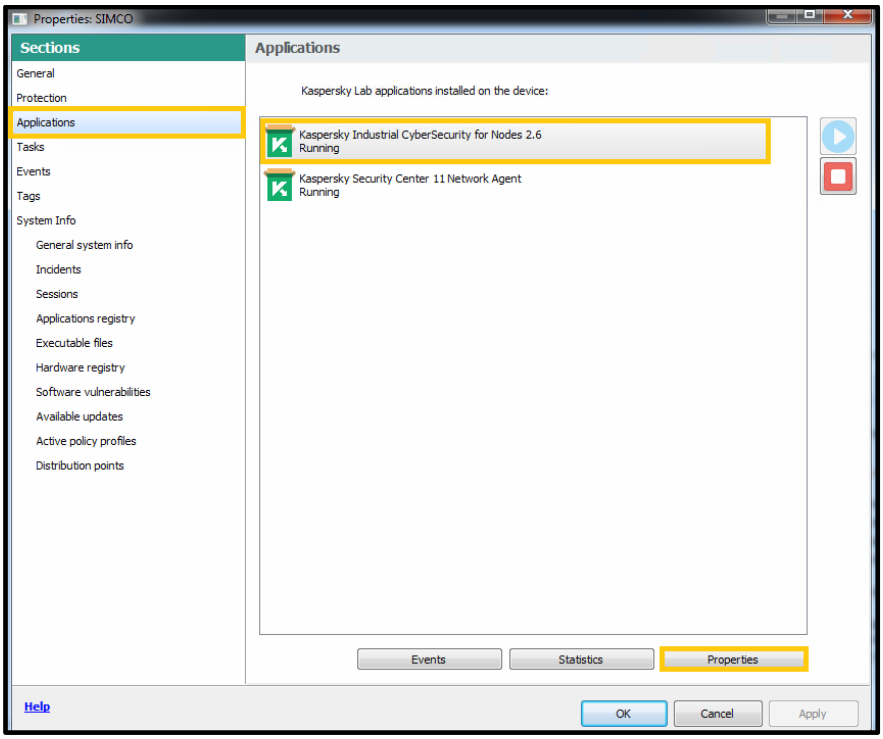
7. Go to **Administration Server->Advanced->Remote Installation->Installation packages**. Right-click on the recently created **Hotfix** installation package and in the context menu choose **Install application**.



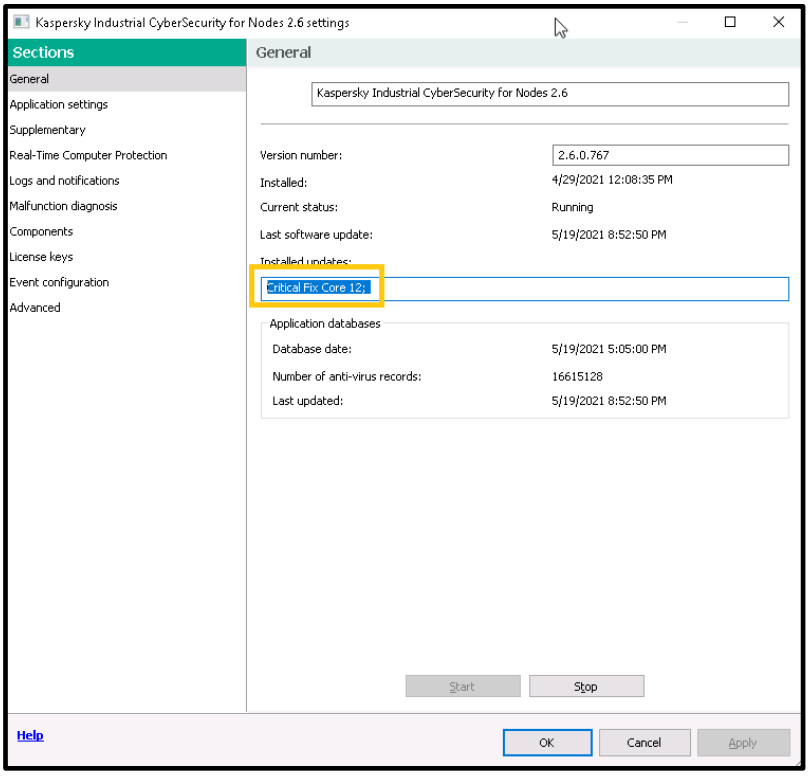
8. Perform exactly the same steps as were described in “Remote installation of KICS for Nodes onto target computers via KLnagent”. At every subsequent prompt of the wizard, specify the same settings as we did during the **KICS for Nodes** remote installation. The remote installation may last up to 10 minutes. During the **Hotfix** installation, target computers may restart the **KICS for Nodes** services.

9. In order to make sure that the **Hotfix** installation has been successful, go to your device located in the managed devices group (in our case, **SIMCO**). Then right-click on the device and select **Properties** in the context menu. Using the **Properties** window go to **Application**, select **Kaspersky Industrial CyberSecurity for Nodes 2.6** and finally press the **Properties** button located beneath the list of installed applications.

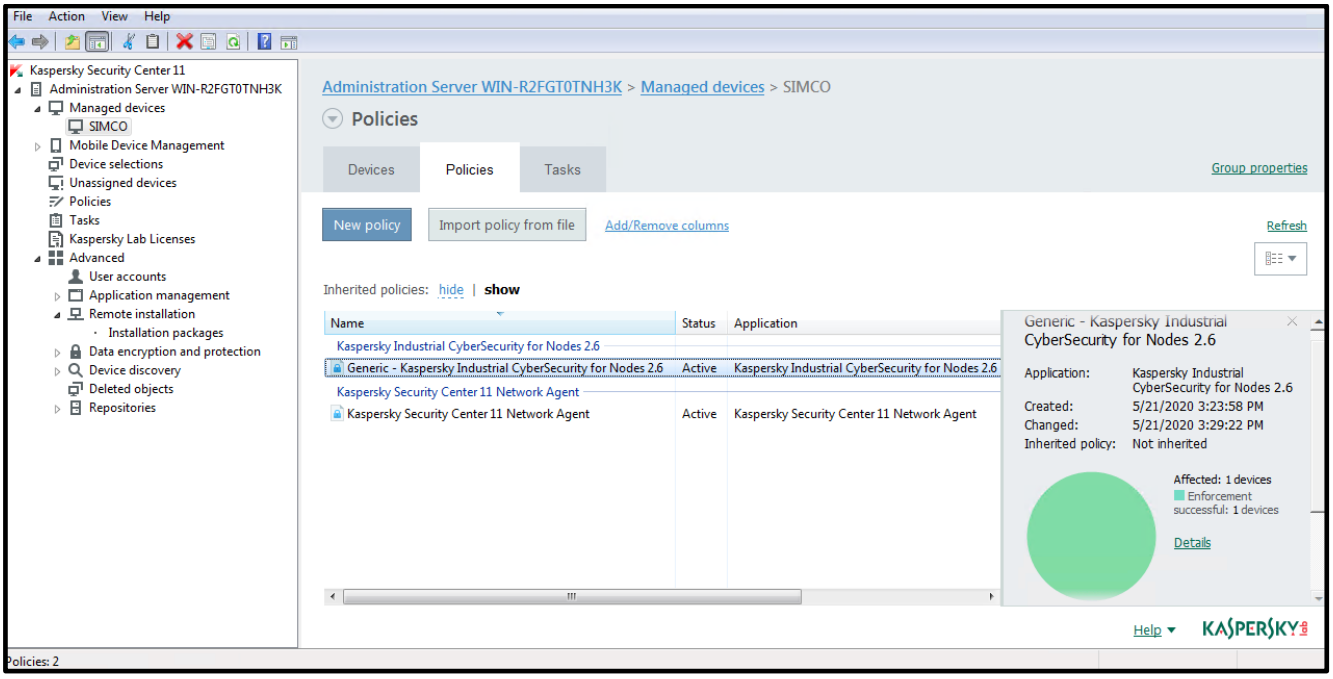




10. If the **Hotfix** installation has been successful, we should see that the **Installed updates** field contains the name of the recently deployed **Hotfix**.



11. Finally, it makes sense to verify that the recently created generic policy has reached the target host. Similar to your tasks, you can track policy enforcement by viewing the right-hand pane as shown below. Wait until the round diagram turns green, which means that the selected policy has been successfully propagated and applied.



Rule generation optimization for Application Launch Control

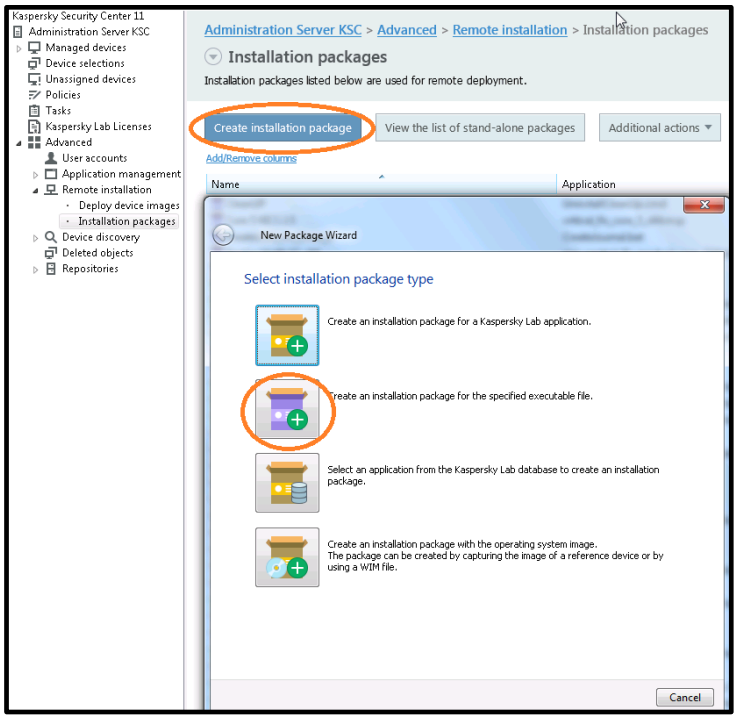
In order to ensure maximum performance and compatibility with **PCS 7 9.1** it is recommended to consider one crucial precaution. Please mind that it is solely applicable to **PCS 7 engineering** workstation; it is not required to perform the following steps on any other type of a **PCS 7** station. If a protected (target) computer hosts the **Simatic Manager** or **STEP 7** engineering software, it is advised to reduce the number of automatically generated allowing rules for **Application Launch Control**. It is done by specifying some generator scope exclusions.

You may use the following batch file to introduce the recommended generator scope exclusions. The file should be once launched on the engineering workstation right after the **Hotfix** installation. The file should be propagated from **KSC** and remotely executed as **system** as guided below:

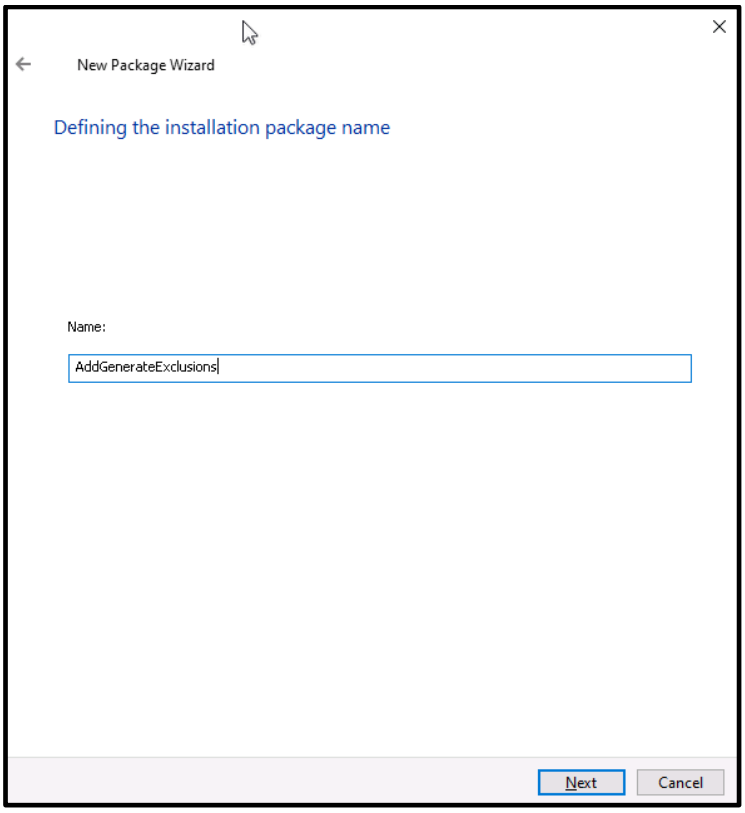
1. Create a batch file with the following contents:
   @echo off
   set exclusion="C:\Program Files (x86)\SIEMENS\STEP7\s7hlp*.js"
   setlocal enableextensions enabledelayedexpansion

   reg query
   "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.6\Environment" >nul
   if %errorlevel% equ 1 goto OUTNOW
   reg add
   "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.6\Environment" /f /v
   ALCRuleGenExclusions /t REG_MULTI_SZ /d %exclusion%
   :OUTNOW
   exit
2. Save the file as **AddGenerateExclusions.bat**.

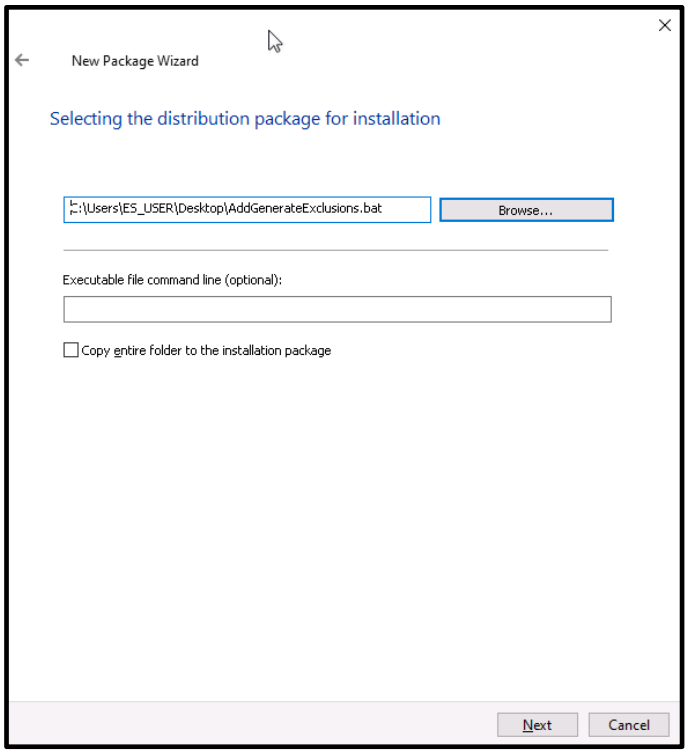
3. Initiate the new installation package creation as shown below.



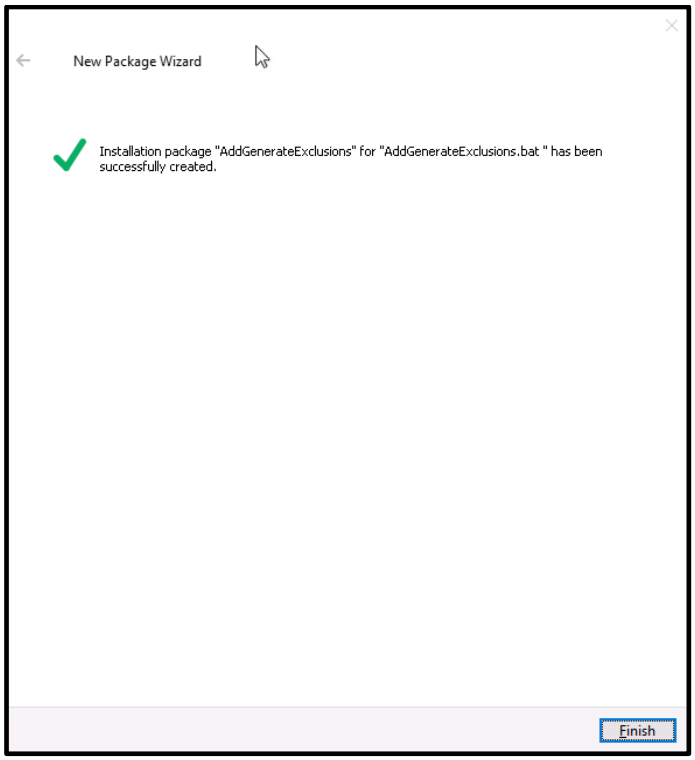
4. Give a meaningful name to the new installation package. Click **Next**.

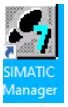


5. Select the **AddGenerateExclusions.bat** file you have just created and click **Next**.

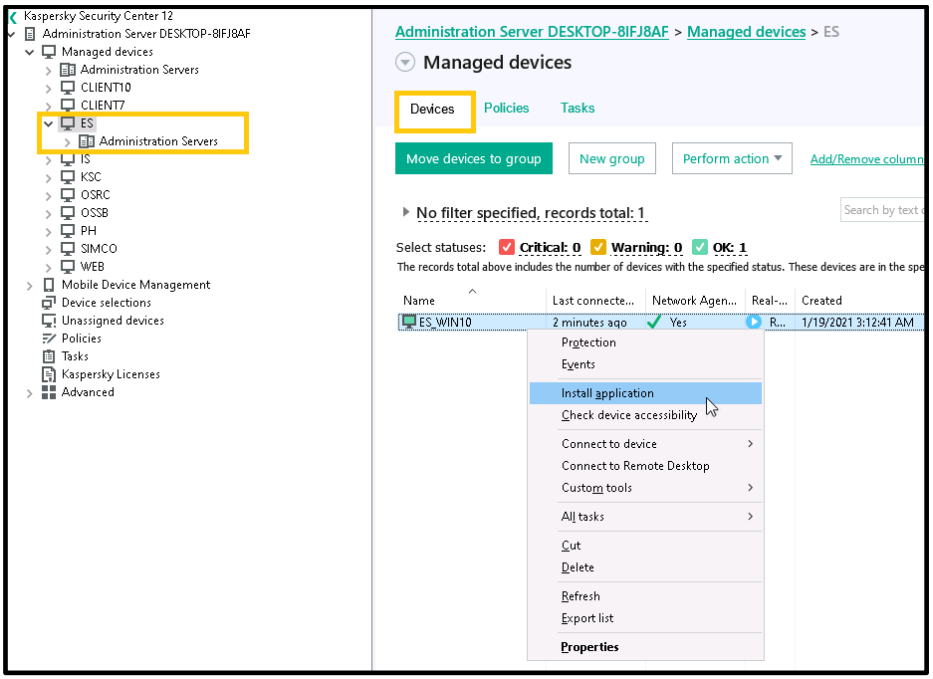


6. Wait until the installation package is created and click **Finish**.

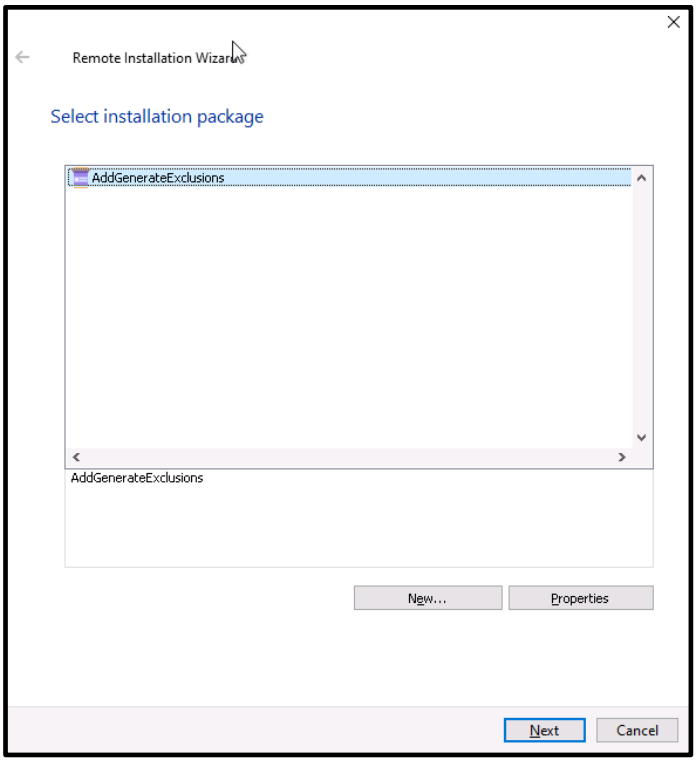


7. Let us suppose, we have **Simatic Manager** 

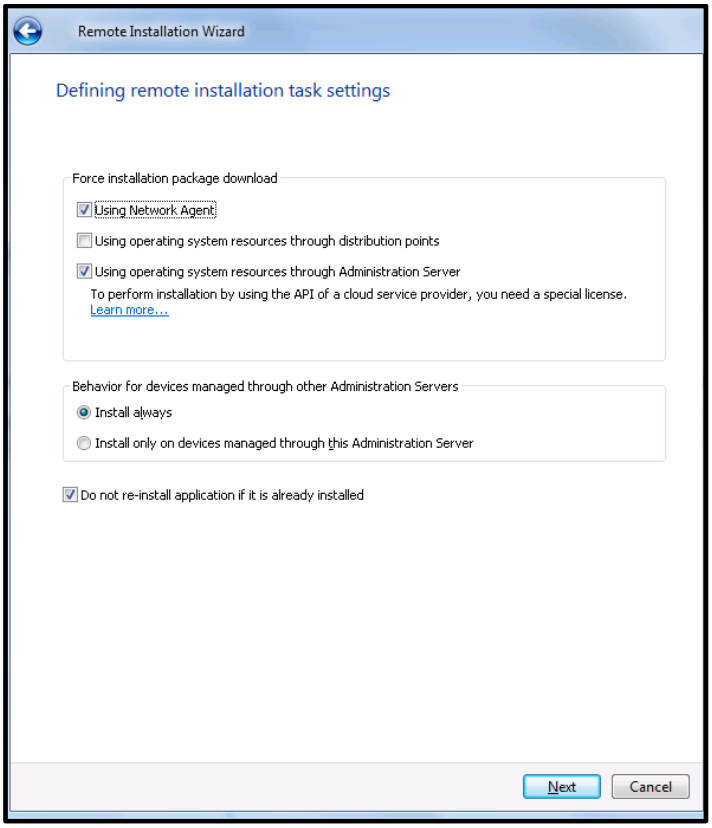
installed on the **ES_WIN10** engineering workstation. As was mentioned before, we need to run **AddGenerateExclusions.bat** to optimize rule generation on that workstation. So, we should go to the **ES_WIN** node, right-click on it and choose **Install application** from the context menu.



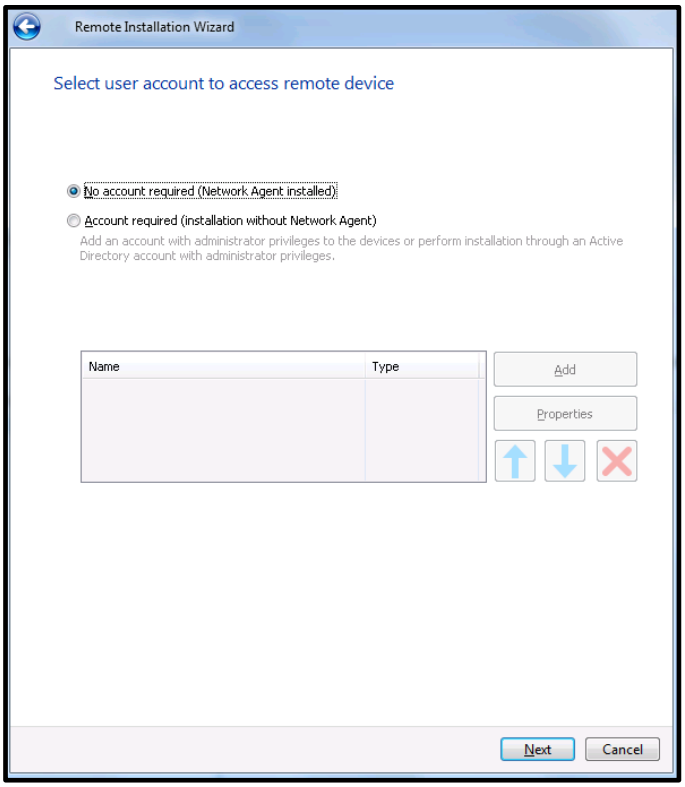
8. Select the recently created installation package containing the batch file and click **Next**.

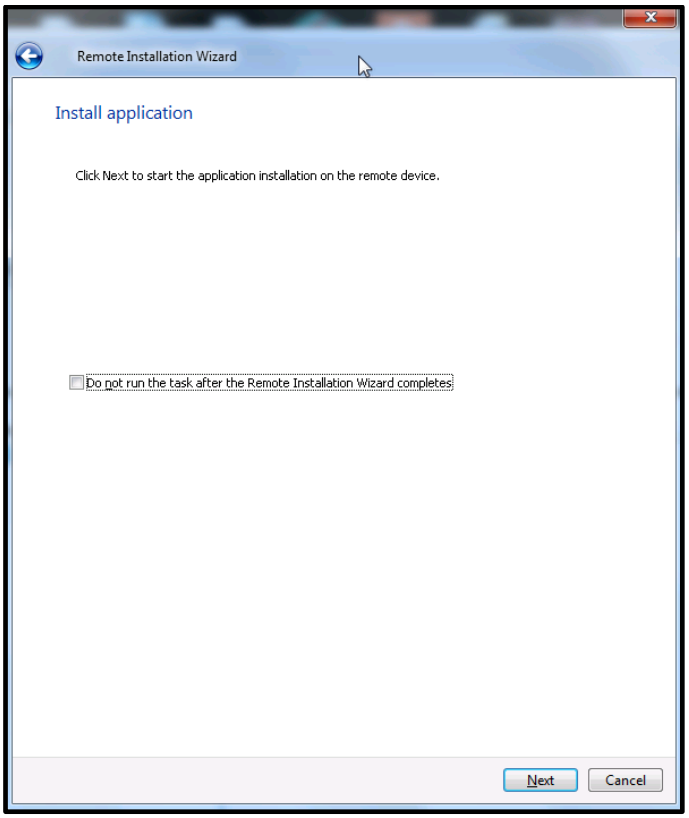


9. Preserve the default settings and click **Next**.

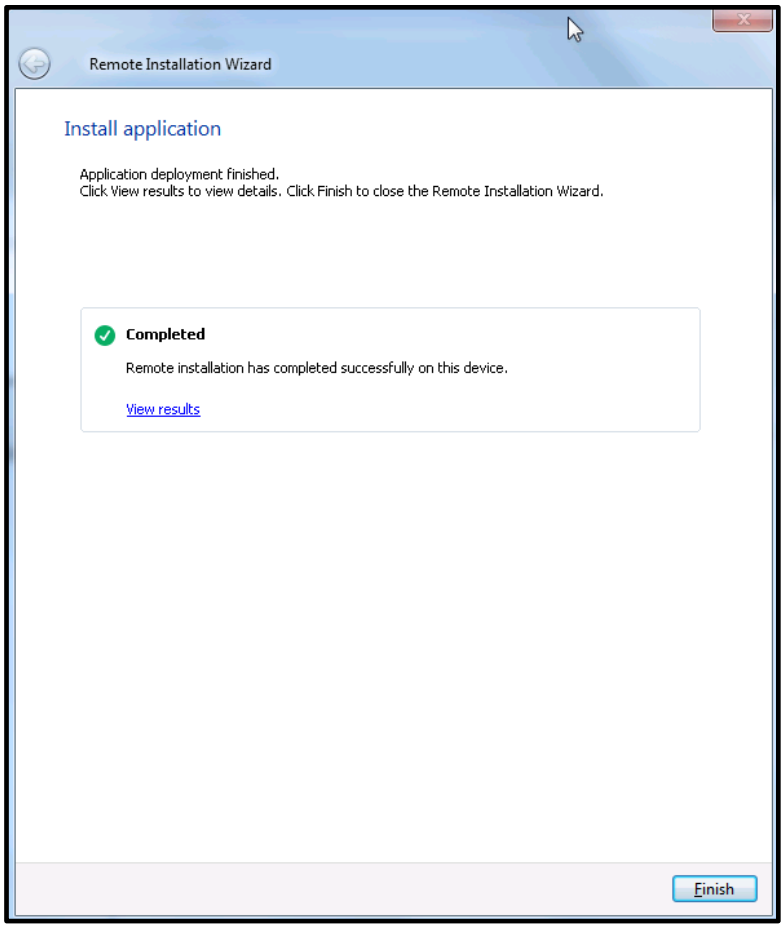


10. Proceed with the default settings as shown below.





11. Wait until the remote installation (execution, in our case) is completed and click **Finish** to quit the wizard.



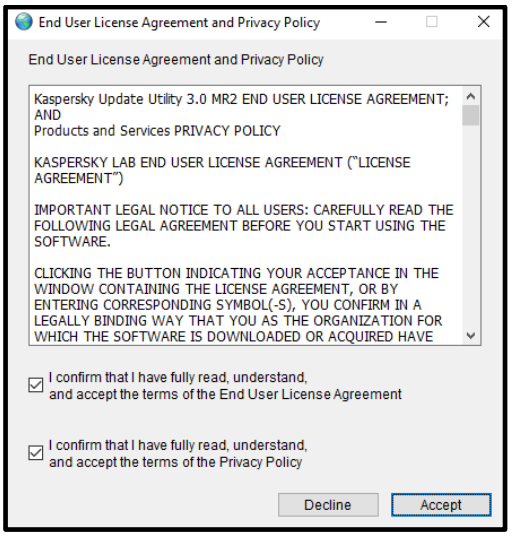
Initial update of antivirus databases

Apparently, it is vitally important to keep **KICS for Nodes** AV definitions up to date. Although **KICS for Nodes** is designed to be tolerant to extremely rare AV definitions updates, it still requires occasional updates ensuring its secure and efficient operation. There are at least three ways you can maintain antivirus databases actualized:

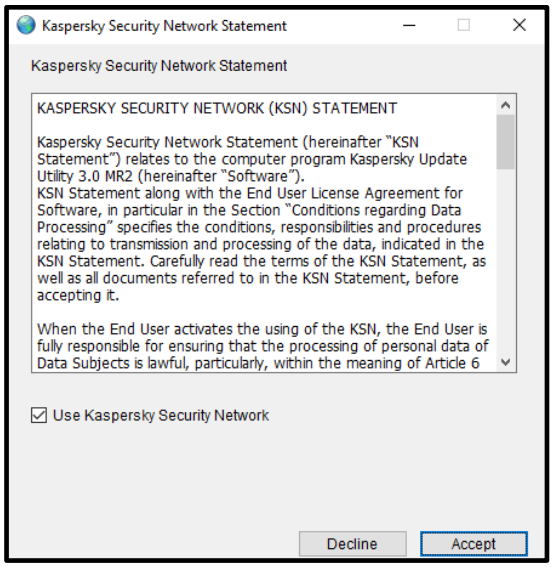
- By letting the **KSC** server retrieve updates from the Kaspersky Lab update sources available on the Internet and by performing databases propagation to **KICS for Nodes** devices directly from the **KSC** repository. This requires that your **KSC** server should be connected to the Internet.
- By letting **KICS for Nodes** devices retrieve updates directly from the Kaspersky Lab update sources available on the Internet. This scheme does not utilize **KSC** but it requires that every **KICS for Nodes** device be able to access the Internet.
- By manual retrieval of updates from the Internet using **Kaspersky Update Utility**. It enables you to store the updates on some intermediary file server (located in DMZ, for example). Once the updates are available on the secure file server, you can tell **KICS for Nodes** devices to retrieve updates from that file server.

The latter scheme seems to be the most realistic for industrial sites. Therefore, we will solely focus on it. To make things simple, we are going to use **KSC** as an intermediary file server storing **KICS for Nodes** updates. In practice, it can be any secure file server, which **KICS for Nodes** devices has network connectivity to.
Follow the instructions given below:

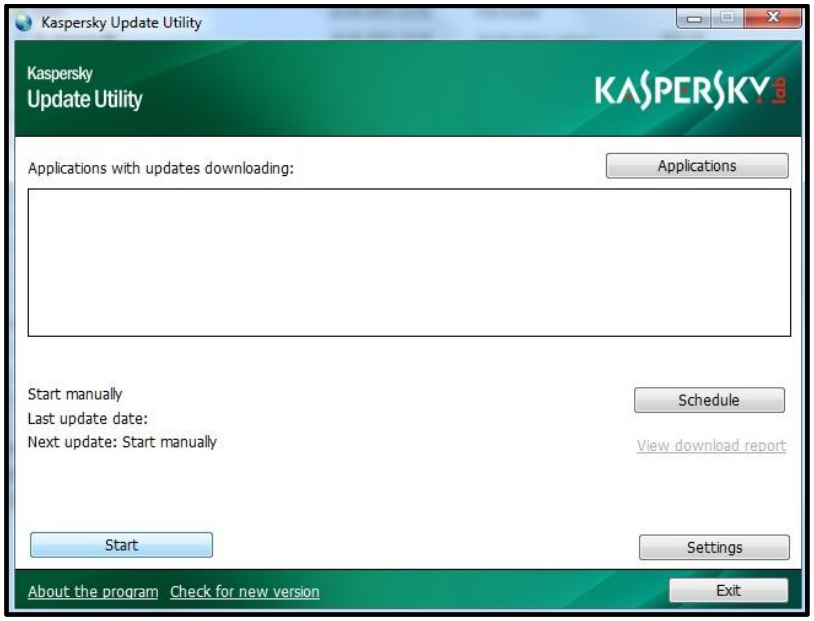
1. Let us create a new folder **KLUpdate** on the **C:** drive of our **KSC** server. This folder will be used for storing antivirus updates.
2. Follow https://support.kaspersky.com/updater3 and download **Kaspersky Update Utility**.
3. Decompress the downloaded zip-archive to the recently created folder **C:\KLUpdate**.
4. Launch **UpdateUtility-Gui.exe** from **C:\KLUpdates.**
5. Accept terms and conditions of use and privacy policy.



6. Accept **KSN** use terms and conditions.

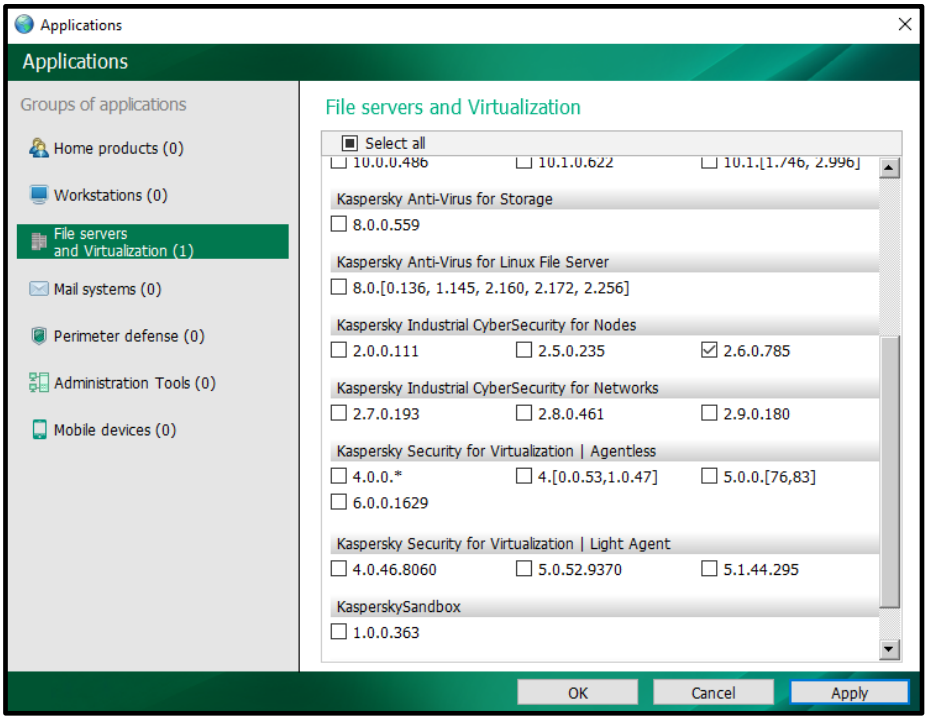


7. The following window should appear.

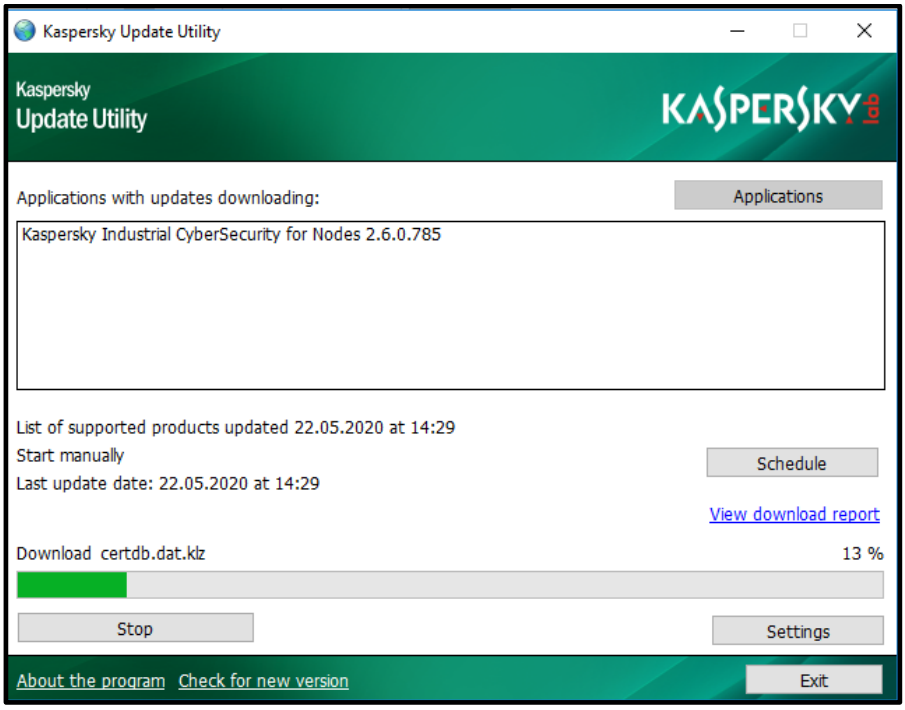


8. Click the **Start** button to update **Kaspersky Update Utility** itself in case its newer version has come out.

9. Press the **Applications** button and go to **File servers and Virtualization.** Check **Kaspersky Industrial CyberSecurity for Nodes 2.6.0.785** as shown below. Click **OK**.

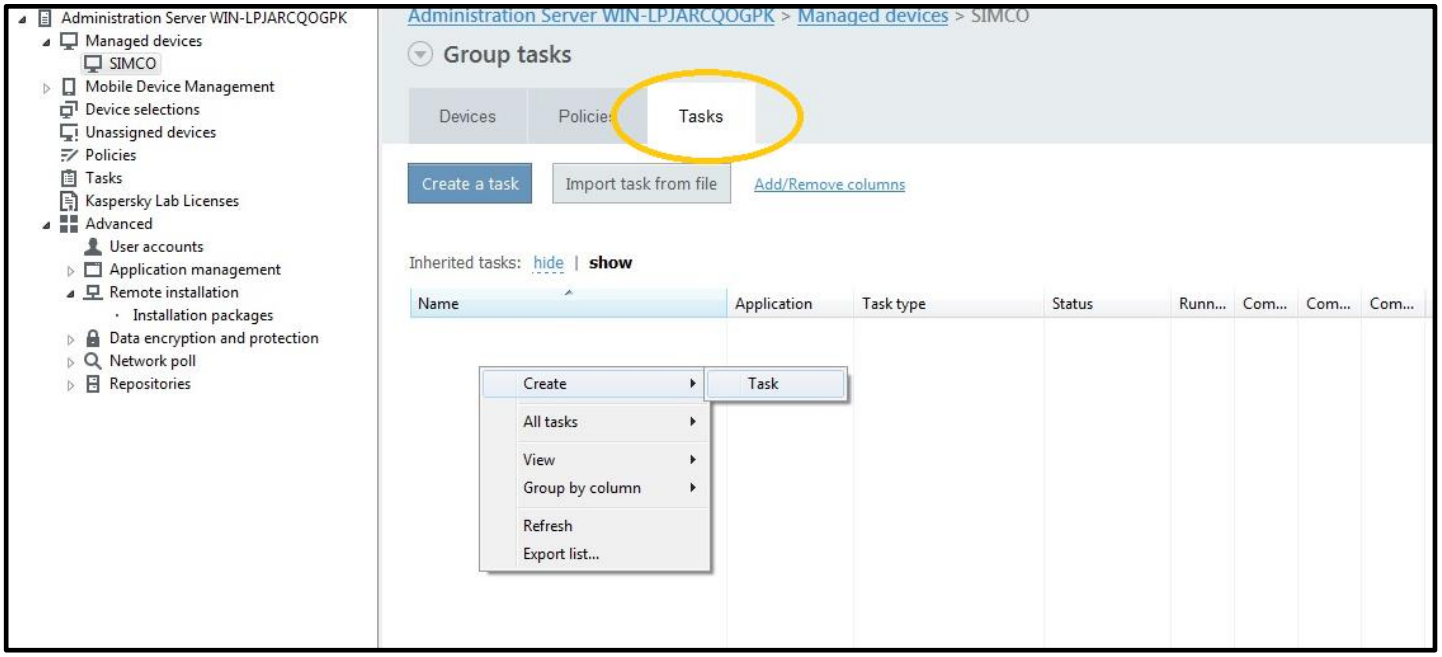


10. In the main window, press the **Start** button again and wait until necessary updates are downloaded. It may take up 20-25 minutes. The size of a regular update package may vary from 20 MB to 600 MB.

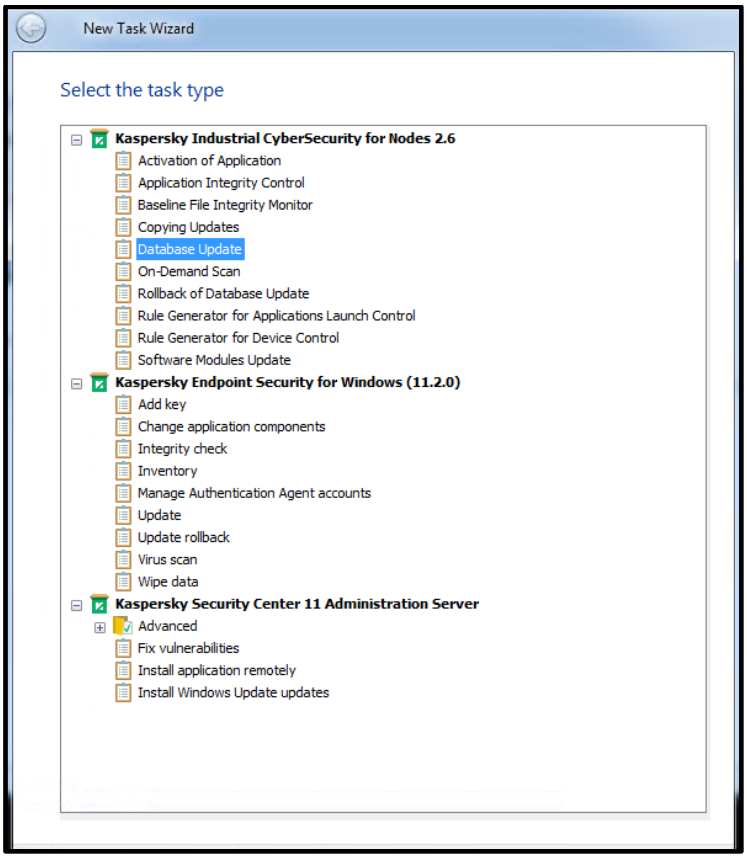


11. When the update process is completed, click **Exit**.

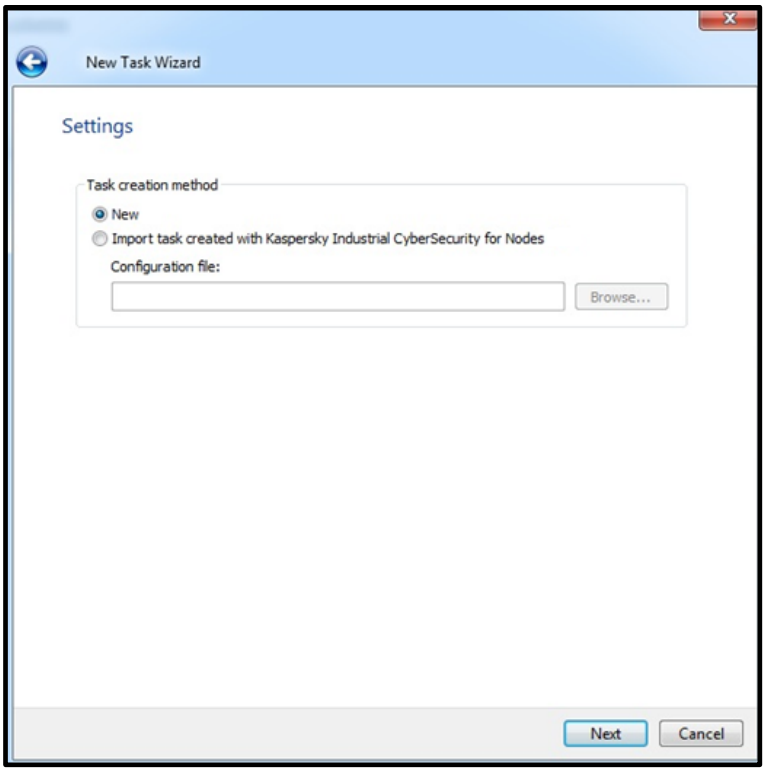
12. Now go back to the **KSC Administration Console**. Go to our managed device (in our case, **SIMCO**); switch to the **Task** tab; right-click on any spare area of the **Tasks** list; in the context menu choose **Create->Task**.



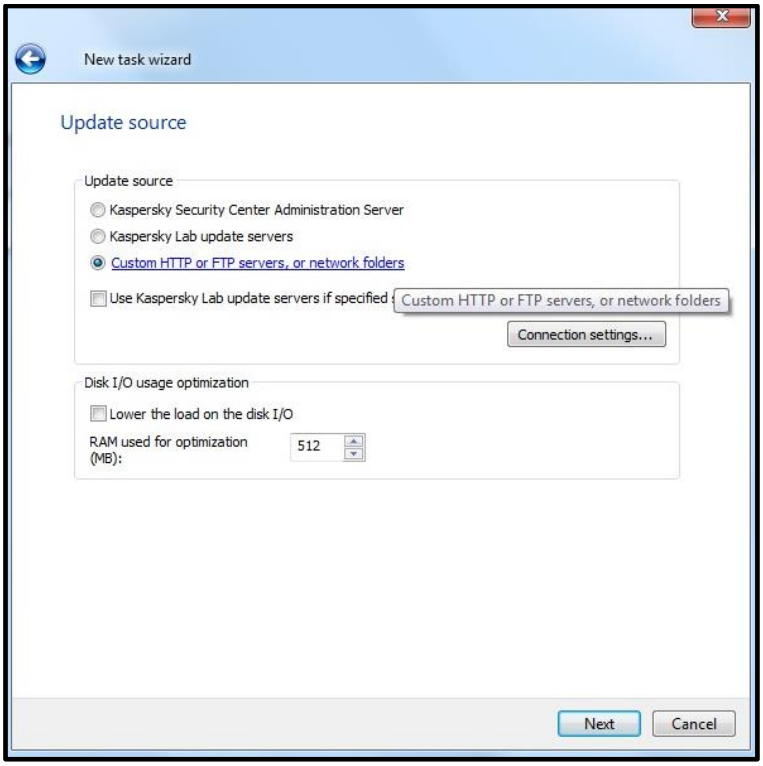
13. In the **Select the task type** window, select **Kaspersky Industrial CyberSecurity for Nodes 2.6->Database Update** and press **Next >**.



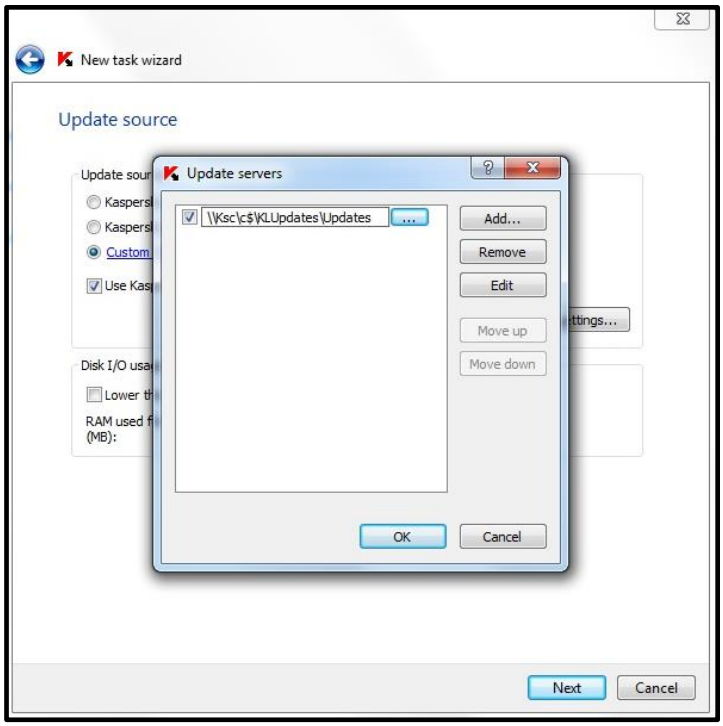
14. Leave the **Task creation method** as **New** and click **Next.**



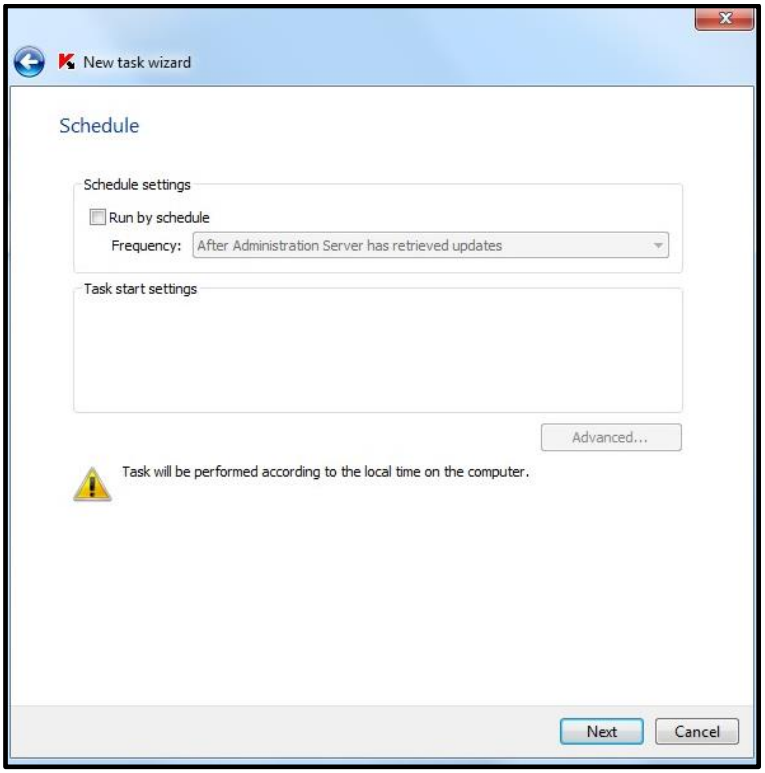
15. In the **Update source** window, check **Custom HTTP or FTP, or network folders** and click the corresponding hyperlink.



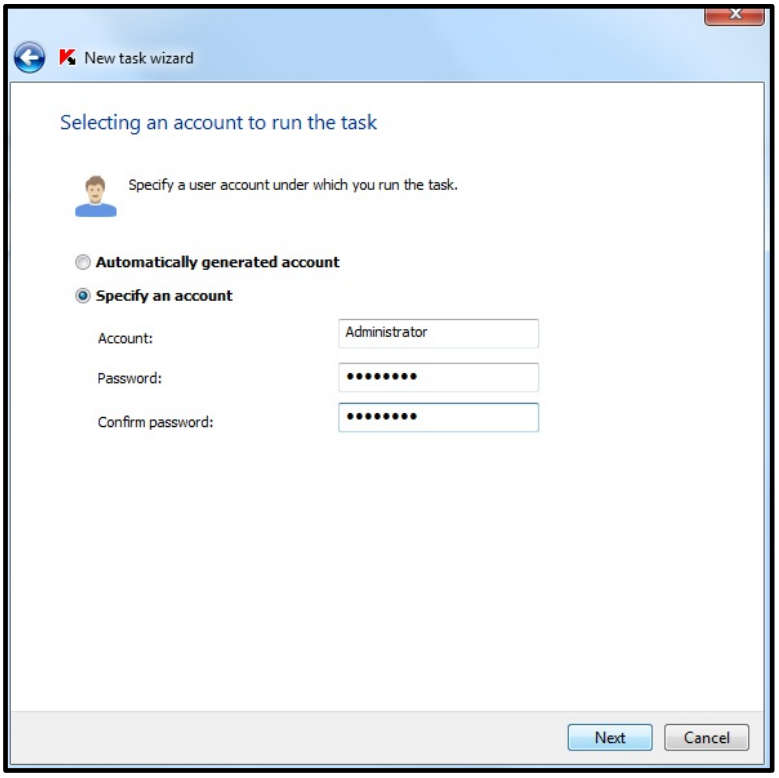
16. In the window that pops up, specify the network path \\KSC\C$\KLUpdates\Updates\ as an update source. Please note, that \\KSC is a network host name of our intermediary file storage. Click **OK** to close the **Update servers** popup window. Click **Next** to move on to the next window of the **New task wizard**.



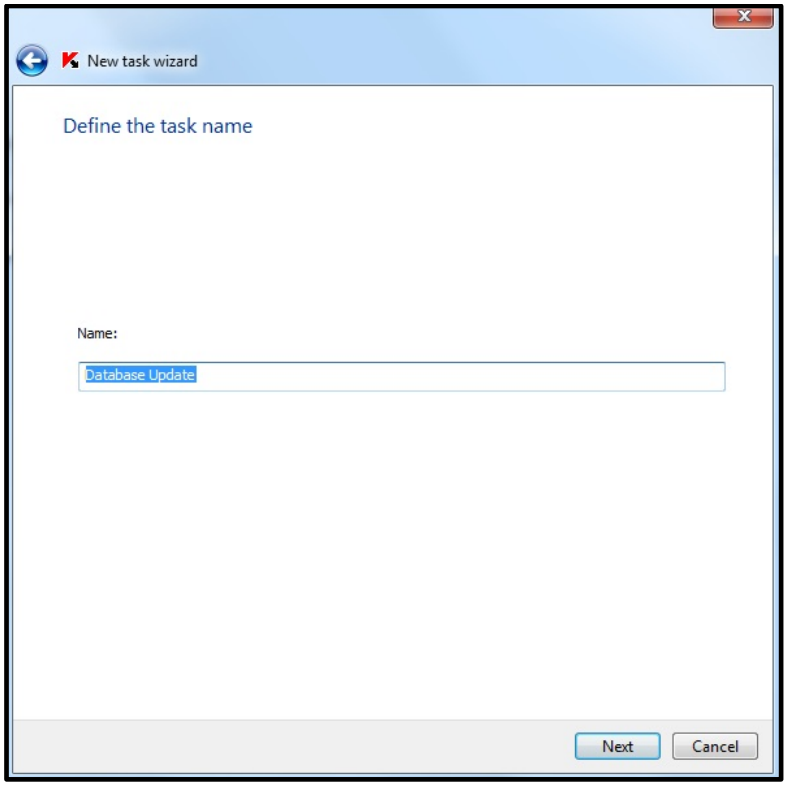
17. Simply click **Next** in the **Schedule** window.



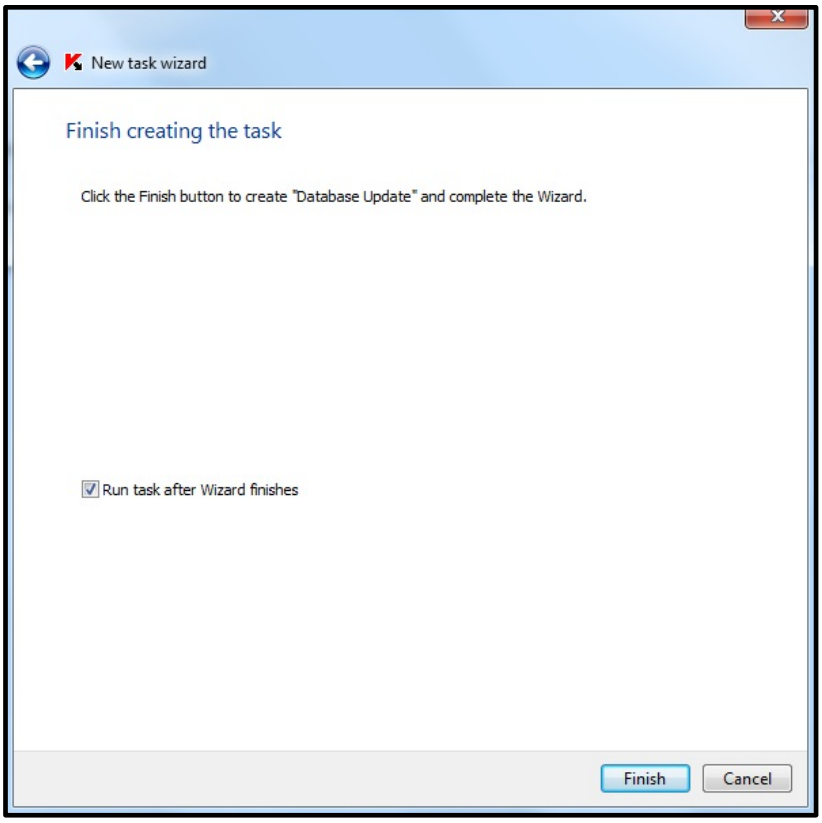
18. In the **Selecting an account to run the task** window, specify the administrator's account that is authorized to access \\KSC\C$\KLUpdate\Updates\ from the network.



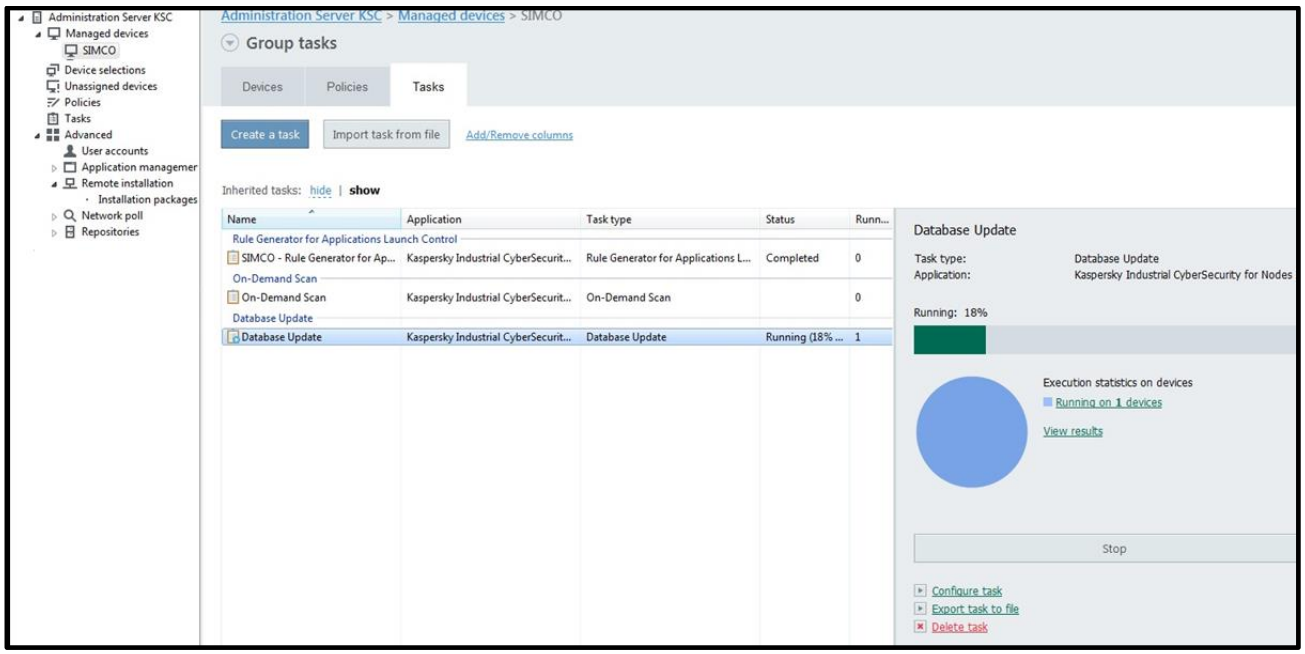
19. Give a meaningful name to the task. Click **Next**.



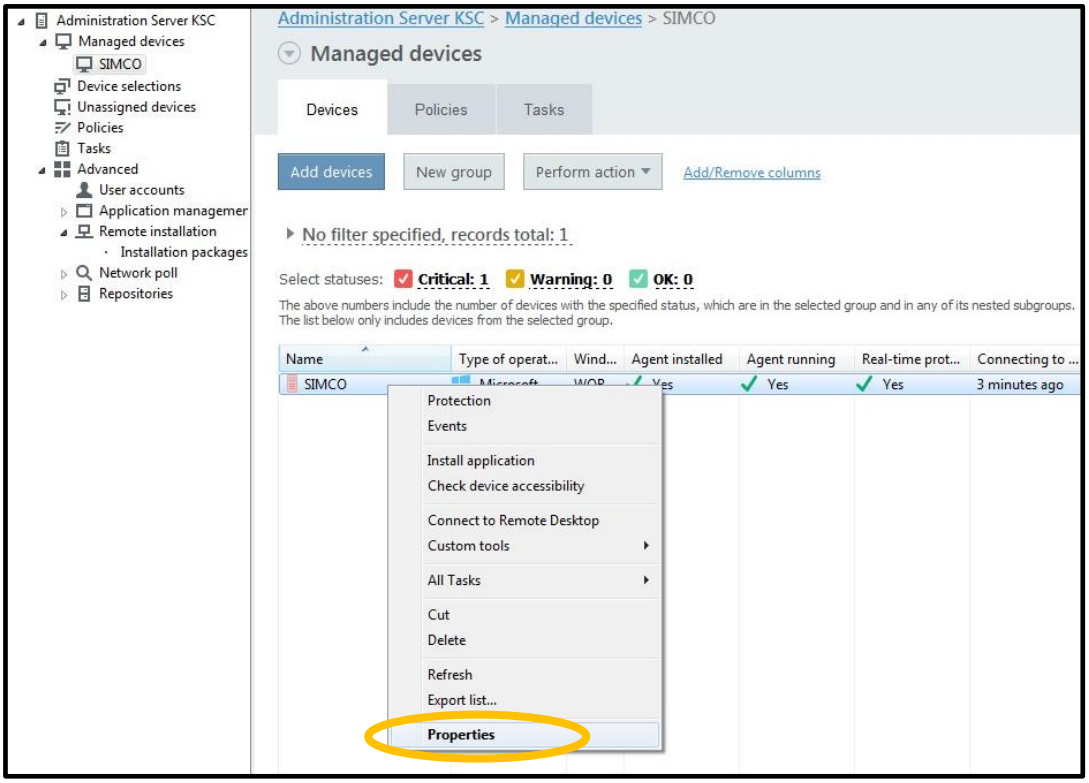
20. In the **Finish creating the task** window, check **Run task after Wizard finishes** and click F**inish**.

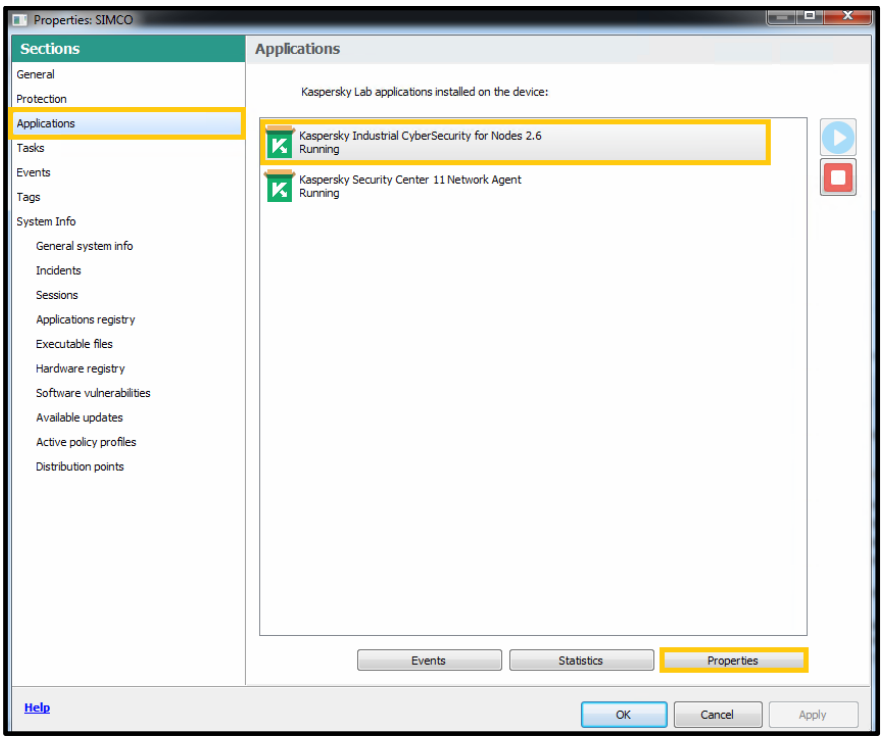


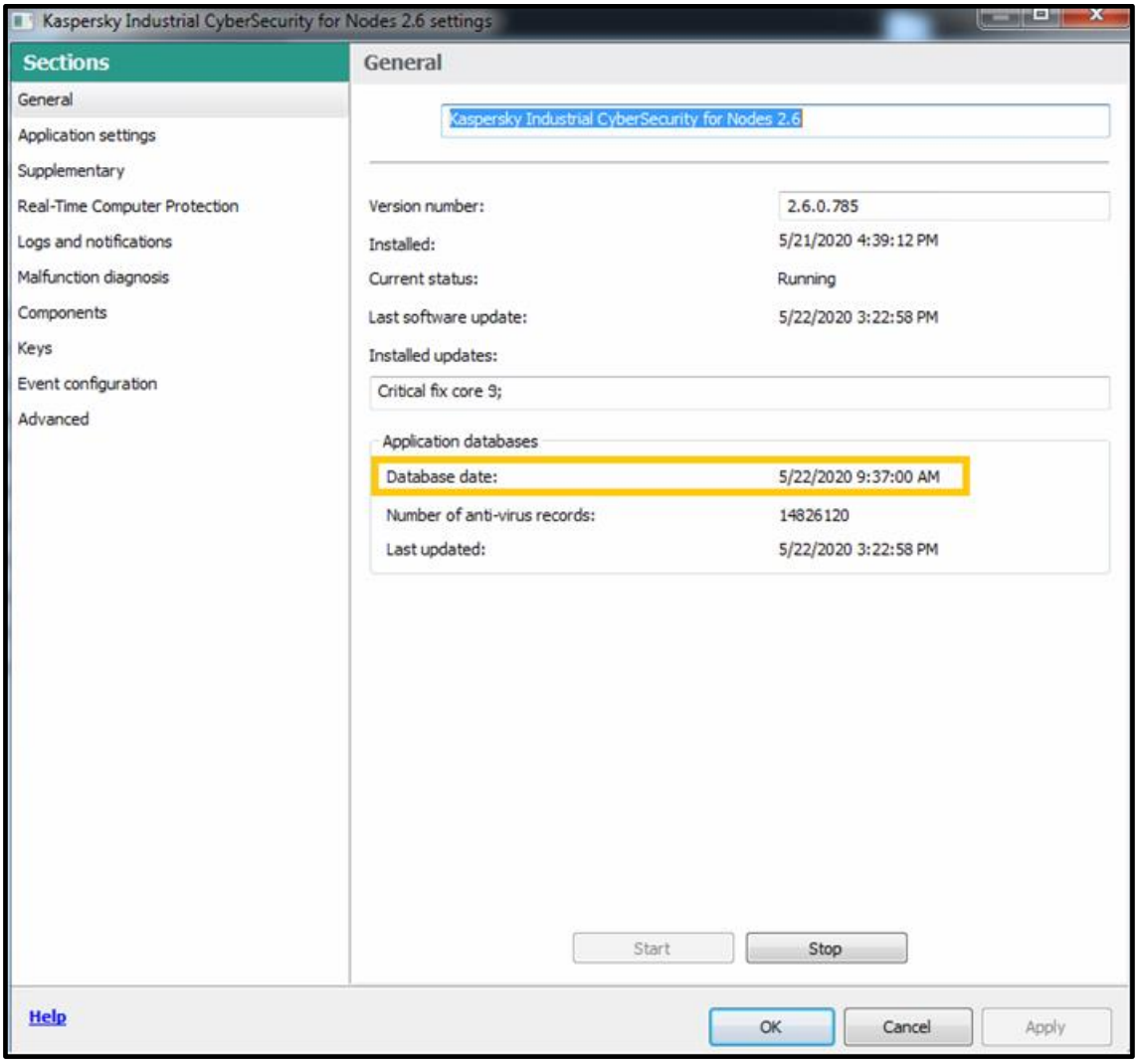
21. If you go to the group task list and select the just created task, you will see its execution progress displayed in the right-hand pane. Wait until the **Database Update** task is completed.



22. In order to make sure that our **KICS for Nodes** host (in our case, **SIMCO**) has received updated AV databases, switch to the **Devices** tab. Then right-click on the device and in the context menu select **Properties**. In the **Properties** window go to **Applications**; select **Kaspersky Industrial CyberSecurity for Nodes 2.6** and press the **Properties** button. In the popup window, refer to the **Database date**.







Alternatively, you can obtain detailed information on the current release of antivirus databases by going to **Administration Server->Reports** tab and double-clicking **Database Usage Report**.

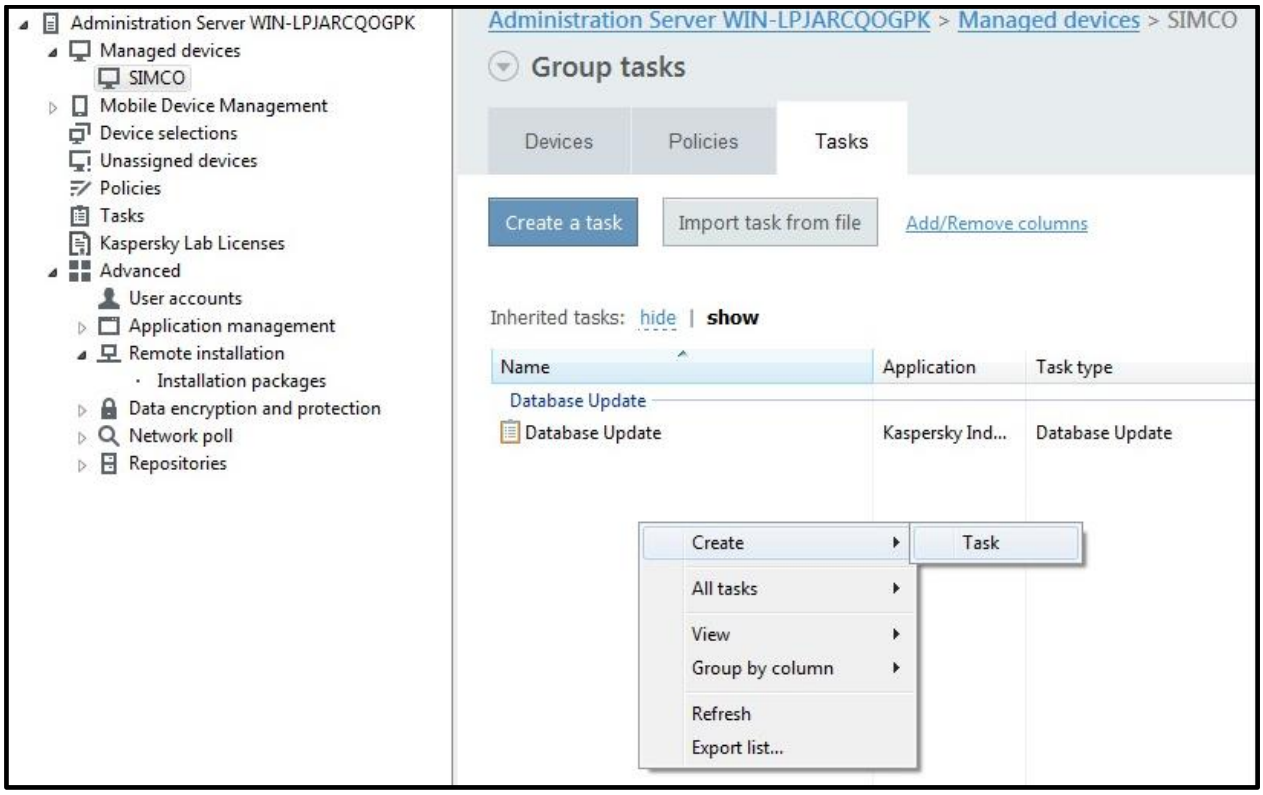
Performing On-Demand Scanning on target hosts

Once we the antivirus databases are up to date, it is highly recommended to configure and start the **On-Demand scan** task on the **SIMCO** host. This essential step aims to ensure that the target host will be free of any malicious software and that no malicious executables will later appear on the **Application Launch Control** white list.

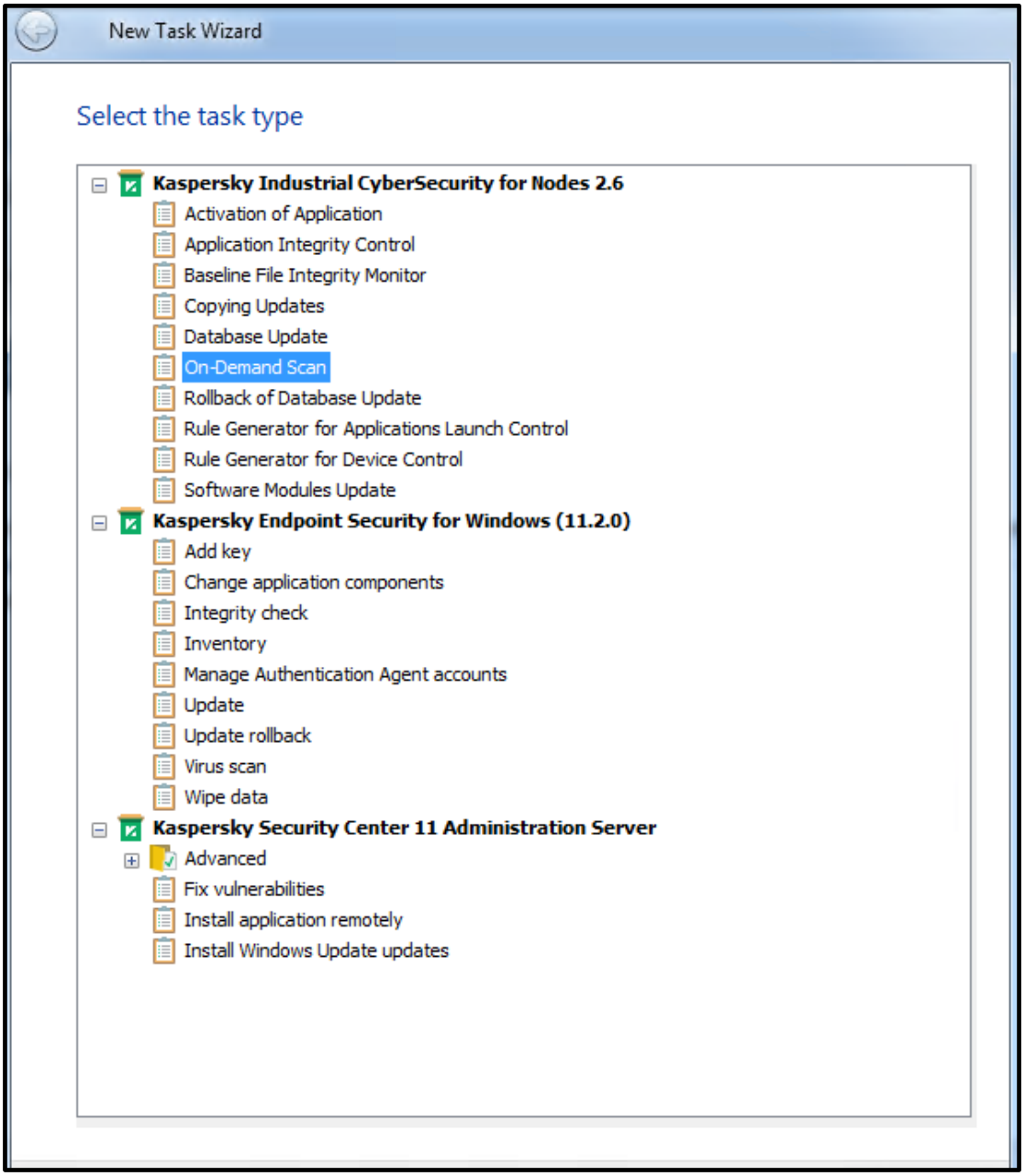
Apparently, the **On-Demand scan** requires some additional processing resources and may slightly deteriorate computer performance. That is why we recommend that you start this task only in the manual mode in order to be able to supervise its execution.

Please perform the following steps to configure the scanner:

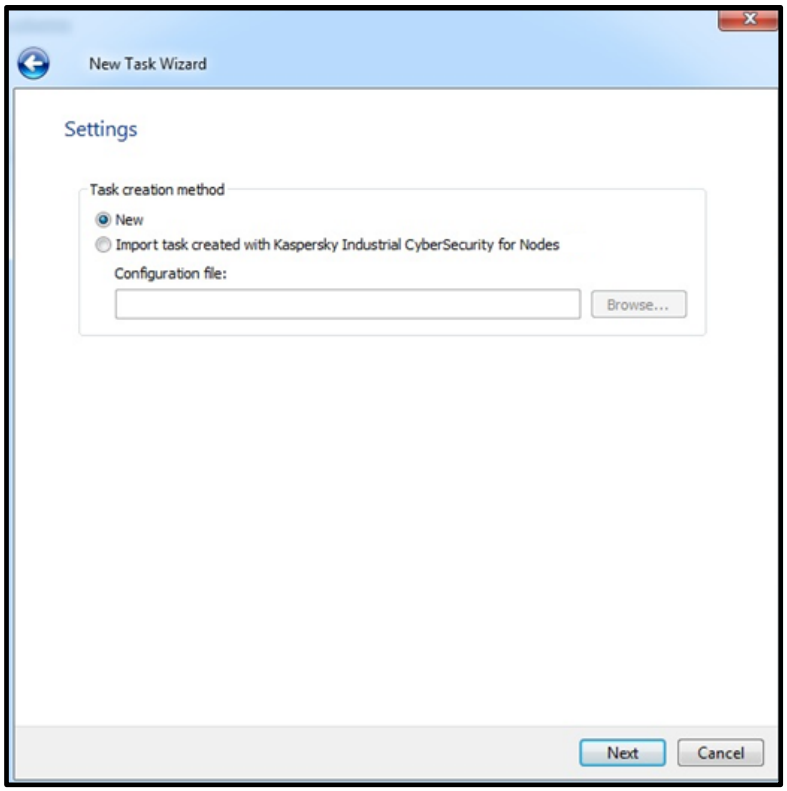
1. Go to the **SIMCO** group and switch to the **Tasks** tab. Using the context menu, start creating a new task as was shown earlier.



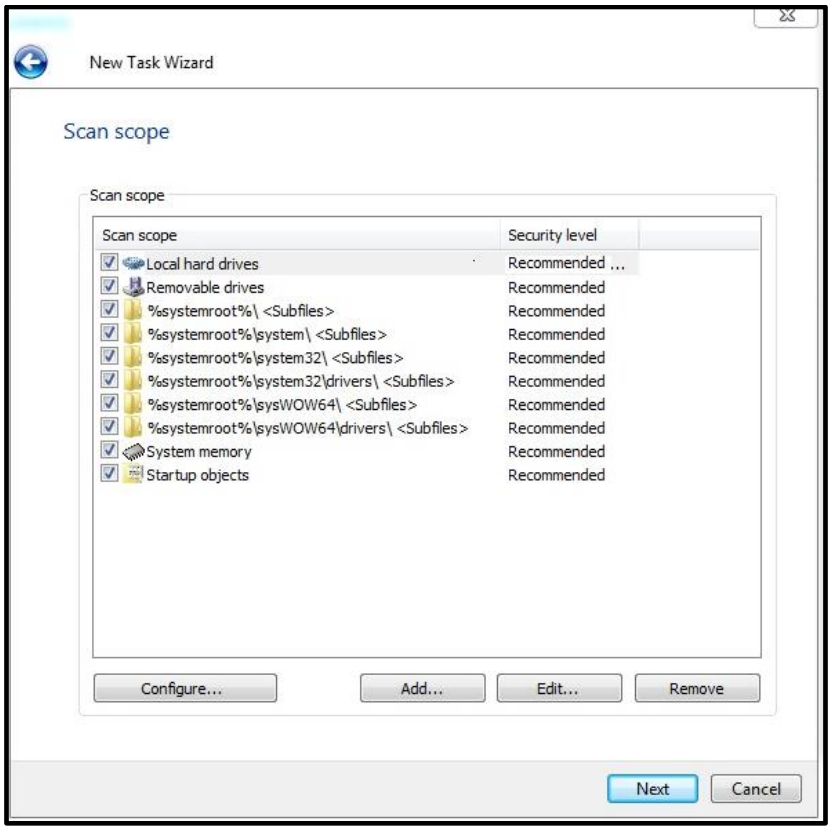
2. In the **New task wizard** window, select **Kaspersky Industrial CyberSecurity for Nodes 2.6 -> On-Demand Scan.** Click **Next**.



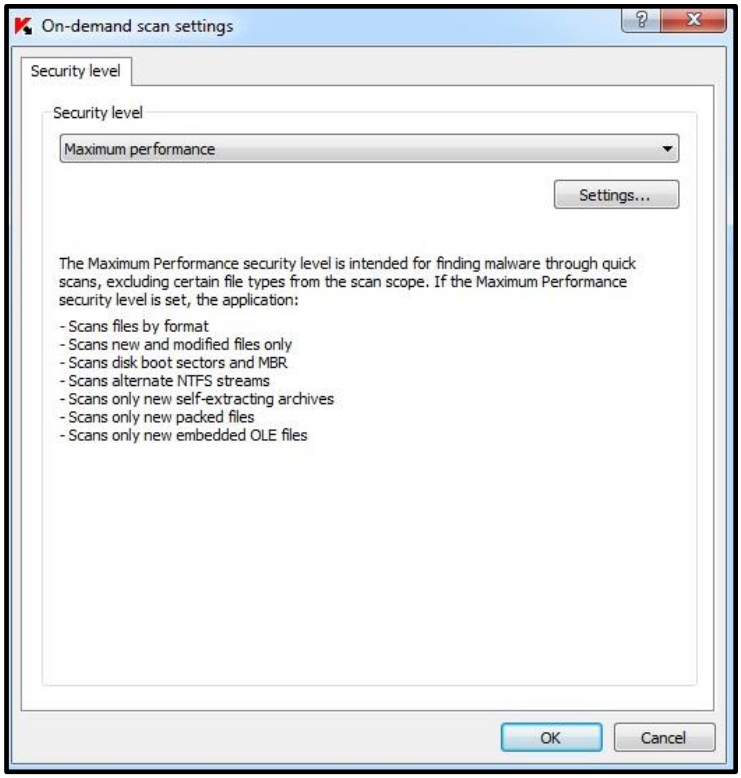
3. Leave the **Task creation method** as **New** and click **Next.**



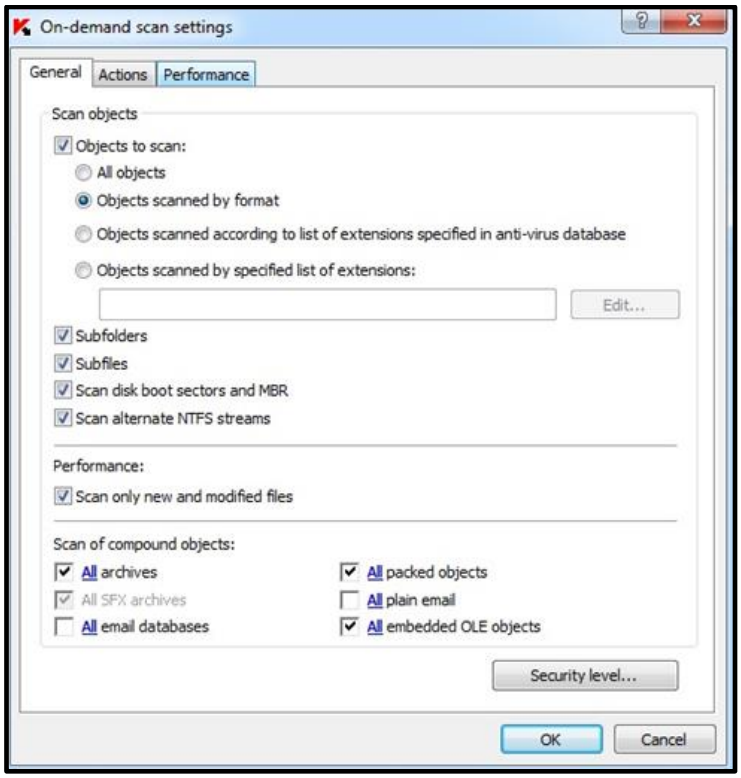
4. Select the **Local hard drives** item as shown below and double-click it.



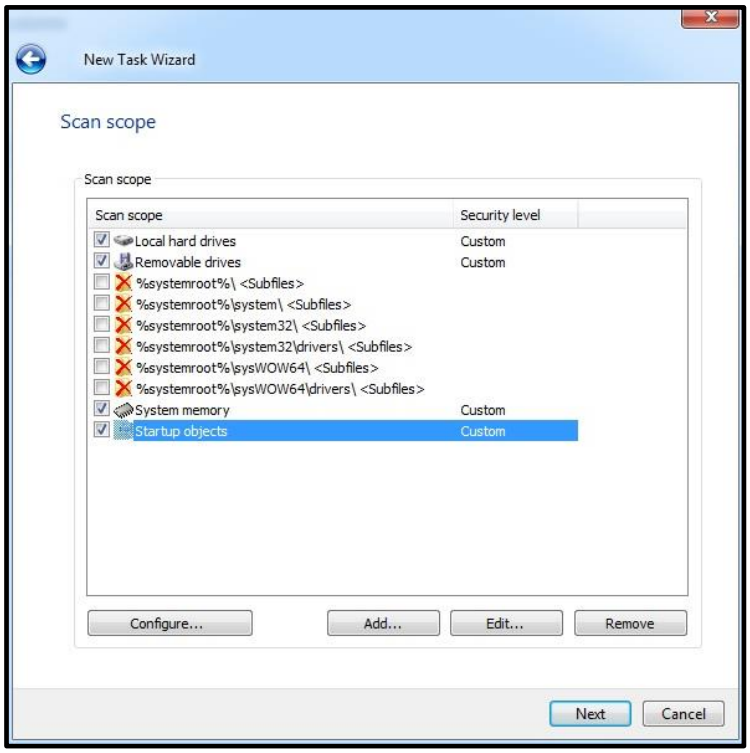
5. In the next window that pops up, set **Security level** to **Maximum performance** and click the **Settings…** button.



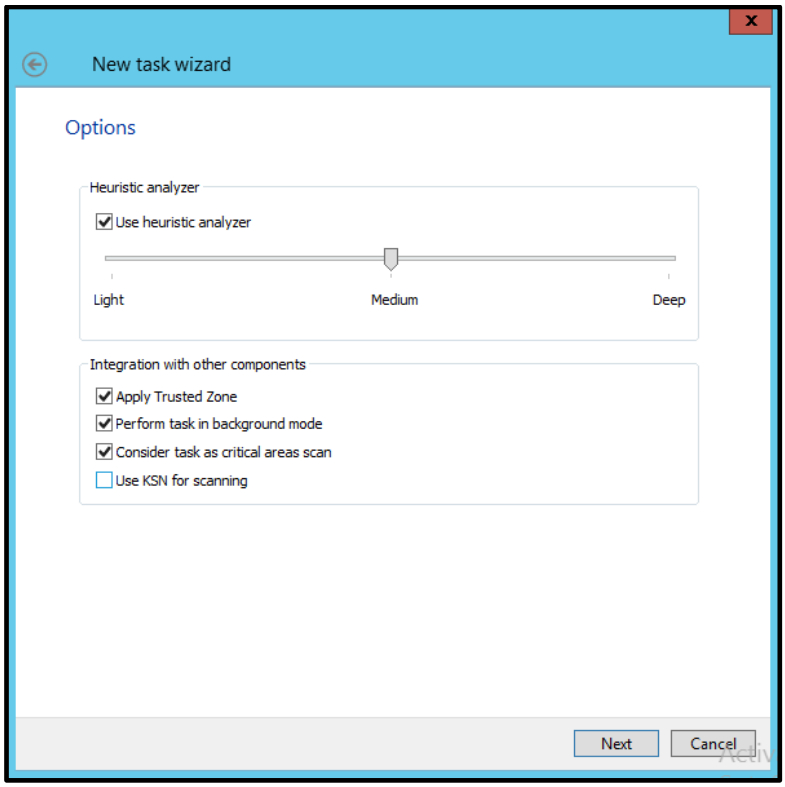
6. In the **On-demand scan settings** window, specify the settings as shown below. Click **OK** when done.



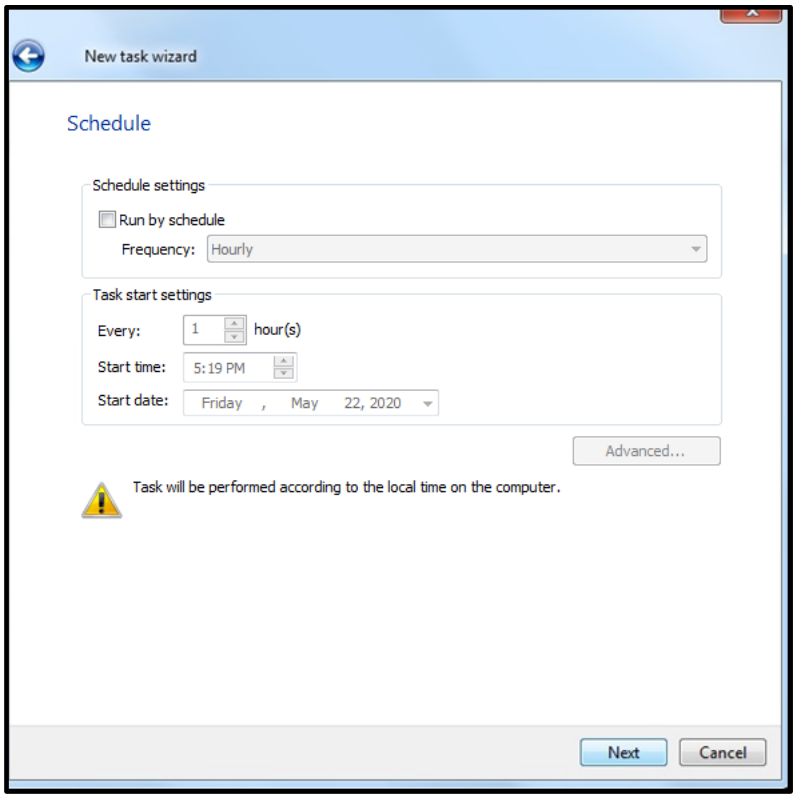
7. Repeat steps 4-6 for the **Removable drives**, **System memory** and **Startup objects** item included in the **Scan scope** by default.
8. Continue to edit the **Scan Scope** by unchecking every **%system root%\...** item. Click **Next**.



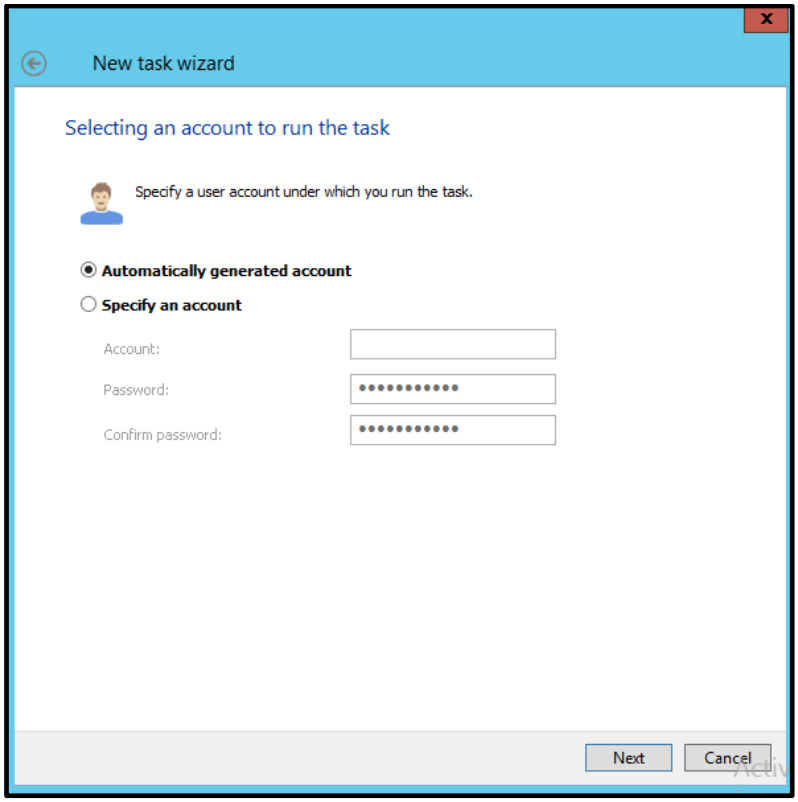
9. In the **Options** window, specify the settings as shown below. Click **Next**.



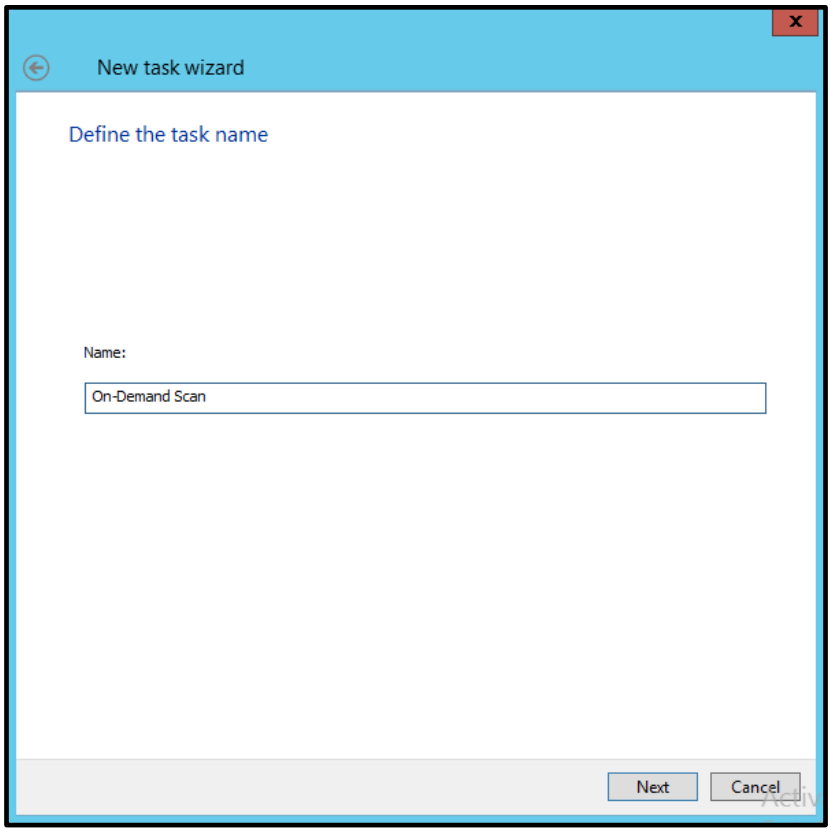
10. In the **Schedule** window, specify the settings as shown below. Click **Next**.



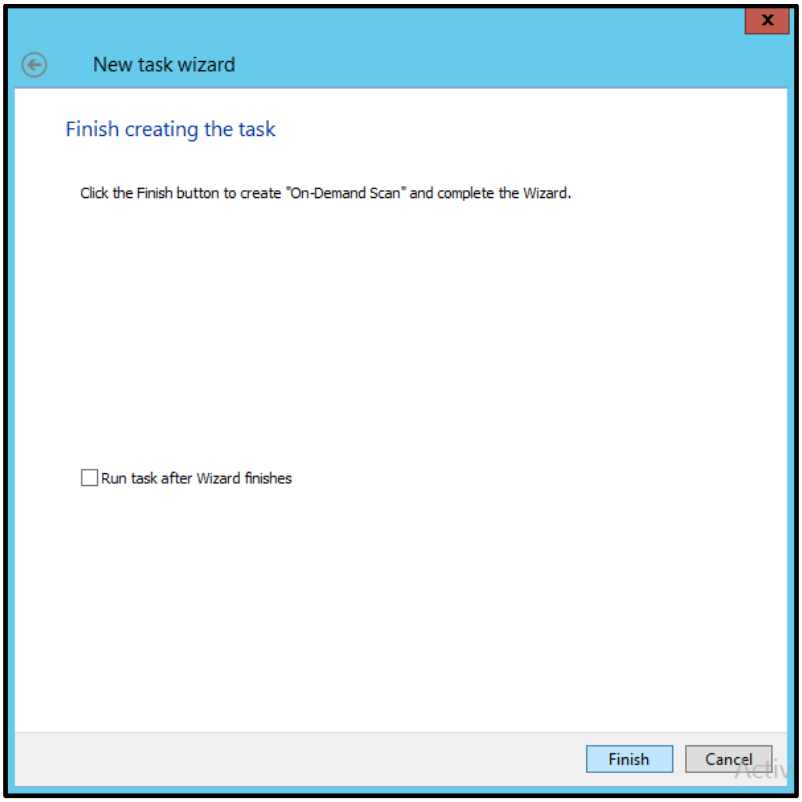
11. In the **Selecting an account to run the task** window, leave the default settings and click **Next**.



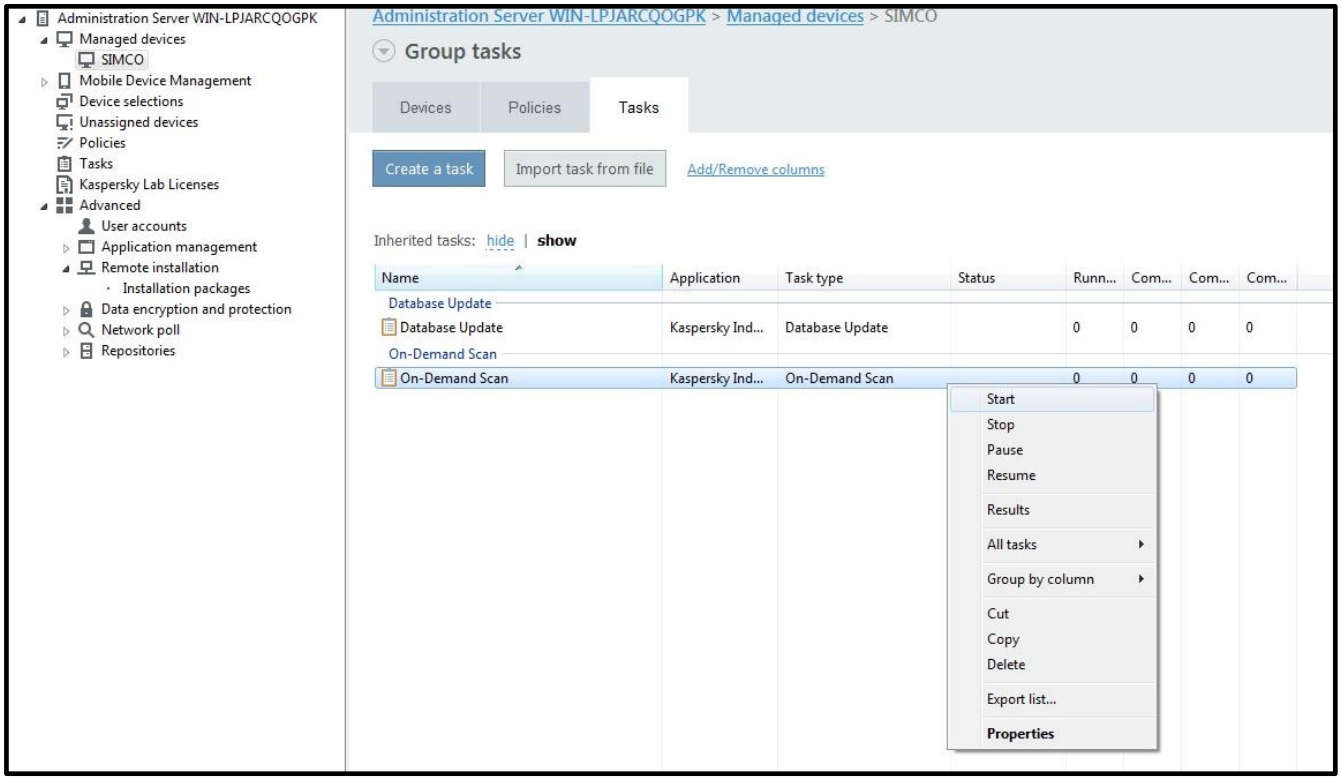
12. Give some meaningful name to the task and click **Next**.



13. In the **Finish creating the task** window, click **Finish**. This will create the task but will not launch it.



14. Using the context menu, start the **On-Demand Scan** task manually.



15. Wait patiently until the task is completed. It may take up to 3 hours depending on the target PC performance and its software composition.
16. When the task is finished, you can view its results by going to the **Administration Server** node, switching to the **Reports** tab and calling the **Viruses report**. We hope that this report will not contain any malware alerts.

kaspersky

Execution of the Generate Rules for Application Launch Control task

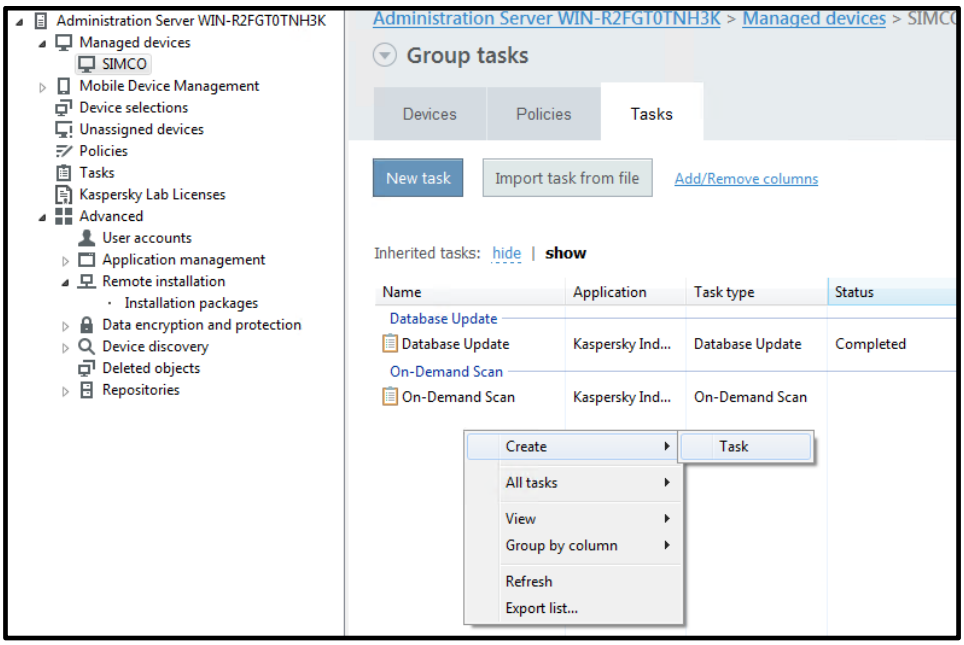
After its activation **Application Launch Control** keeps on watching executable files launches by referring to the predefined list of legitimate applications (to the, so called, white list). The module can also process DLL calls as well as script runs. **Application Launch Control** can function in either of the two modes – **Statistics only** and **Apply Default Deny**.

- While running in the **Statistics only** mode, the module does not actually block executable files, which are not on the white list. It only alerts when an authorized file is launched.
- While running in the **Apply Default Deny** mode, the module blocks execution of those files, which are not on the white list.

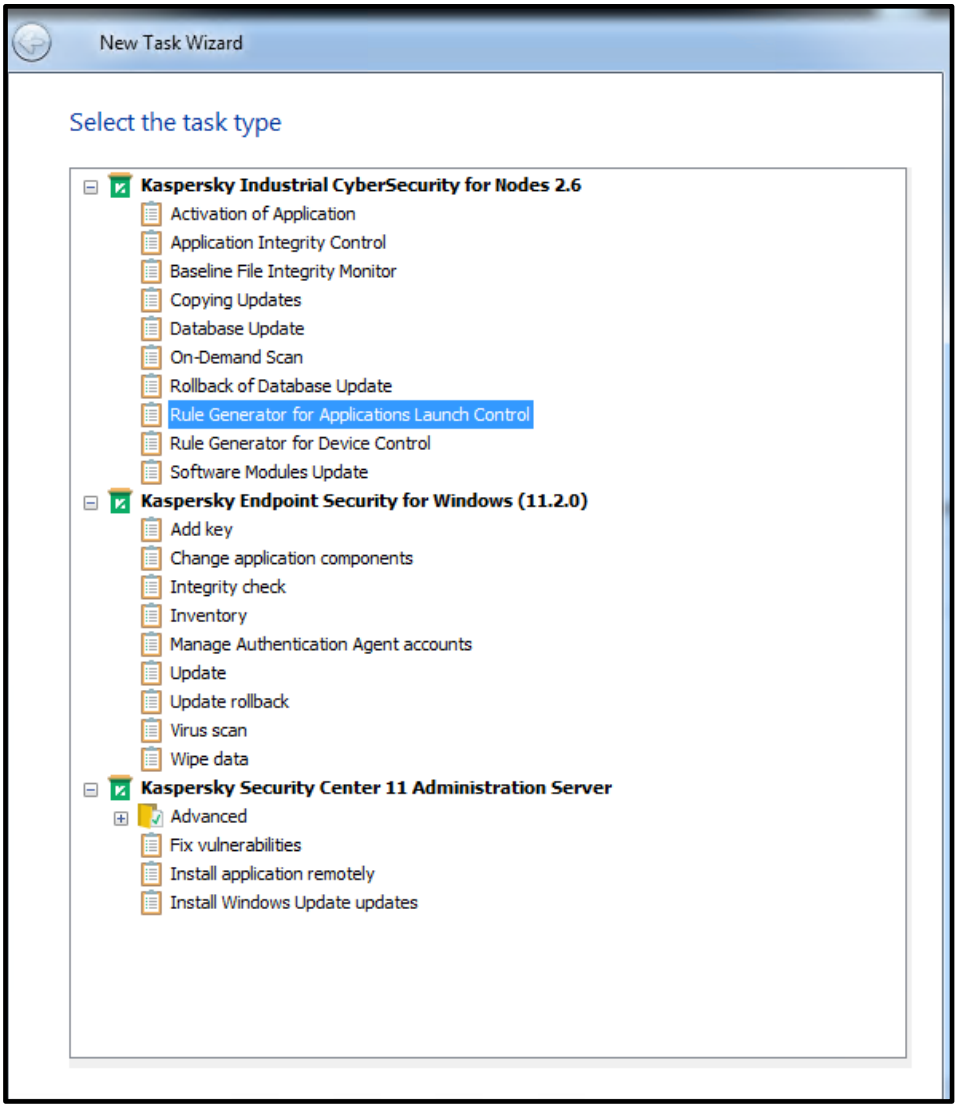
Please note, that the **Statistic only** mode is the most appropriate option for industrial control systems as it provides an optimal balance between preserving DCS performance/robustness, on the one hand, and attaining to the sufficient cyber protection level, on the other.

Please go through the following steps in order to have the **Application Launch Control** white list automatically generated**.**

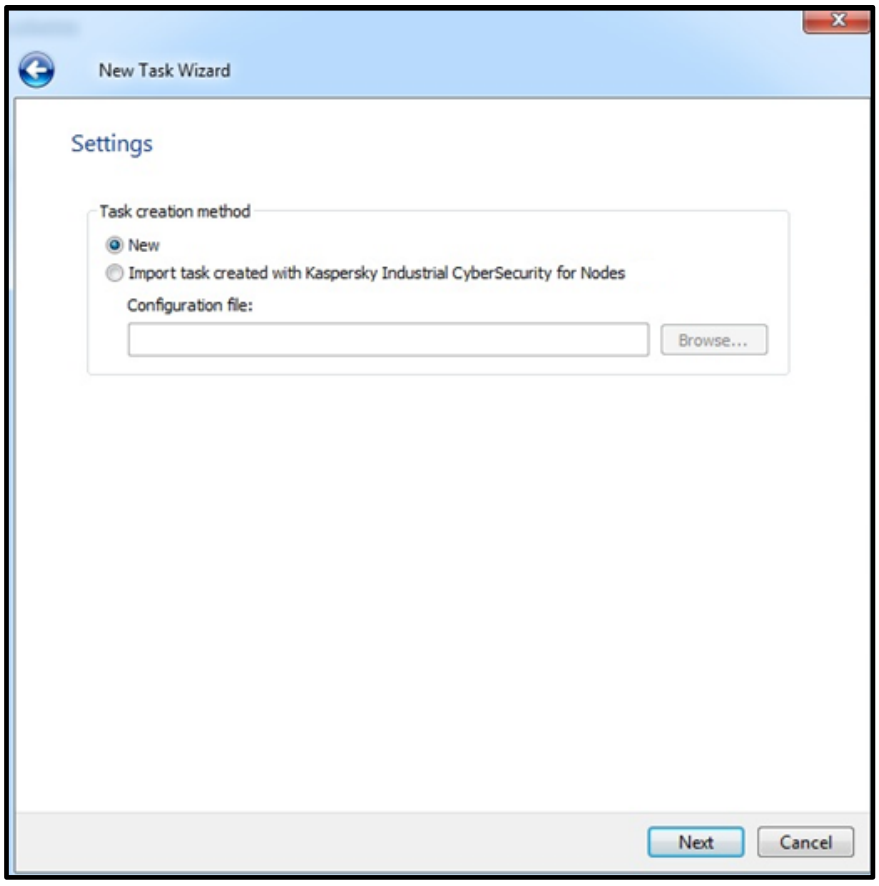
1. Go to our managed devices group (**SIMCO**, in our case) and enter the **Tasks** tab. Right-click on the **Tasks** list and in the context menu choose **Create->Task**.



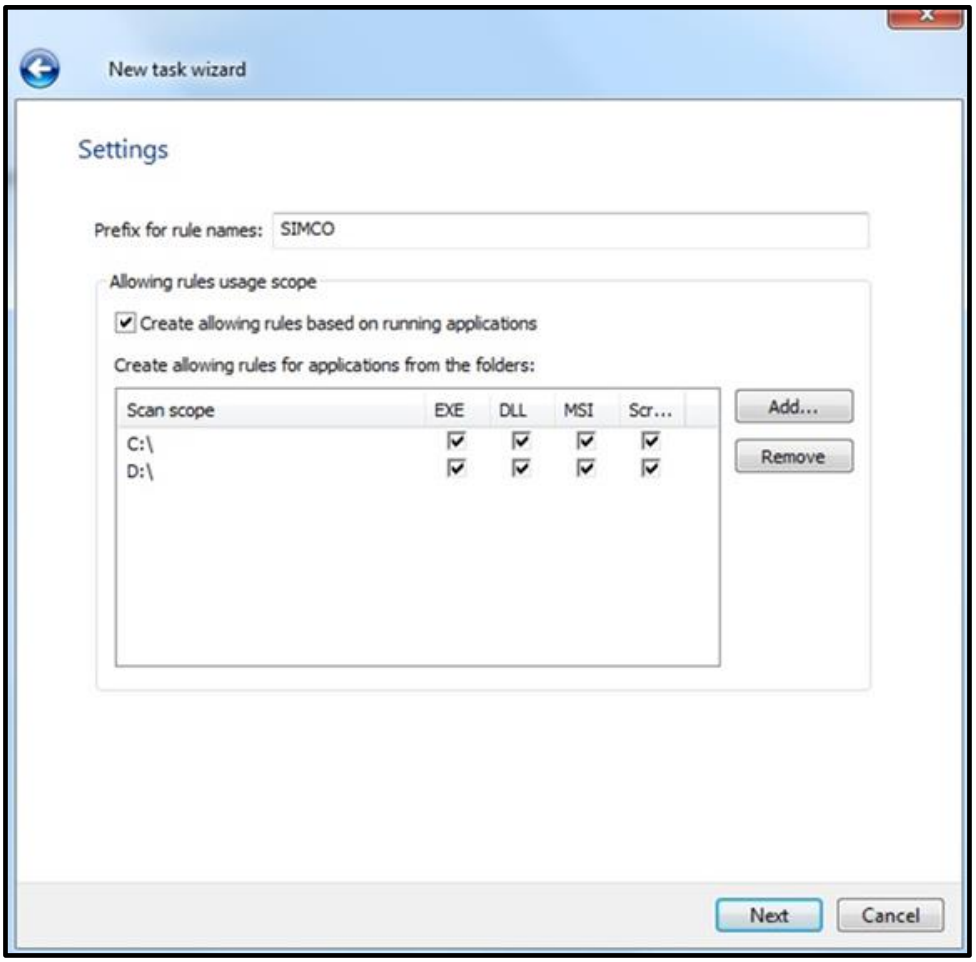
2. In the **Select the task type** window that pops up, select **Rule Generator for Application Launch Control**. Click **Next**.



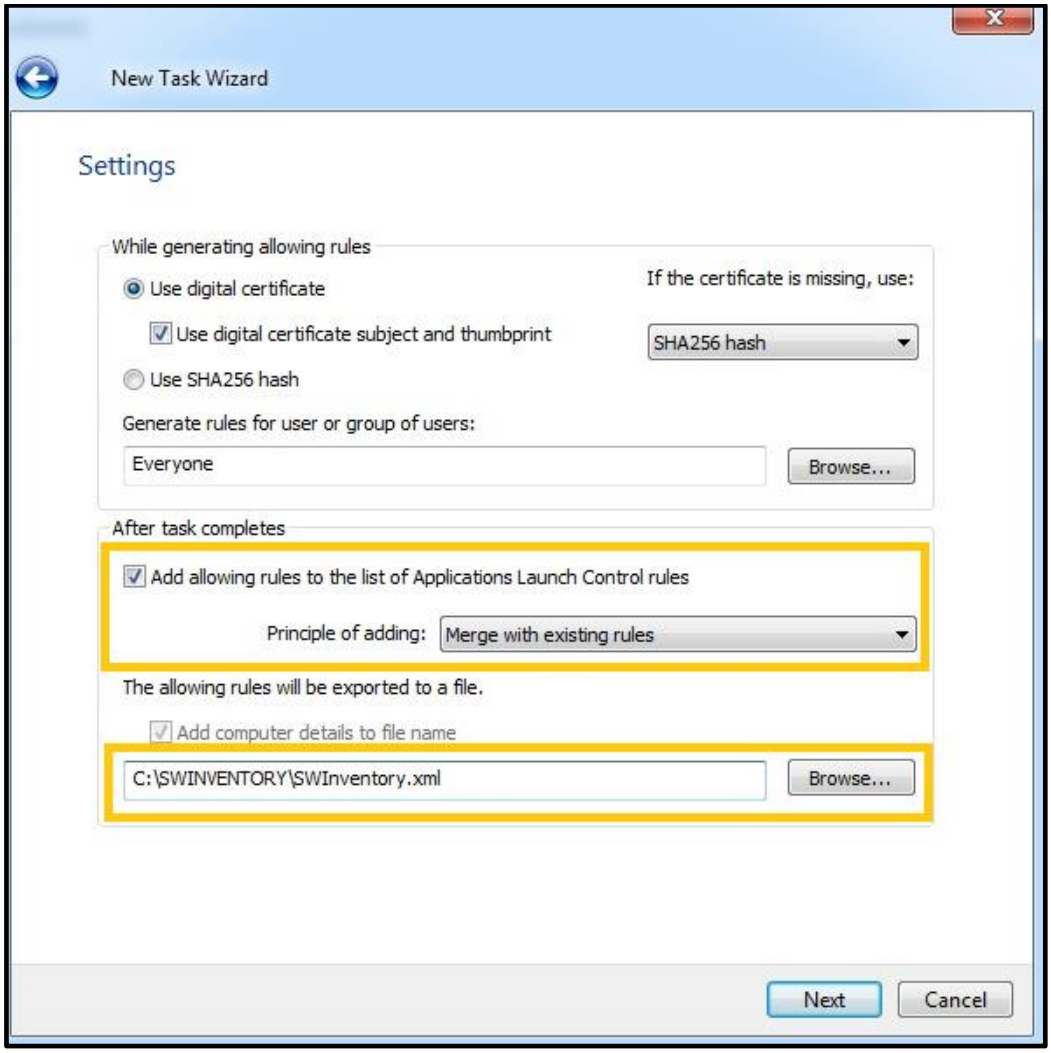
3. Leave the **Task creation method** as **New** and click **Next.**



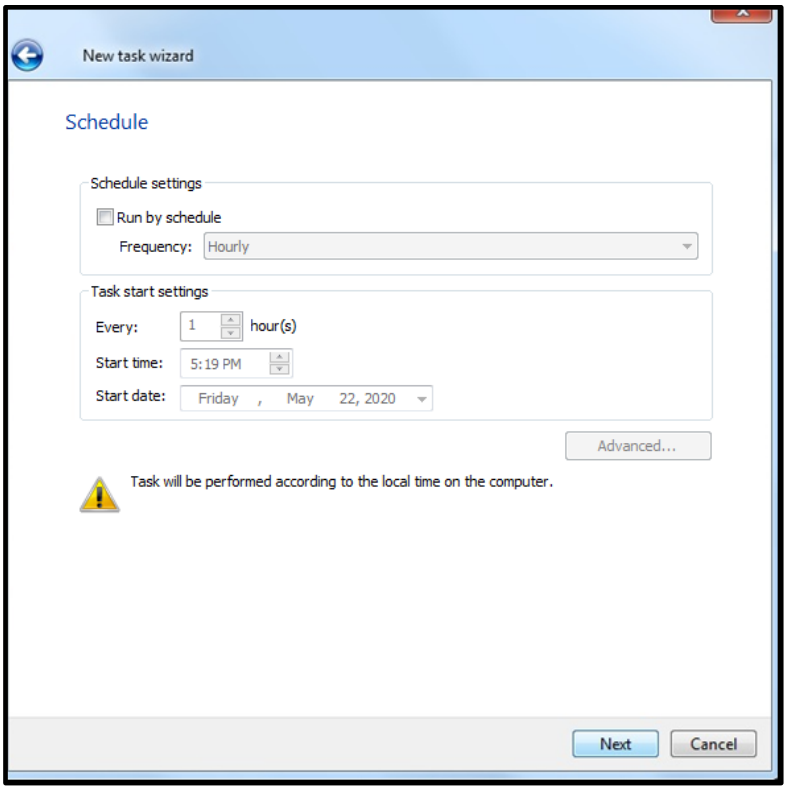
4. In the **Settings** window that follows, specify the settings according to the example shown below. Apparently, our **SIMCO** workstation/server has only two partitions: **C:** and **D:**. When the settings are complete, click **Next**.



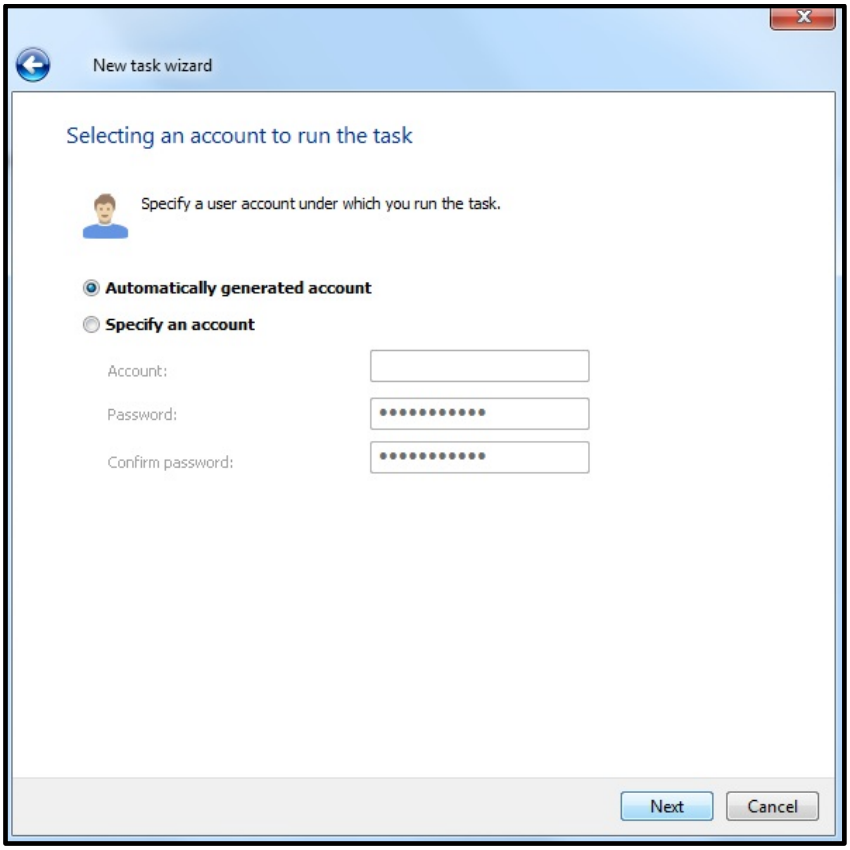
5. In the following window, specify appropriate settings as shown in the example below. In our case, we have previously created the **SWInventory** folder on the **C:** drive of our **SIMCO** station. It is where the automatically generated rule list will be stored to as soon as the task finishes. In practice, you can specify any **existing** folder on a target host. Always select **Use digital certificate** and check **Use digital certificate subject and thumbprint**. Also, remember checking **Add allowing rules to the list of Application Launch Control list**. This option facilitates module configuration so that we will not need to deal with an XML-file import (although this file will still be created). Click **Next**.



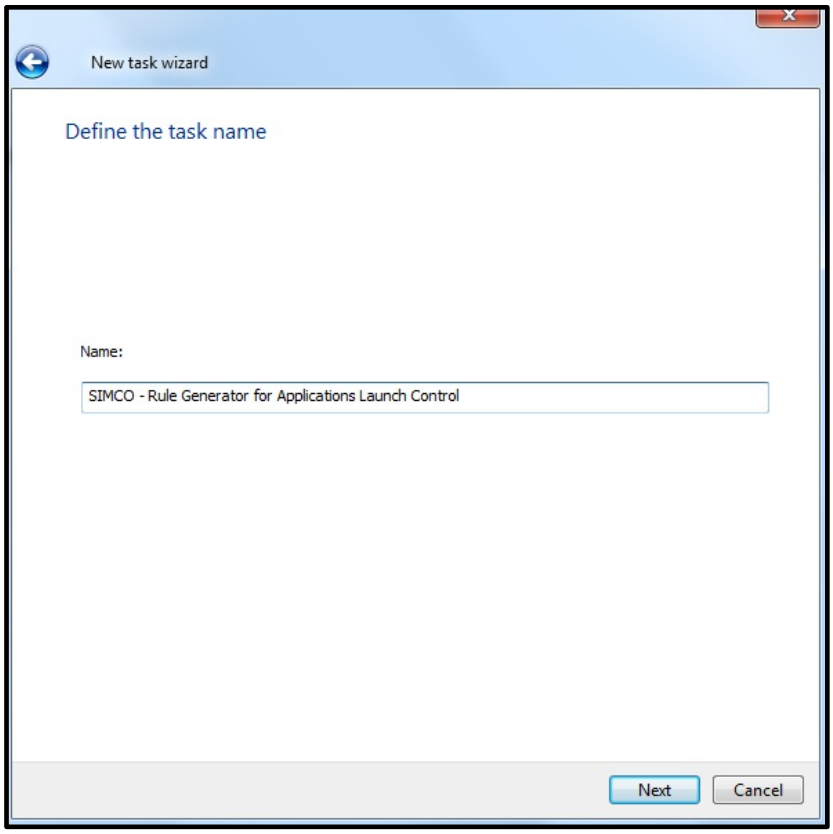
6. In the **Schedule** window, simply click **Next**.



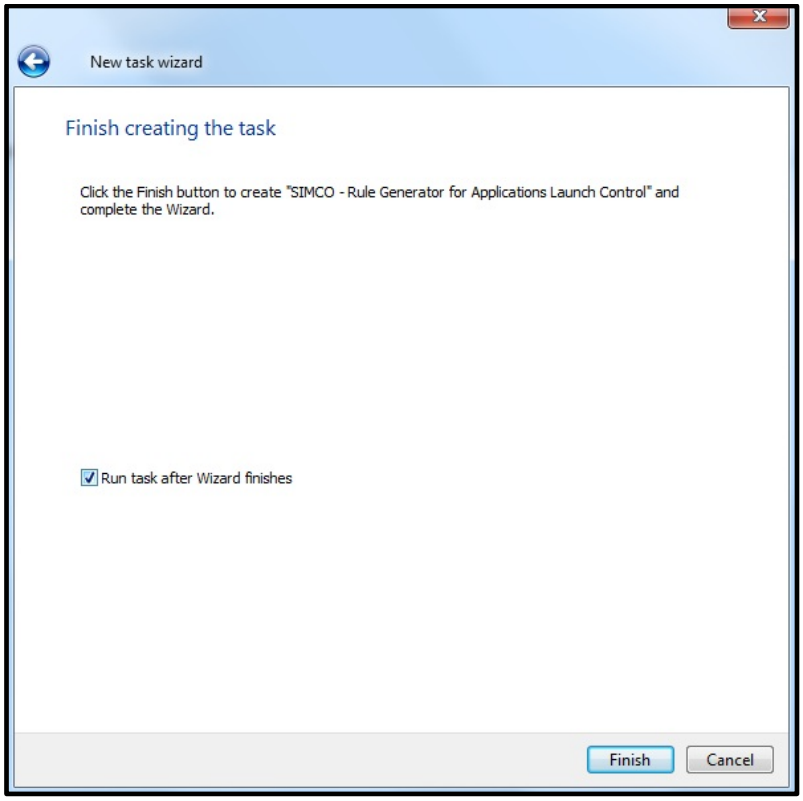
7. In the **Selecting an account to run the task** window, select **Automatically generated account** and click **Next.**



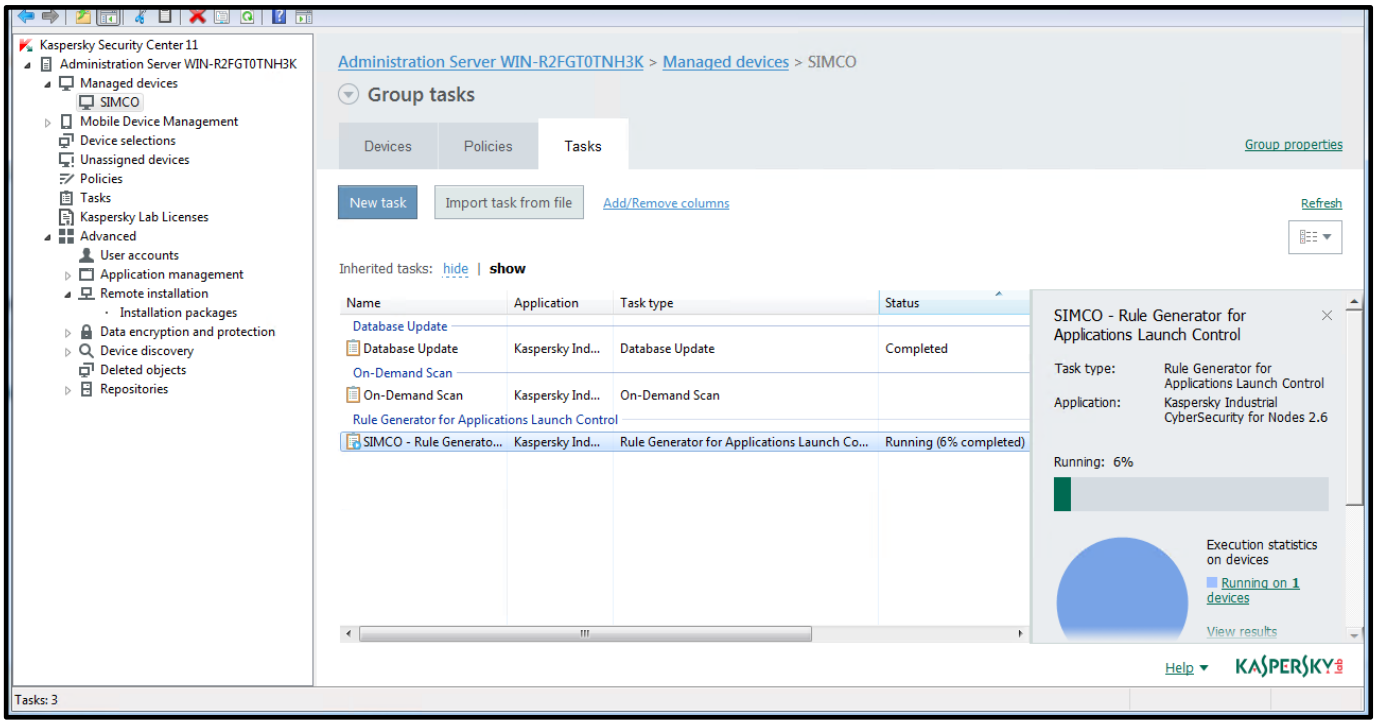
8. In the **Define the task name** window, specify some meaningful and relevant name for the task. Click **Next**.



9. In the **Finish creating the task** window, check **Run task after Wizard finishes** and click **Finish**.



10. We have now created and started the **Rule Generator for Application Launch Control** task. Actually, this task affects every device located in the management devices group (in our case, we have just one device in our group – **SIMCO**). If you select this task, you will be able to track its execution progress displayed in the right-hand pane. **Please note that the task may last for several hours depending on the software composition of the target host and its hardware performance. Please take your time!**



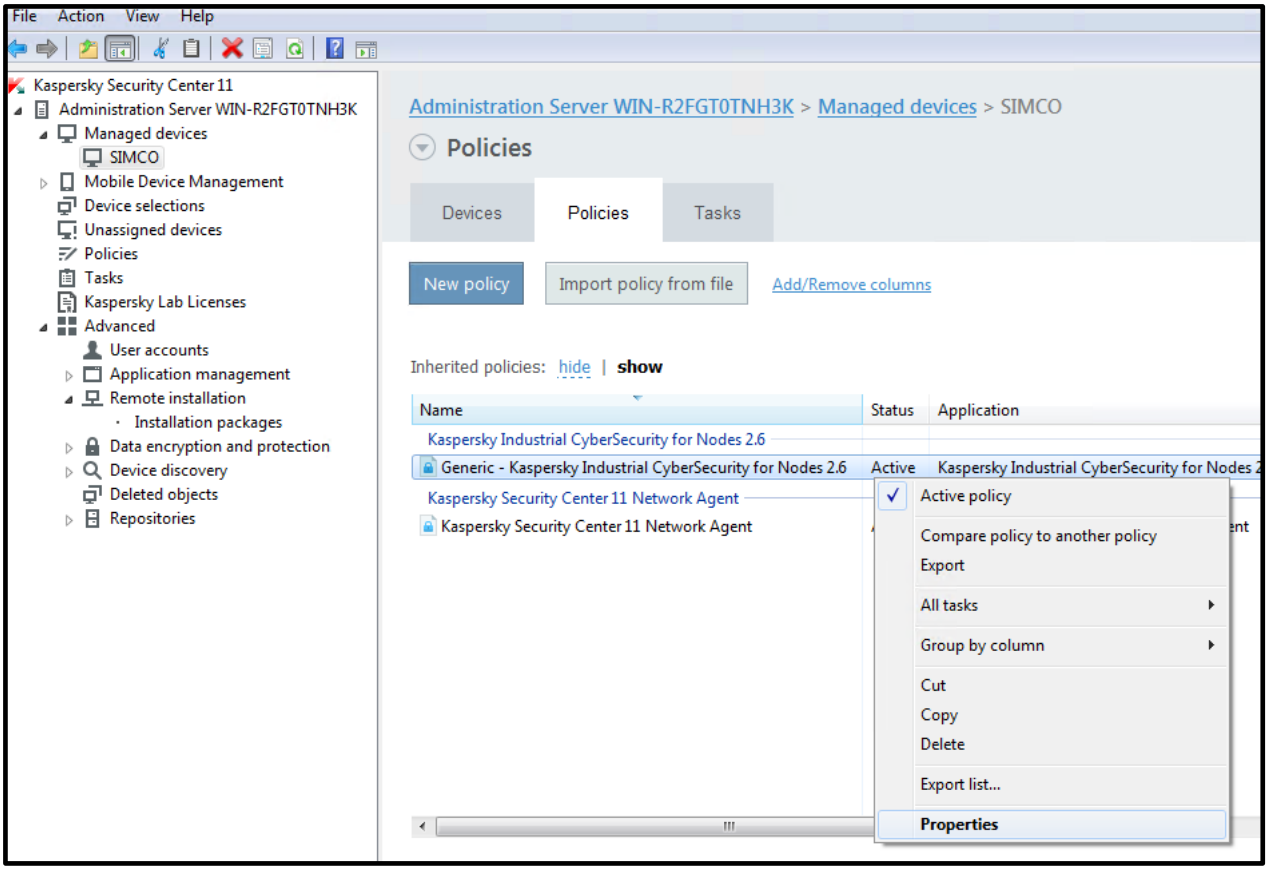
11. After the task is completed, go to the target host and make sure that the rule list (***.XML** file) resides in the export folder you have specified before (in our case, it should be present in **C:\SWInventory**).
12. Using the task context menu, you can start/stop/restart it at any time. You can also edit the properties of the existing task unless the task is running.

Setting up Application Launch Control whitelisting

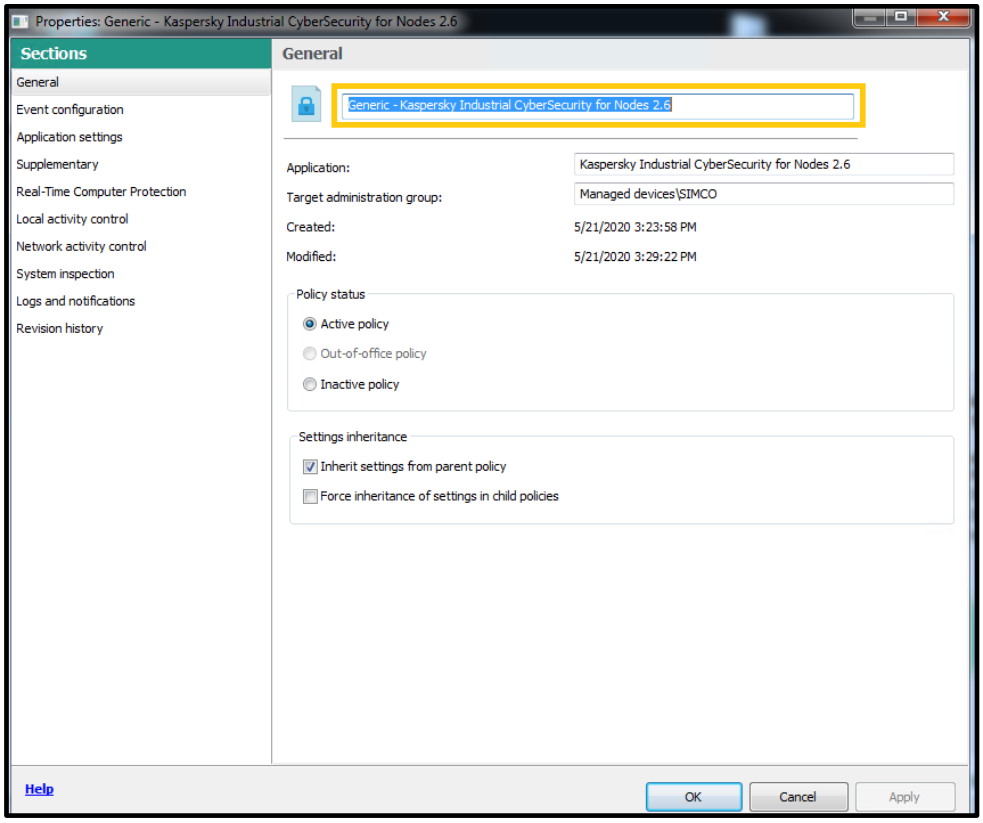
Now we are ready to fine-tune our generic (“backbone”) policy, which we have created and applied to the **SIMCO** host earlier.

Please perform the following steps to set up **Application Launch Control**:

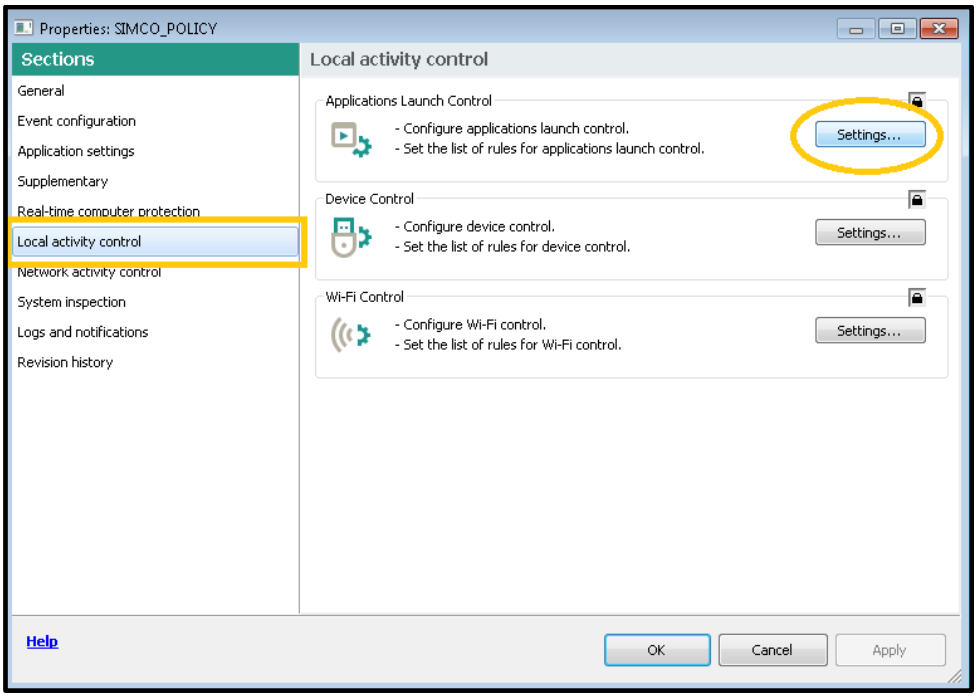
1. Go to the **SIMCO** subgroup and switch to the **Policies** tab.
2. Locate the **Generic – Kaspersky Industrial CyberSecurity for Nodes 2.6** policy, which we have created before, and enter its **Properties**.



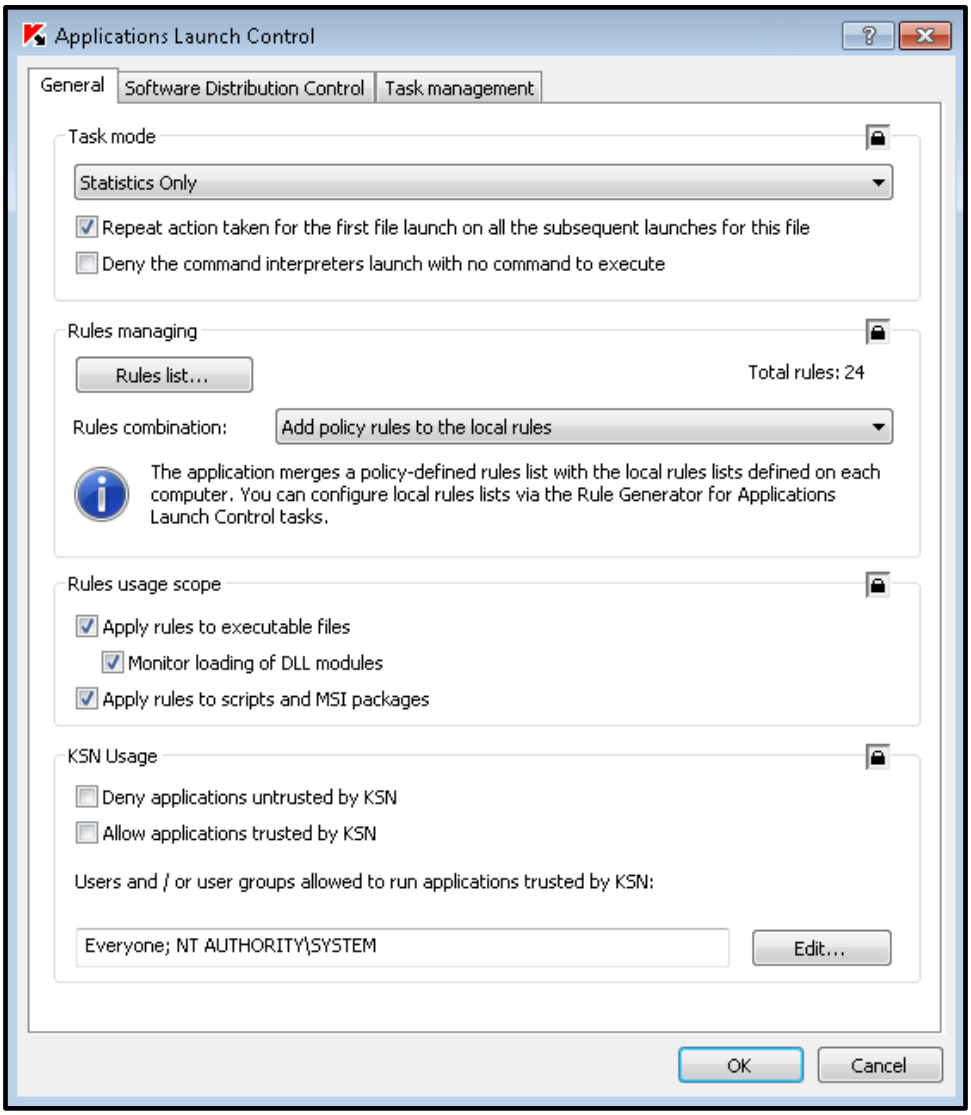
3. In order to avoid confusion, give the policy some more specific and unique name by editing the text field as shown below. In our case, we will rename the policy into **SIMCO_POLICY**. Press **Apply**.



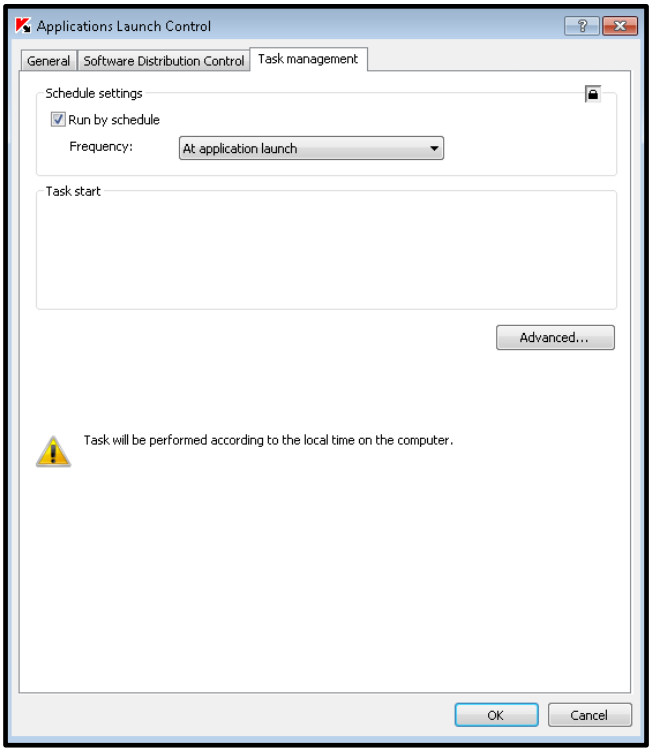
4. Go to **Local activity control,** press the **Settings…** button located on the **Application Launch Control** panel.



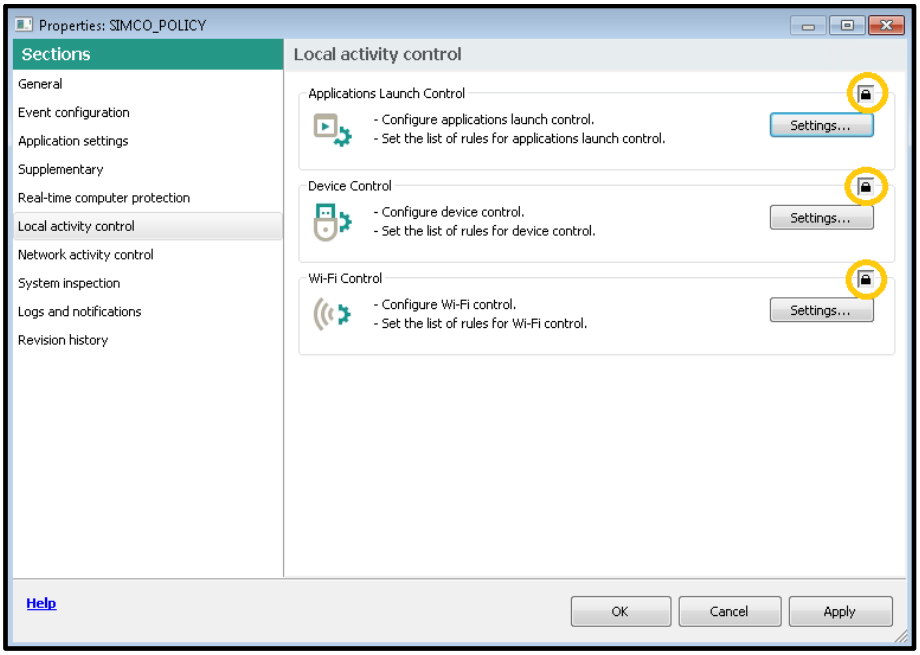
5. Go to the **General** tab and make sure all the settings match those shown in the screenshot below. The individual rule list (white list) for each host has been generated by the **Generate Rules for Application Launch Control** task and then has been stored on a local host.



6. Now go to the **Task Management** tab and specify the settings as shown below. Additionally, make sure that **At application launch** is selected from the **Frequency** drop-down list. Click **OK** to close the window.



7. Once you have reverted to **Local activity control,** close all **locks**  , press **Apply** and **OK** to exit editing the **SIMCO_POLICY** policy properties.

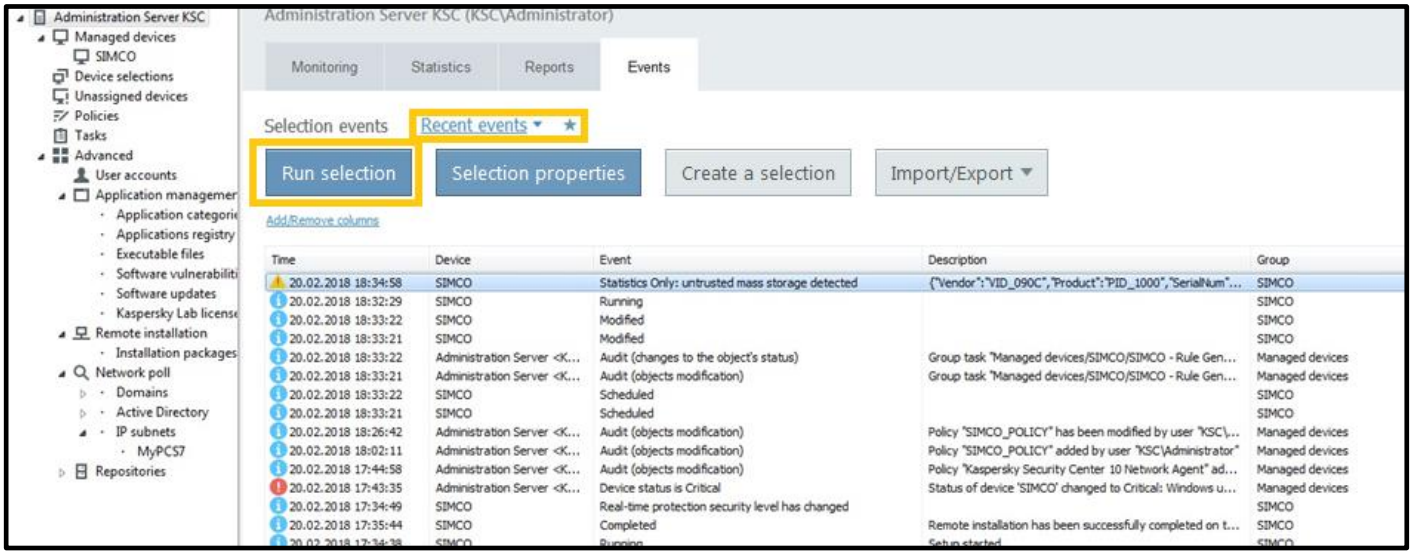


Our **KICS for Nodes** policy is no longer a generic one because now it contains application restrictions specific to a particular host (**SIMCO**, in our case).

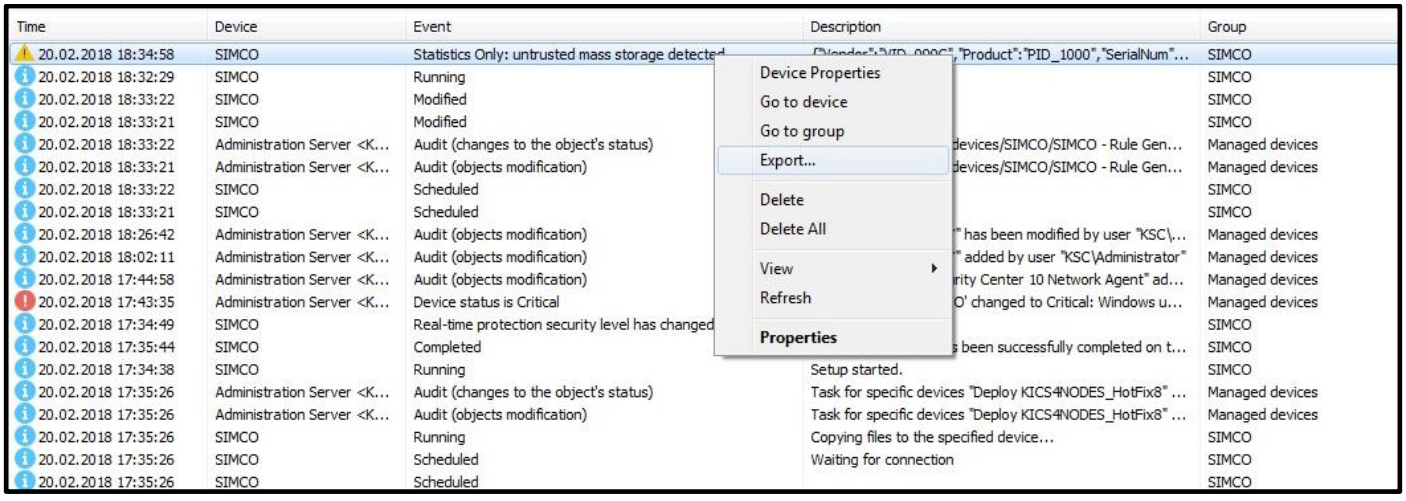
Setting up Device Control whitelisting

So far, we have set up **Device Control** to operate in the **Statistics Only** mode but the **Device Control** white list is still blank. Now we are going to add one removable storage device to the white list of legitimate devices.
Please go through the following steps:

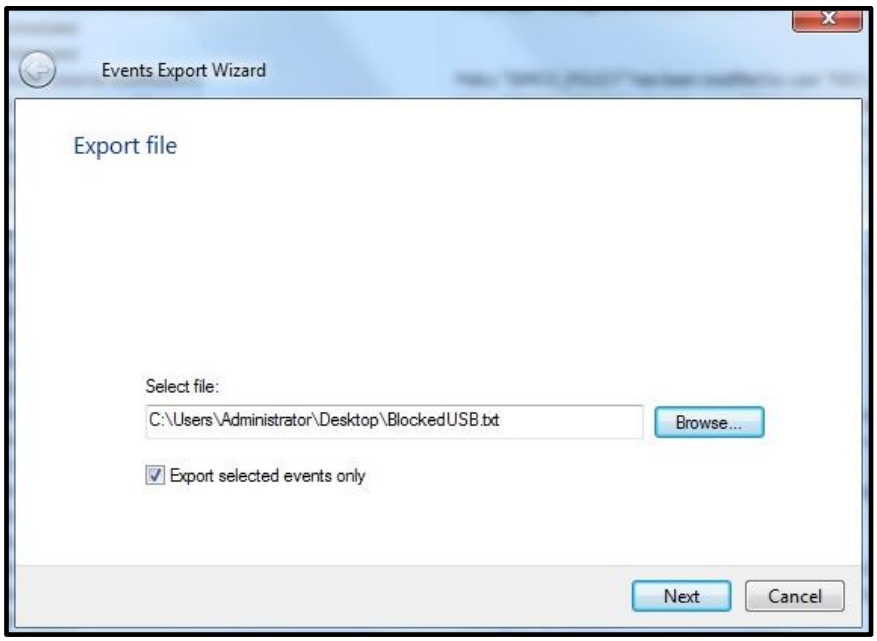
1. Take your USB storage device, which is deemed as trusted, and plug it into the target host running **KICS for Nodes**. In our example, it is **SIMCO**.
2. Wait for some minutes and then unplug the USB device.
3. Refer to the **KSC Administration Console**. Go to **Administration Server** and switch to the **Events** tab. Choose the **Recent events** selection and press **Run selection** to apply the filter.



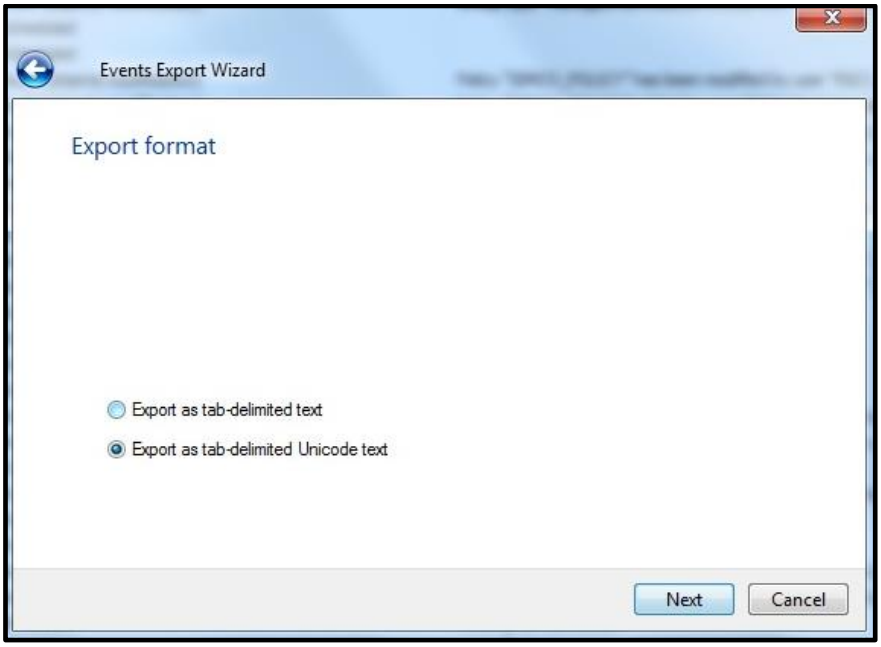
4. On the **Events** list find the recent notification **Statistics Only: untrusted mass storage detected**. This behavior is correct because our **Device Control** white list is still empty. Therefore, any USB device connected to the target host is treated as an untrusted one.
5. Select this event, right-click on it and in the context menu select **Export…**



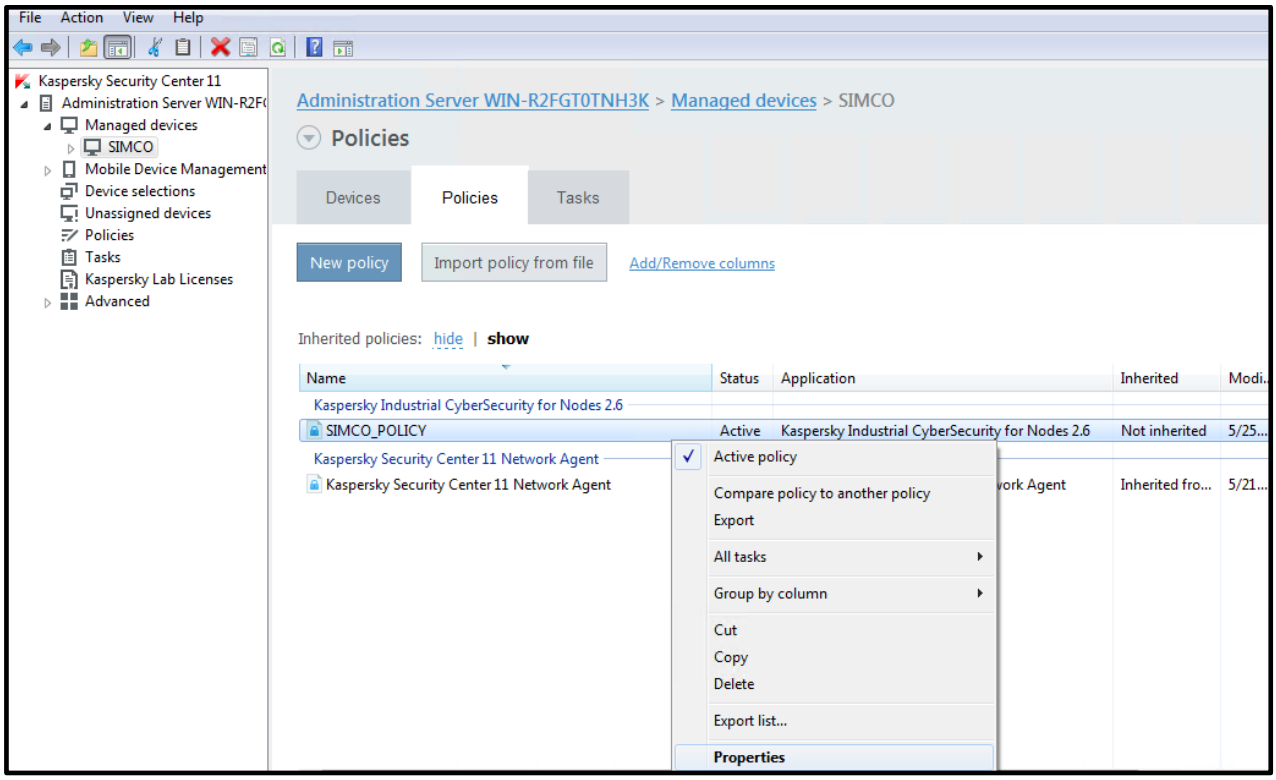
6. In the **Events Export Wizard** that pops up, check **Export selected events only** and specify the destination file you want to export data to. Click **Next**.



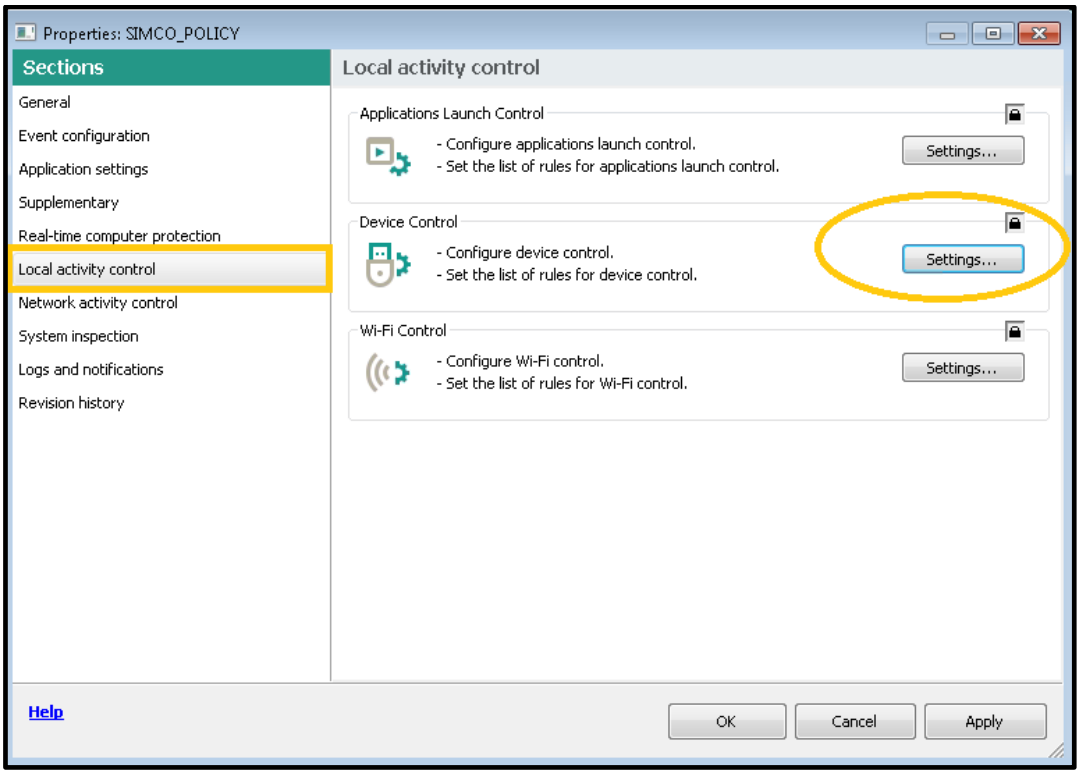
7. Specify the export format as shown below. Click **Next**.

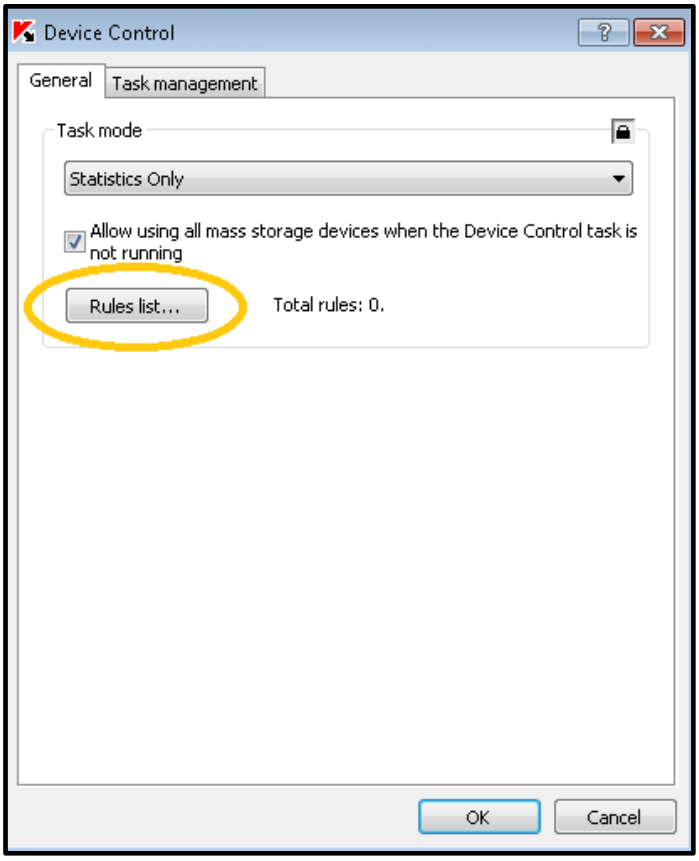


8. Now revert to the recently created **KICS for Nodes** policy and enter its **Properties** again.

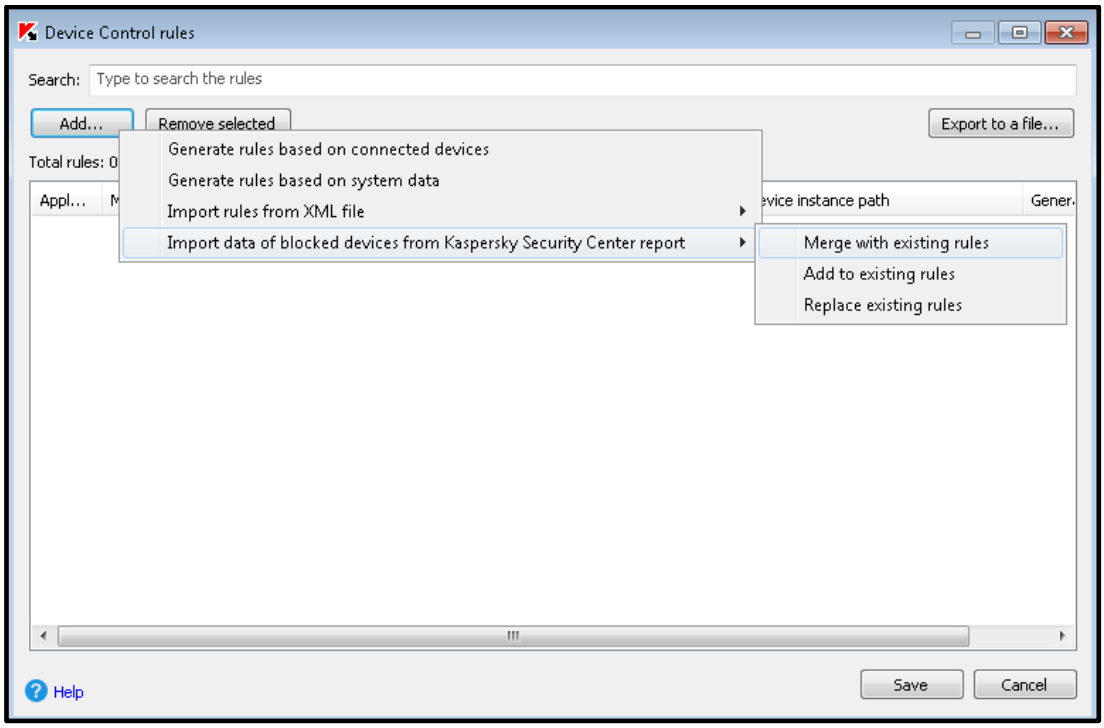


9. Go to **Local activity control->Device Control**. Click the **Settings…** button. In the popup window, click **Rules list…**

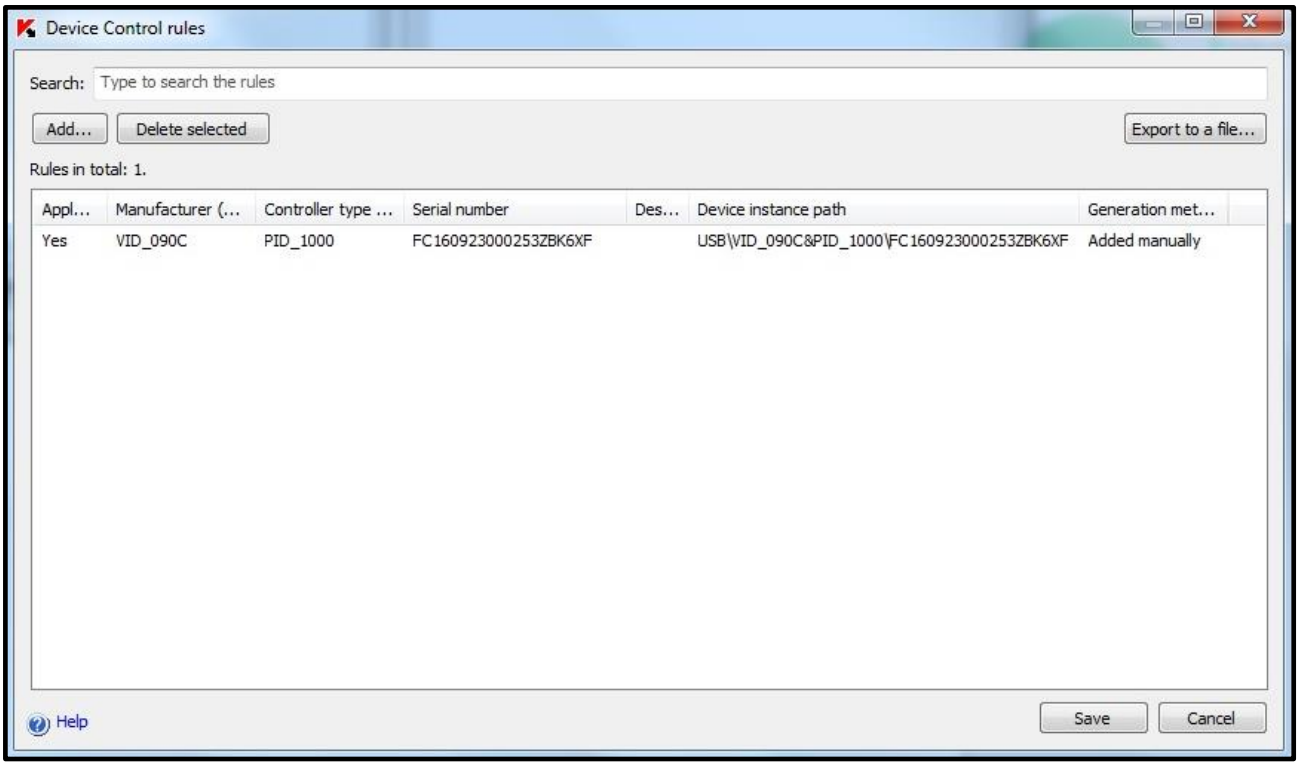




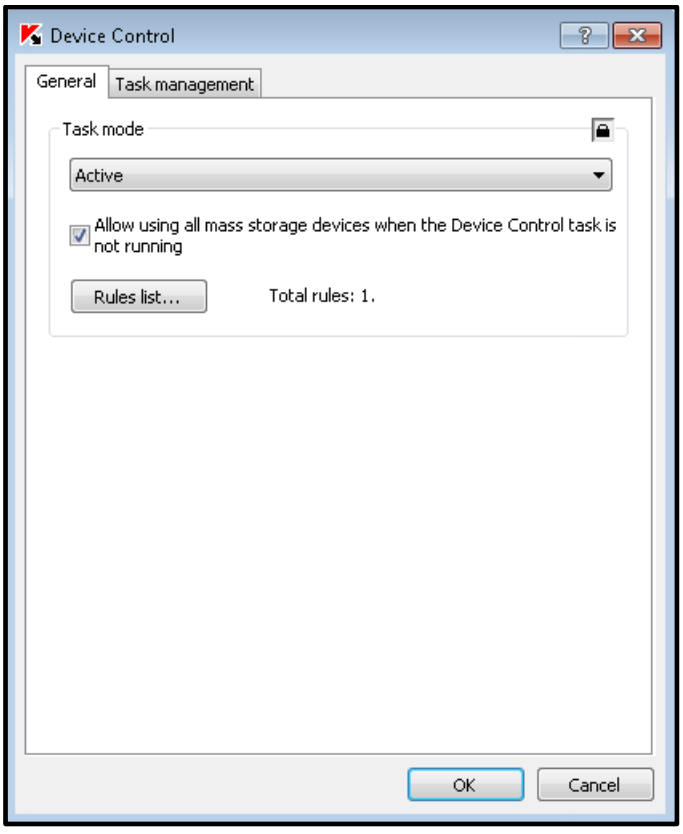
10. In the **Device Control rules** window, click the **Add…** button and select **Import data of blocked devices from Kaspersky Security Center report->Merge with existing rules**.



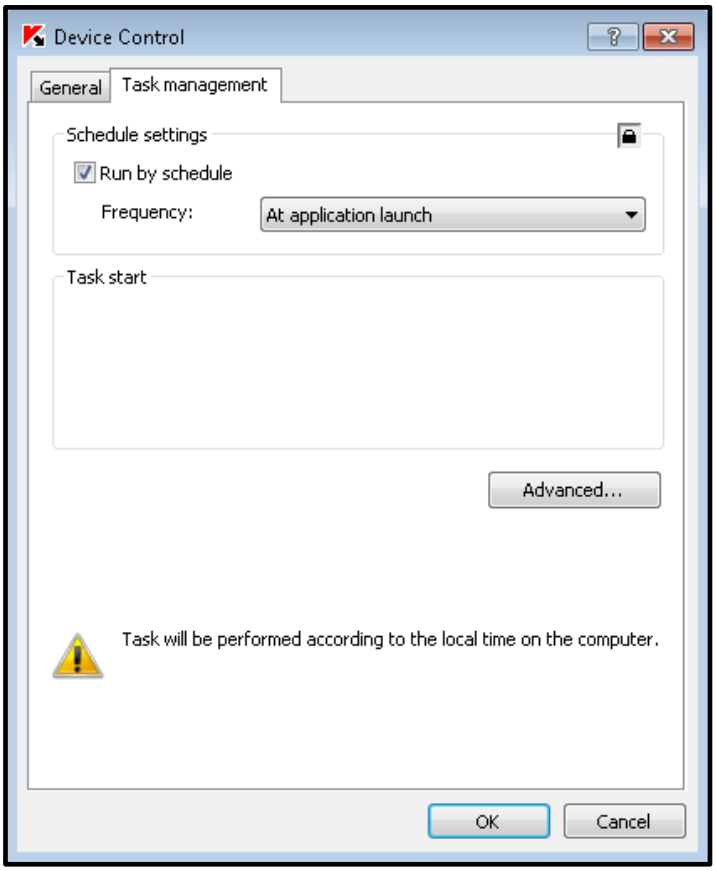
11. In the file browser window, find the recently created event file containing the blocked device information. In our example. It is **BlockedUSB.txt**. As a result, we have got one rule added to the **Device Control** white list as shown below. Click **Save** in the **Device Control rules** window.



12. Now set **Task mode** to **Apply Default Deny** and click **OK**.



13. Similar to **Application Launch Control**, proceed to the **Task Management** tab and specify the settings as shown below. Additionally, make sure that **At application launch** is selected from the **Frequency** drop-down list. Click **OK** to close the window.



14. Click **Apply** and **OK** in the policy **Properties** window. Wait until the policy enforcement finishes.

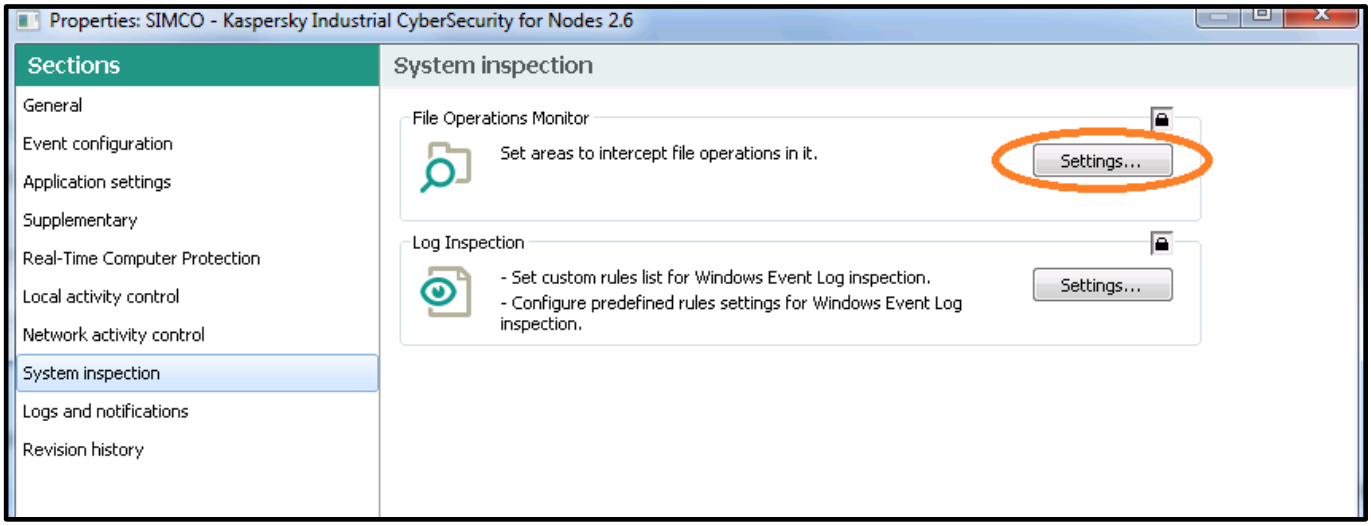
Setting up File Operations Monitor

In most cases, it is necessary to adapt the configuration of the **File Operations Monitor** to your control system configuration. Normally, this procedure implies matching the monitored folders to those where your automation project files are actually stored. However, you can instruct this module to monitor any location(s) at your discretion.

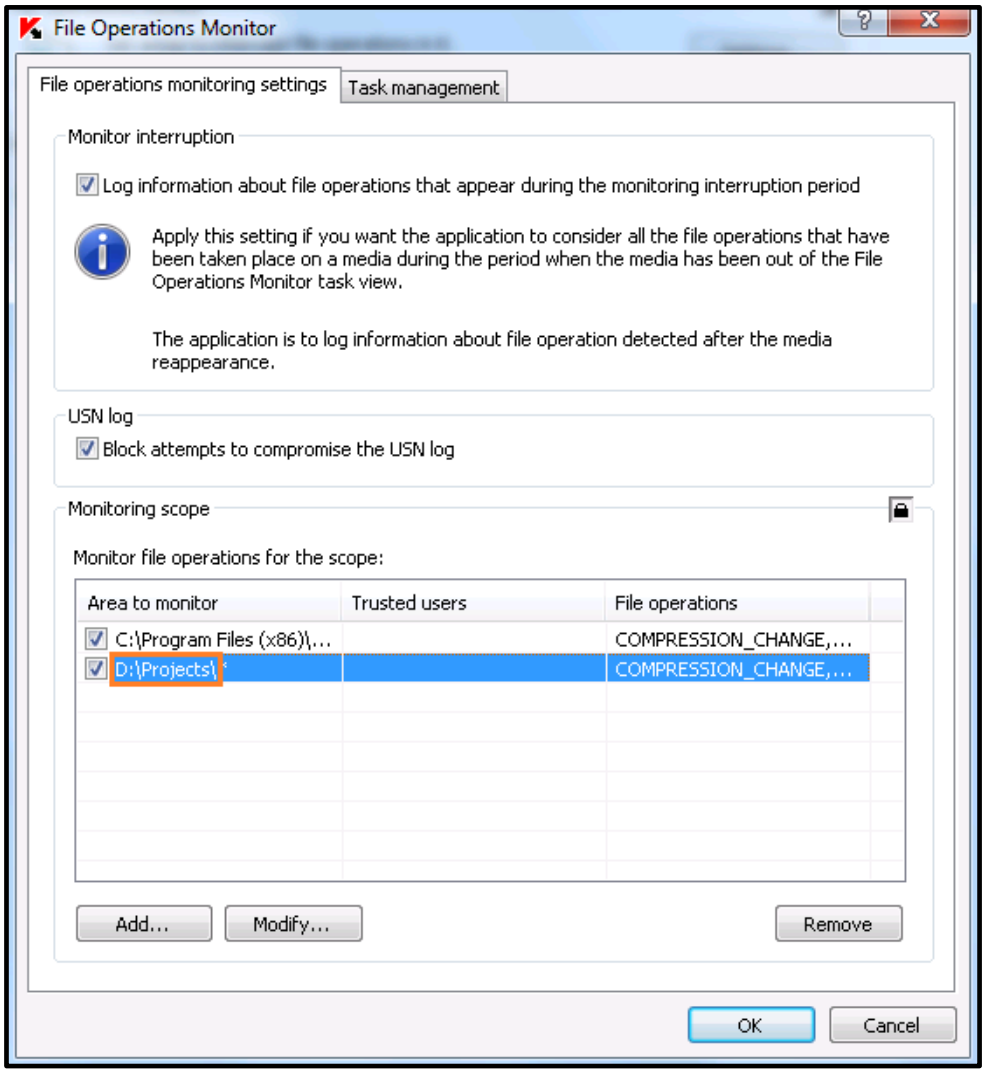
You may benefit from the preconfigured **KICS for Nodes** security policy contained in **Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp**. The default security policy already specifies some most common **WinCC** project locations available for file integrity monitoring. The file monitoring is set up so that false notifications would hardly ever bother you unless you start downloading an OS project using **Simatic Manager**.

Nevertheless, some fine tuning is still necessary.

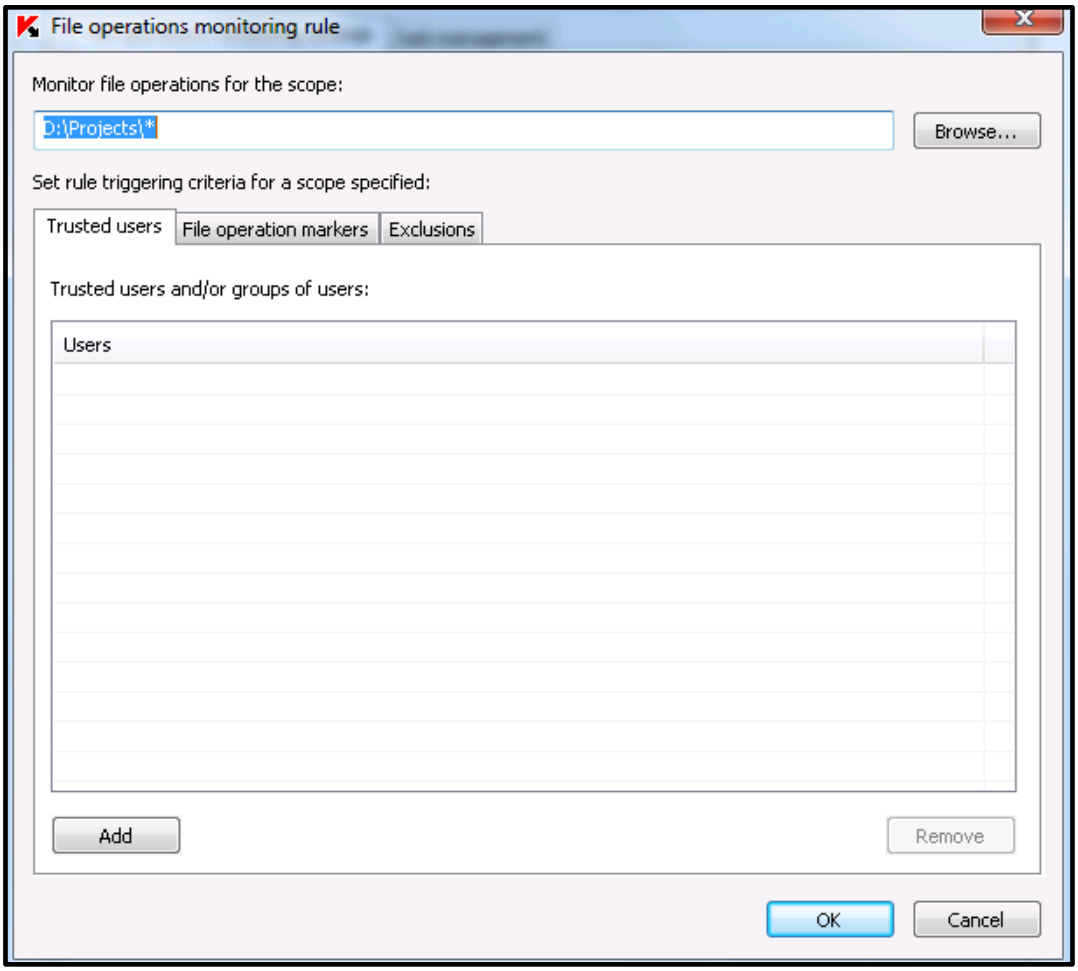
1. Go to the **KICS for Nodes 2.6** security policy and enter its properties. Switch to **System inspection** and click **Settings**… in the **File Operations Monitor pane**.



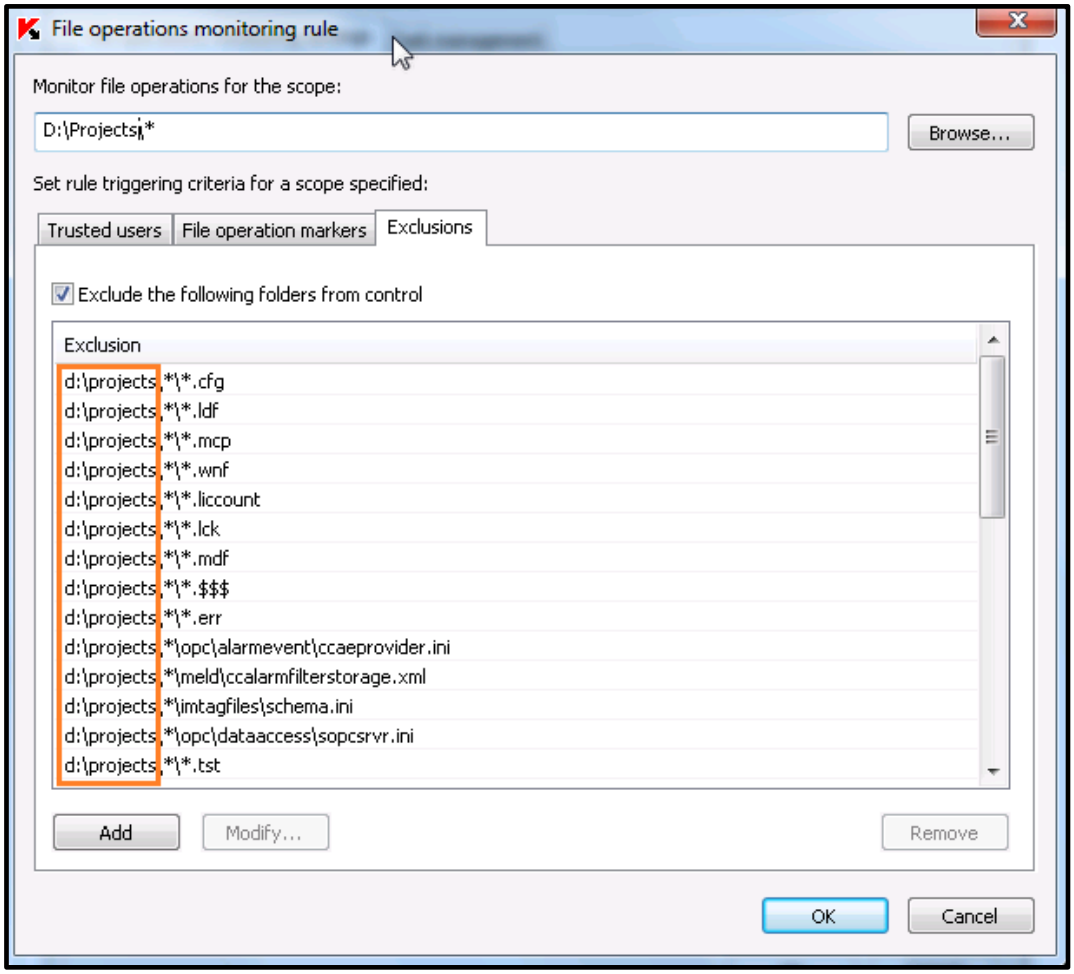
2. Select the second item from the **Monitoring scope** list and actualize the path of the **OS project location**. This mainly relates to **OS clients** and **OS servers**. In the default case, we assume that you store the **OS project** in the **D:\Projects** folder, but in practice the project path may vary. To make changes press **Modify…**



3. First modify the project path if required (highlighted in blue). Then switch to the **Exclusions** tab.



4. There are numerous paths (selections) on the list. Most of them are masks. You have to match the primary (highlighted) part of each path to the actual **OS** folder location. Leave the rest of each path intact. For example, if you store the **OS project** in **E:\MyPCSProjects**, then you have to convert **D:\Projects**.cfg** into **E:\MyPCSProjects**.cfg** and so on.



5. Click **OK** when done. This finalizes the **File Operations Monitor** fine-tuning.

Please mind that this module operates in the notification-only mode. Do not expect it to interrupt any file operations for it might affect the control software functions.

Setting up PLC Integrity Checker

PLC Integrity Checker controls the integrity of control logic by polling a target PLC and comparing its control application to the reference one. The polling interval is customizable.

In order to benefit from this module, the following prerequisites should be fulfilled:

- There must be at least one **Siemens S7-300/S7-400(H)** series PLC on your plant network.
- The target PLCs should be accessible via TCP/IP (the Siemens ISO communications are not supported at present). Try PINGing your PLC in order to check your control device accessibility.
- **PLC Integrity Checker** should be activated on those hosts that have network access to the target PLC. Assign **one** polling host to each target PLC.

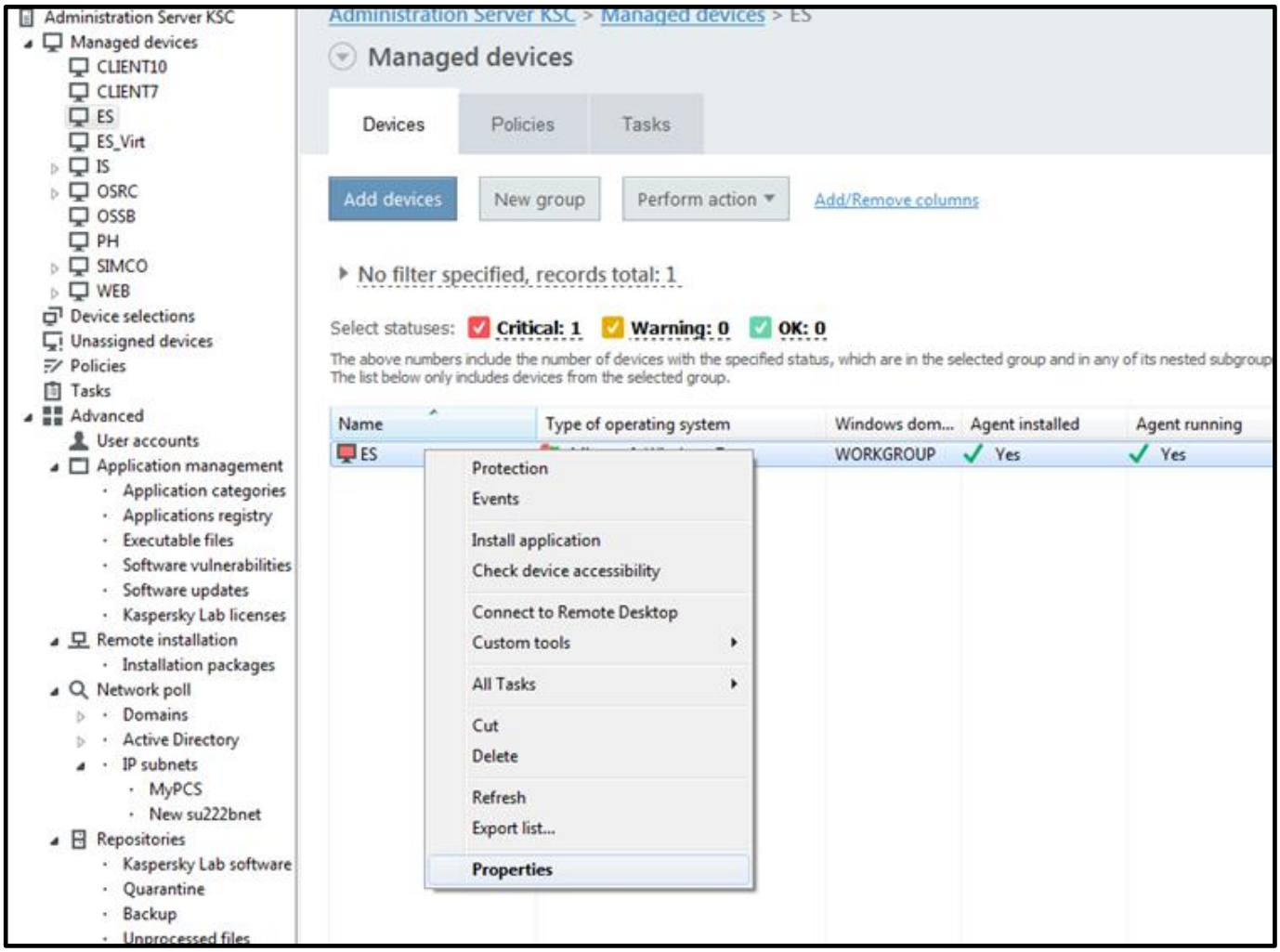
PLC Integrity Checker is not to be customized by means of security policies. Its configuration is carried out by parametrizing respective tasks.

In our example, we have added on more host (**Engineering Station, ES**) to the managed devices. **ES** is located on the same IP subnet (plant bus) as our target PLC.

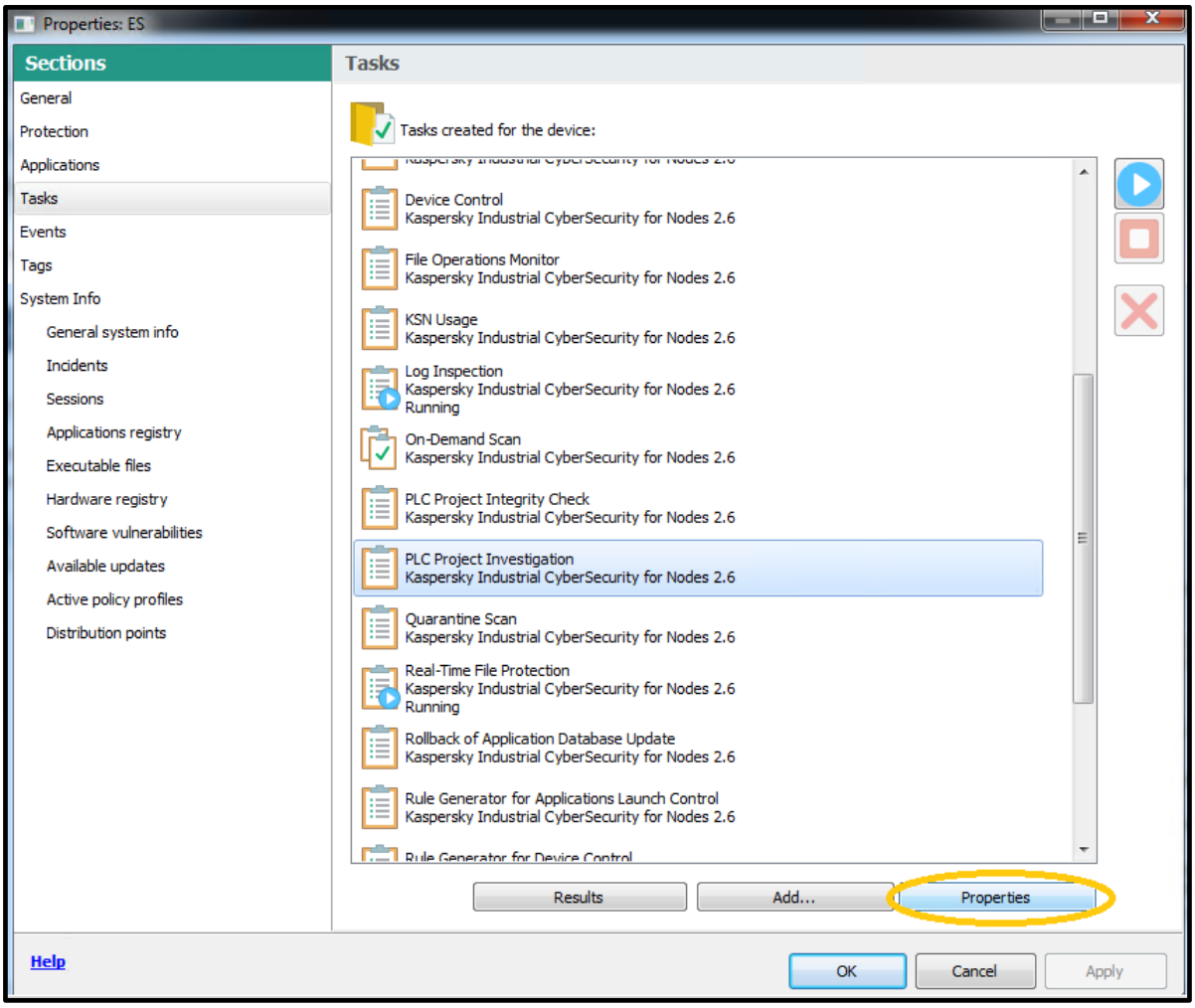
In this guide we will show you how to work with a Siemens S7-400H series PLC. For the other PLC models please refer to **“KICS for Nodes 2.6 Administrator’s Guide”**.

Please perform the following steps in order to set up **PLC Integrity Checker**:

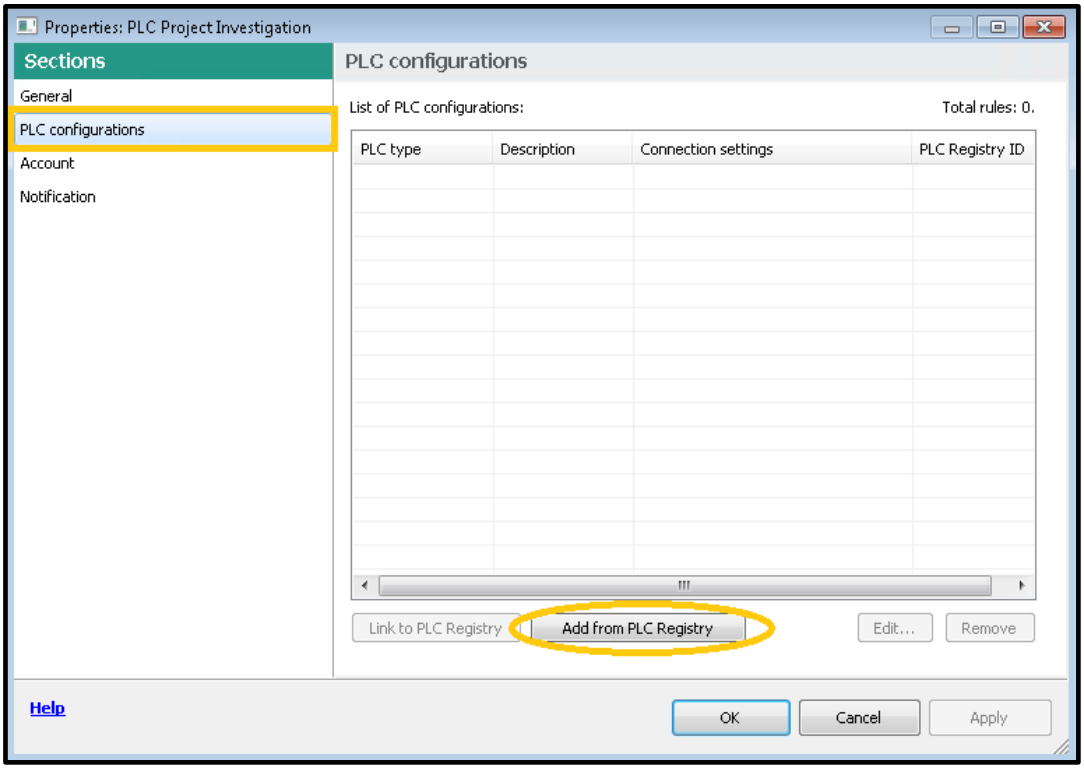
1. Go to **Administration Server->Managed devices->ES** and switch to the **Devices** tab**.** Right click on **ES** and select **Properties**.



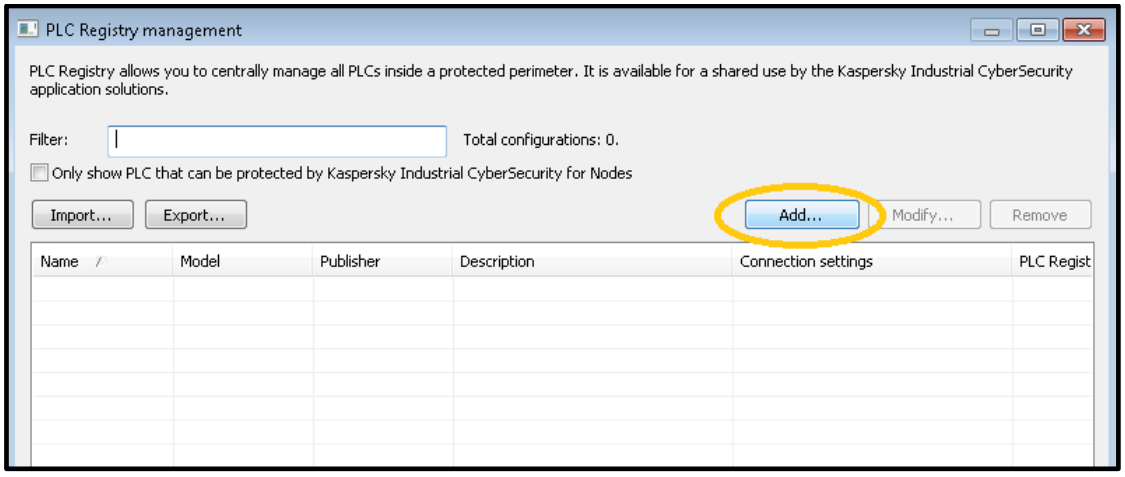
2. In the **Properties** window that pops up, go to **Tasks**. Scrolling down the **Tasks** list, find the **PLC Project Investigation** task and click the **Properties** button. This task is used to form or update a reference control logic snapshot.



3. In the task **Properties** window that pops up, go to **PLC configurations** and click the **Add from PLC Registry** button as shown below.

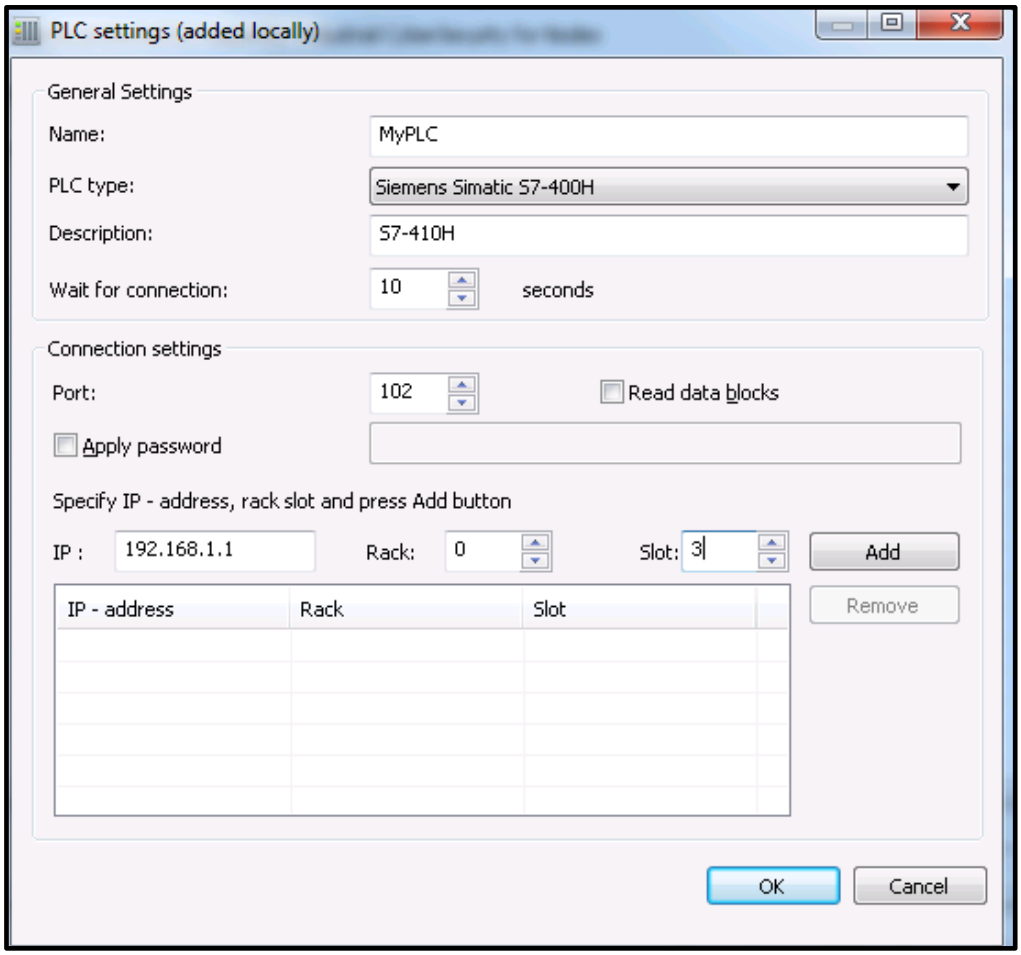


4. Now we have to add a monitored PLC to the **PLC Registry**. Press the **Add…** button.

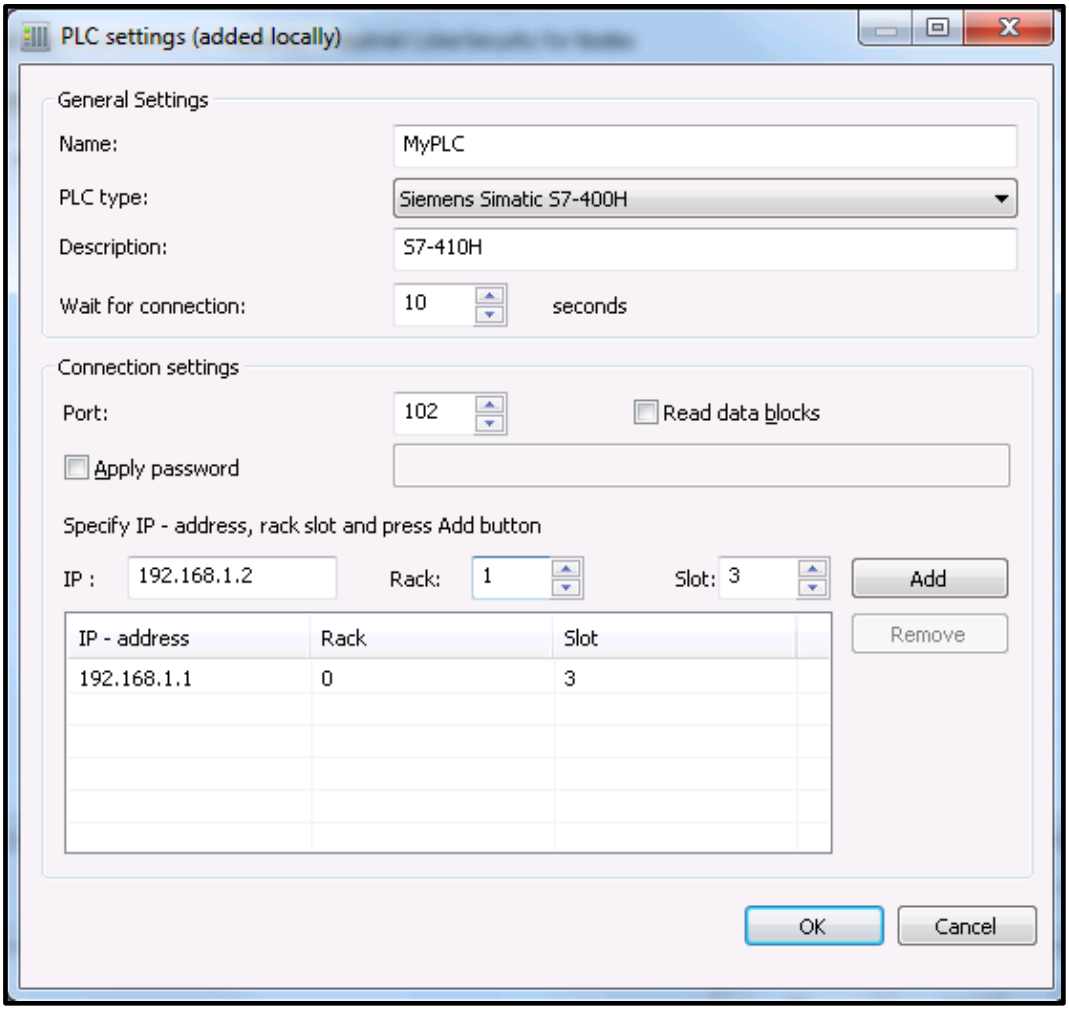


5. In the **PLC settings** window that pops up, choose an appropriate **PLC type**, enter an arbitrary name (description) of the PLC and enter the device **IP address**. Also specify the **Rack number**, **Port** and **Slot number** values depending on your **PLC type** and its hardware configuration. In most cases, for **Siemens SIMATIC S7-300** PLCs you can assume **Rack number=0**, **Port=102**, **Slot number=2**. For fault-tolerant **Siemens SIMATIC S7-400H** PLCs, the MASTER CPU has normally **Rack number=0**, **Port=102**, **Slot number=3** whereas the STANDBY CPU has **Rack number=1**, **Port=102**, **Slot number=3.** In our example, we have got the **S7-410-5H** fault-tolerant PLC available at **192.168.1.1(MASTER CPU)/192.168.1.2(STANDBY CPU)**. Click **OK** when done.

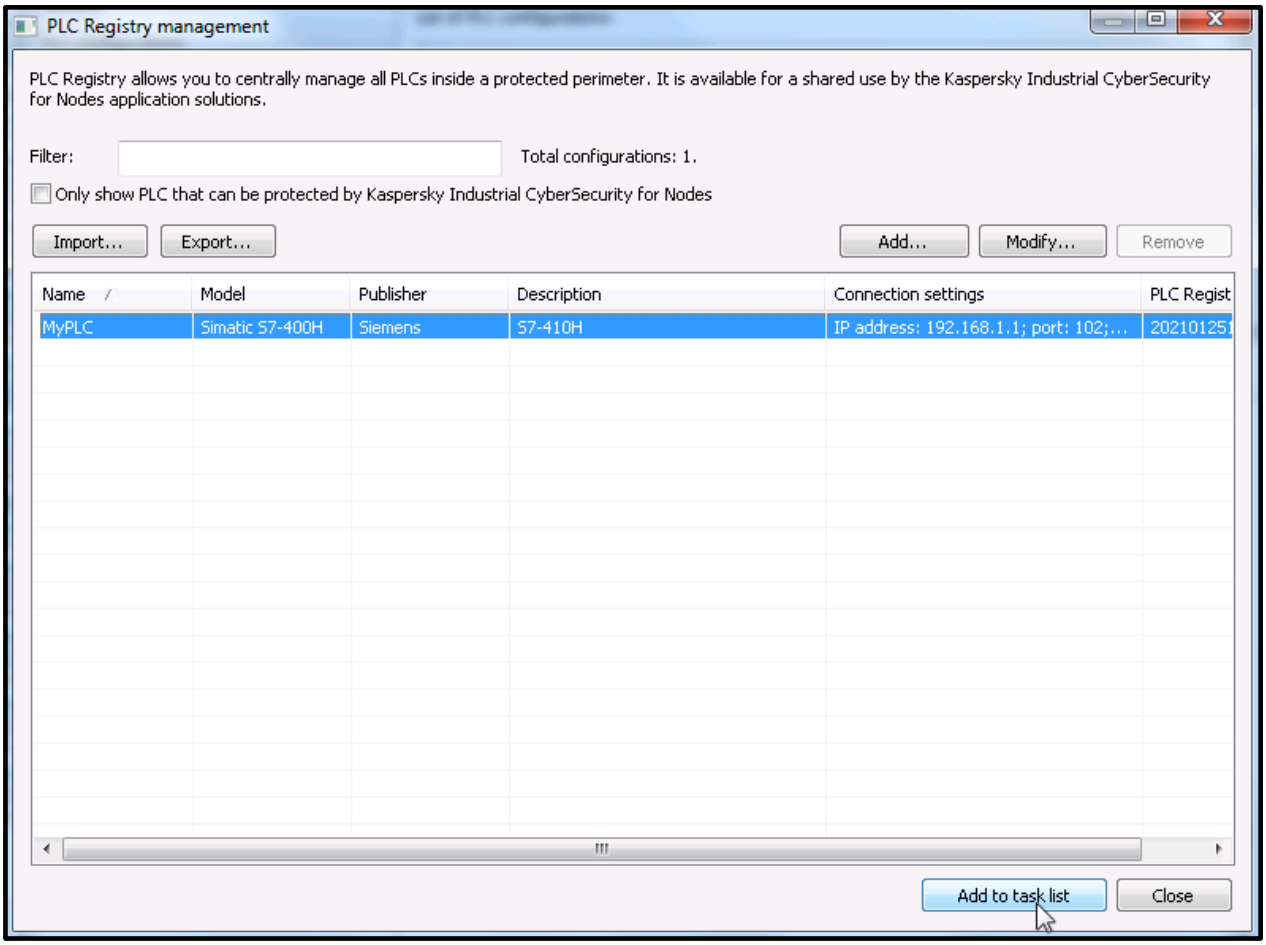
6. So, we enter the configuration for the **MASTER CPU** as follows and we click **Add**. Please note, that we are not willing to track **DB**s as they contain constantly changing variables which may lead to multitude of false positives.



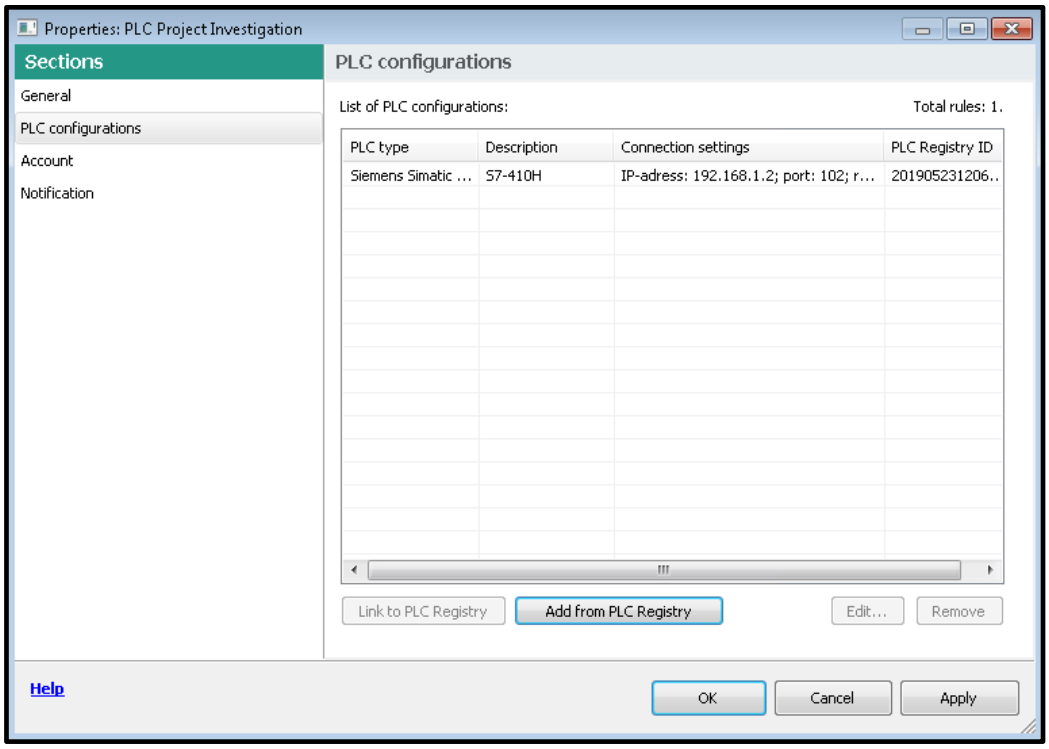
7. Now we enter the respective configuration for the redundant partner and we click **Add**. Once we completed two halves of our PLC we press **OK** to quit the PLC specification.



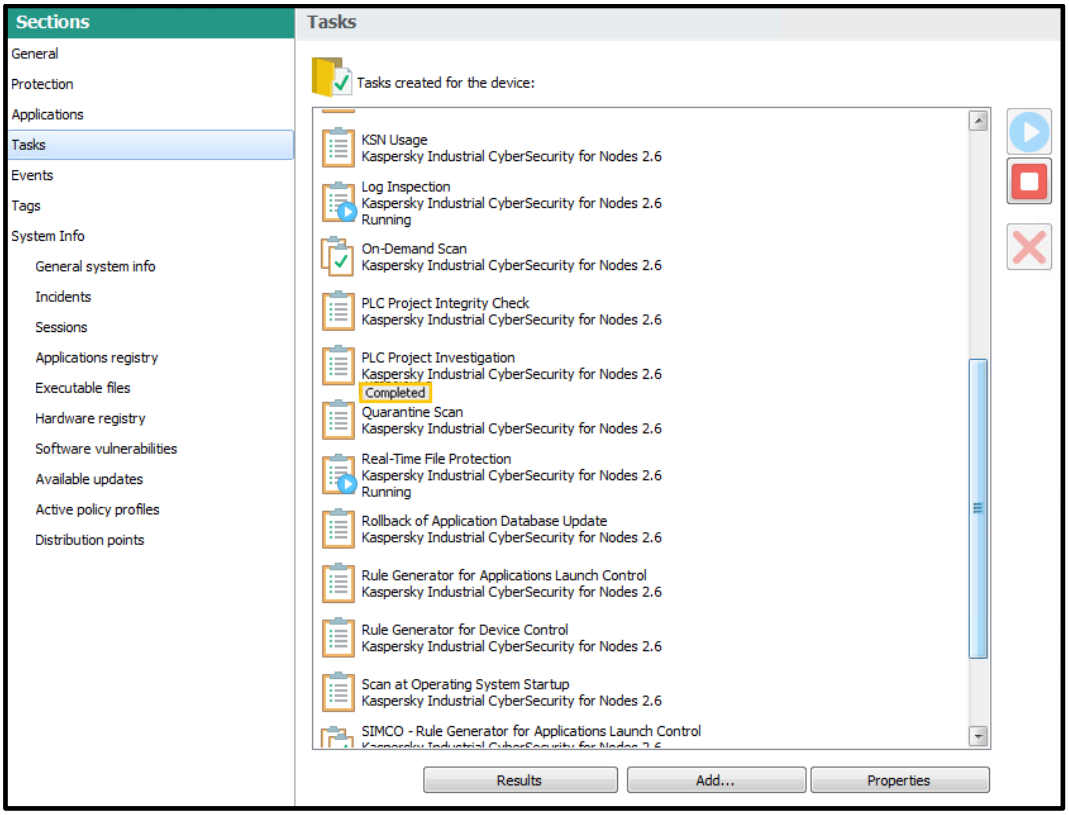
8. In the parent window, you should now see the just added PLC (as shown below). Revise the PLC configuration by expanding the **Connection settings** column and click **Add to task list** if everything is correct. Click **Close** to close the window.



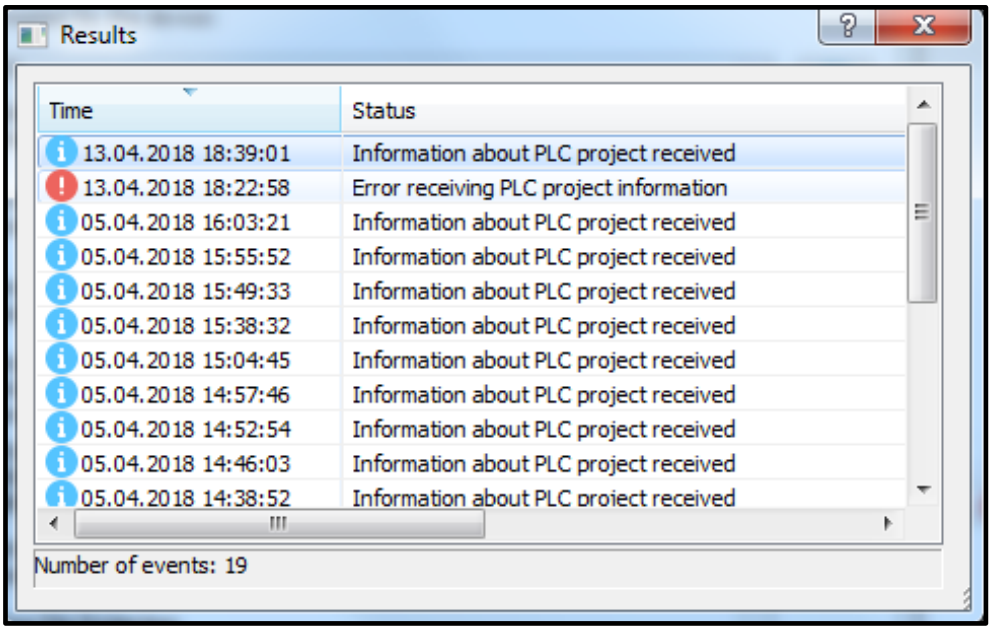
9. Click **OK** in the parent window to finalize the task parametrization.



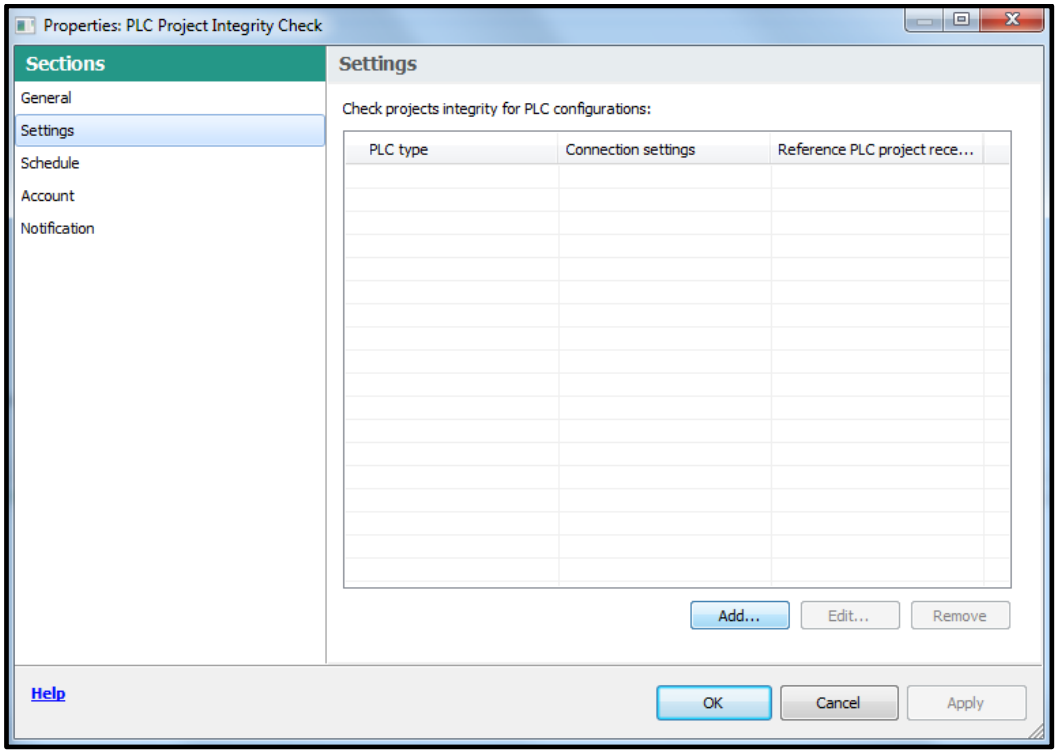
10. Select the just configured **PLC Project Investigation** task and start it by pressing  . Wait until the task is displayed as **Completed**.



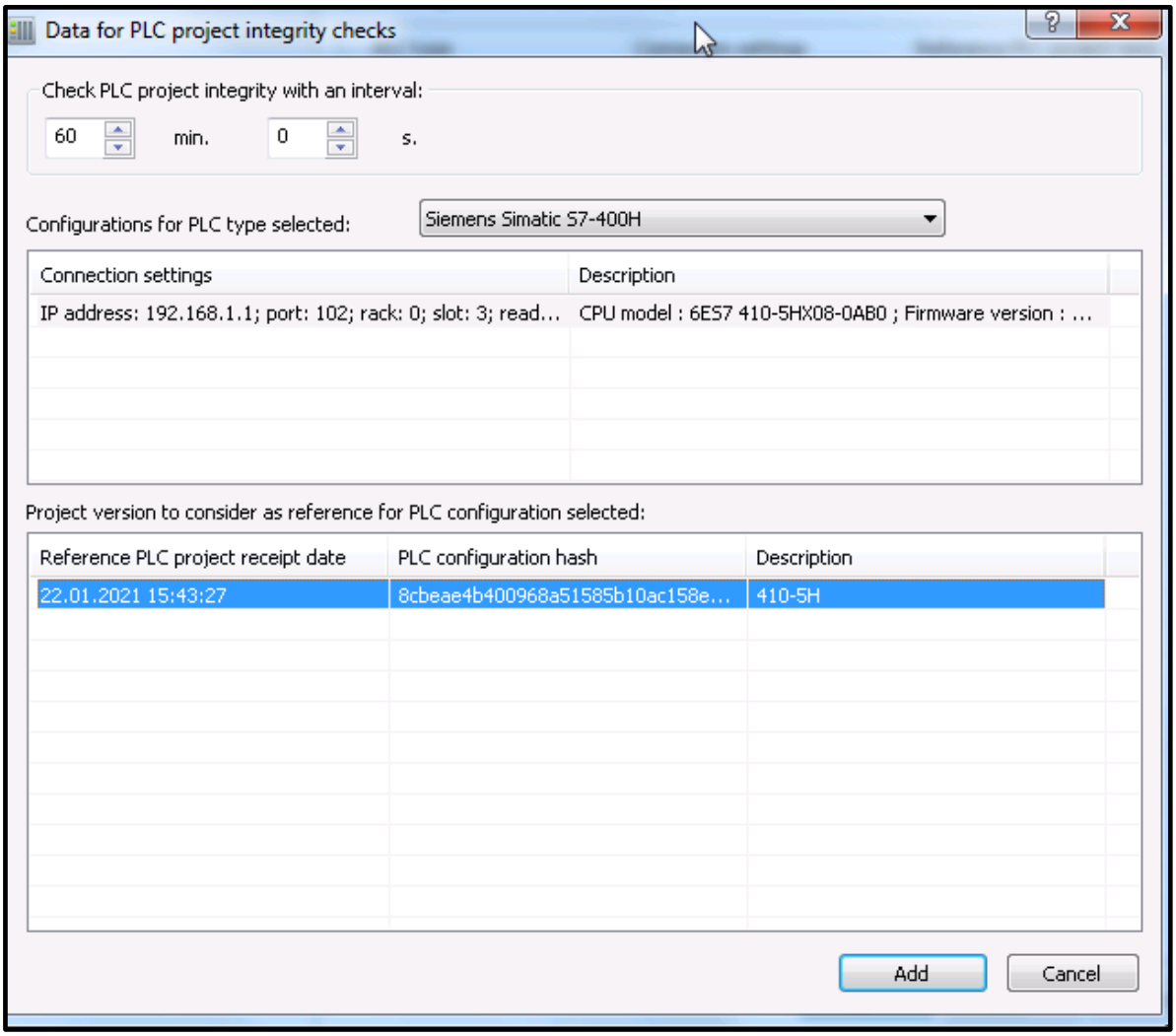
11. In order to make sure that the reference control logic has been successfully retrieved from the PLC, click the **Properties** button. Make sure that in the popup window the most recent status is displayed as **Information about PLC project received**. Close the popup window.



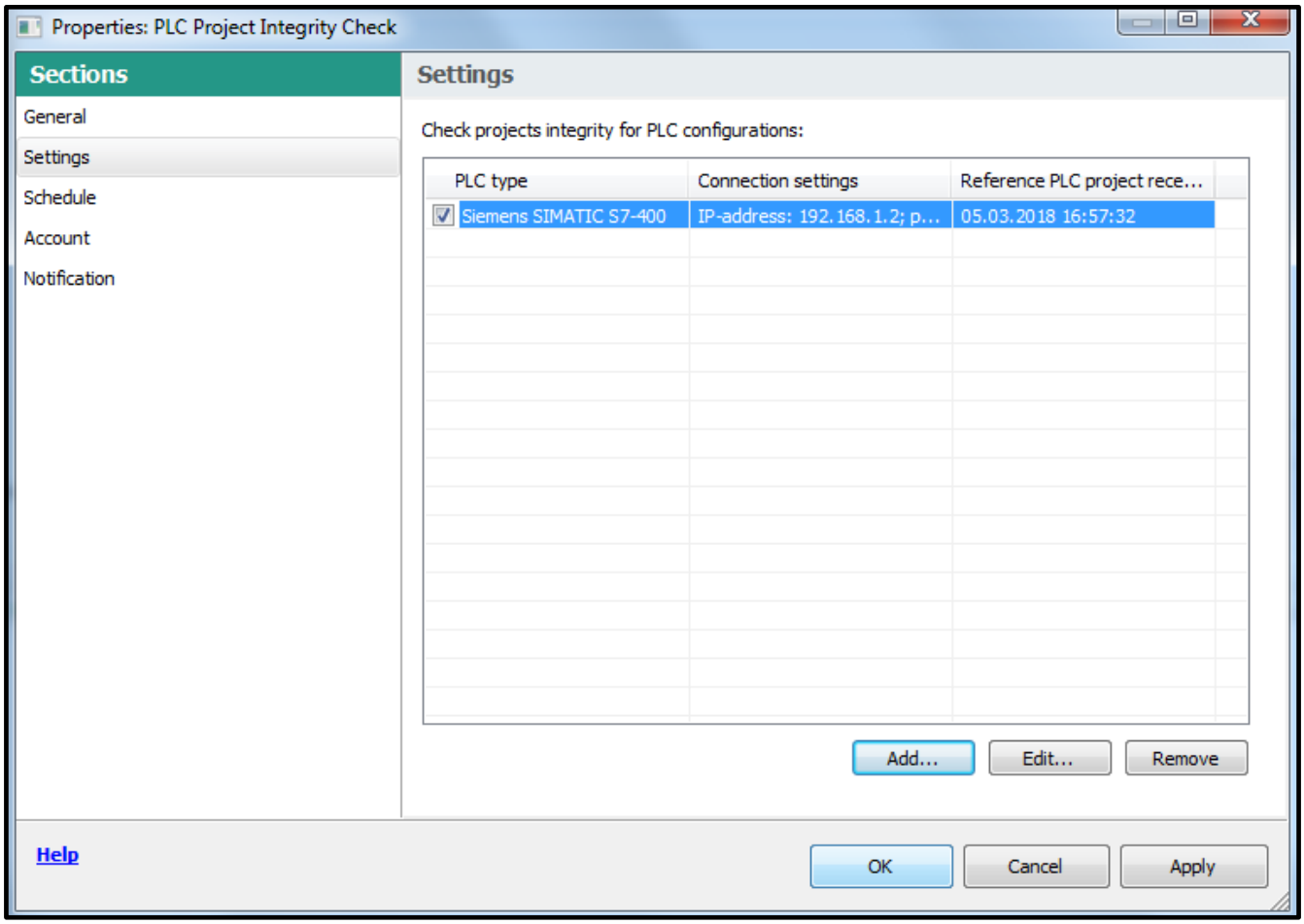
12. Now, wait a little bit until the inter-task synchronization is completed. It takes 15 minutes.
13. Select the **PLC Project Integrity Check** task and press the **Properties** button.
14. In the window that appears, go to **Settings**. Click the **Add…** button.



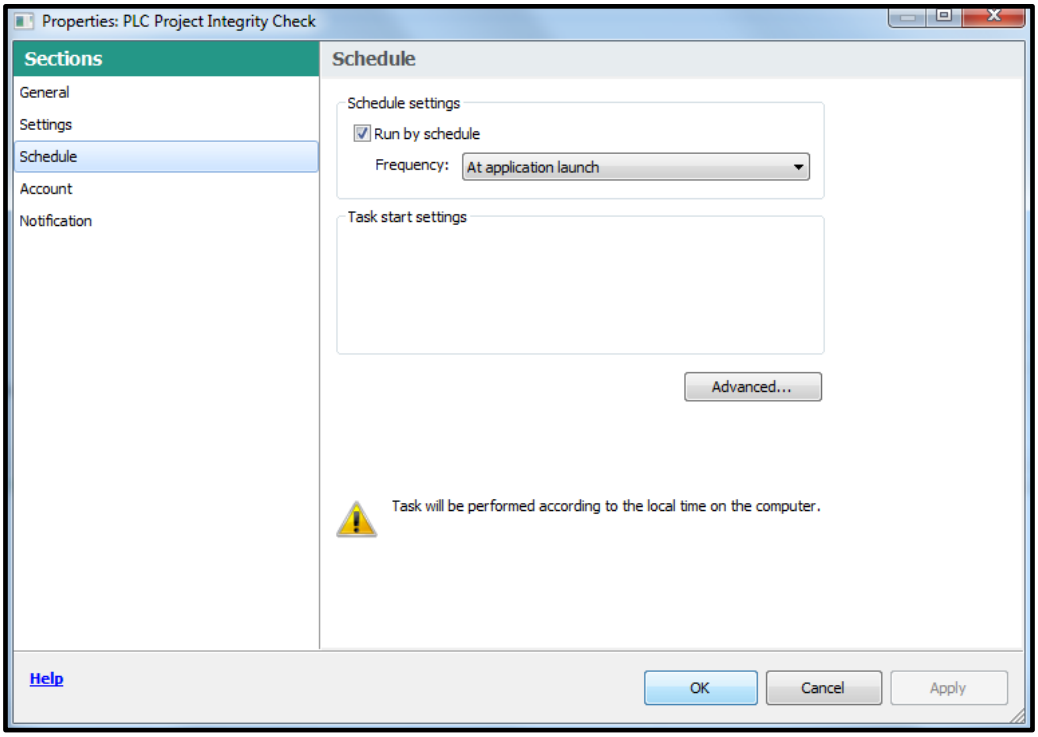
15. In the window that appears, select the corresponding **PLC type** and choose the most recent **PLC project snapshot (hash)** which the **PLC Project Investigation** task has previously generated. The selected hash will be a basis for subsequent PLC polls comparison. Specify an adequate polling interval. Avoid excessively frequent polling since it may deteriorate network performance. In most cases, one polling request per hour seems a reasonable frequency. Click **Add…** when done.



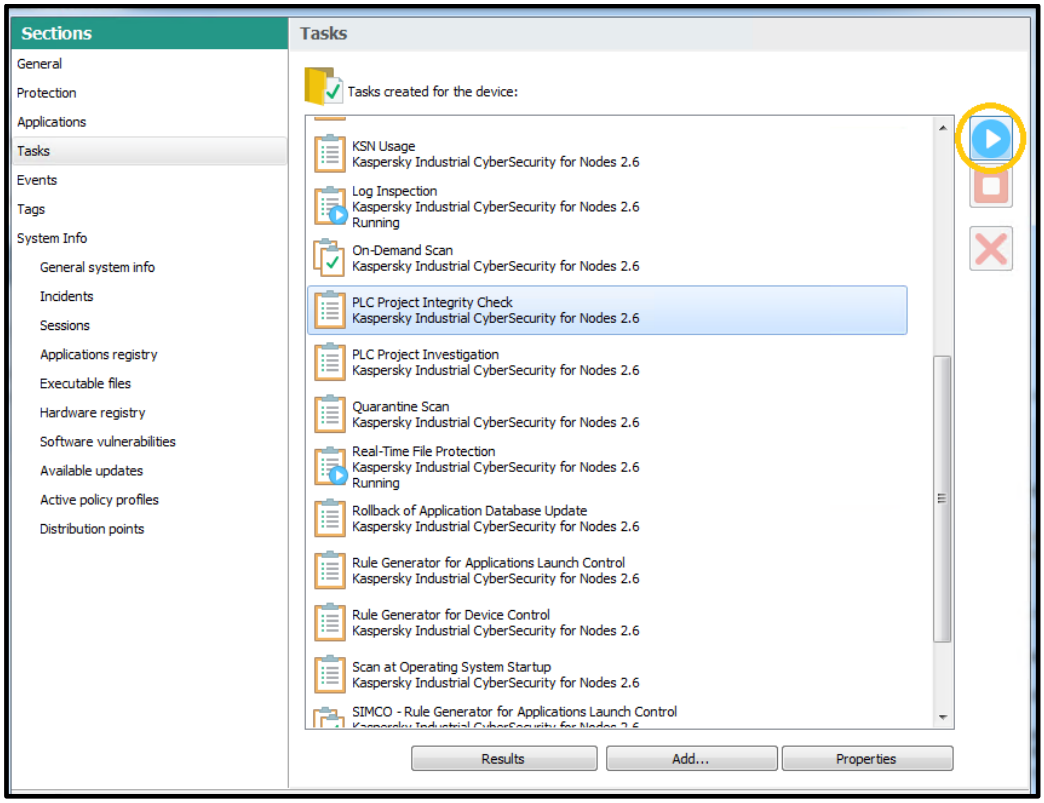
16. In the parent window, check the just added reference project as shown below and proceed to **Schedule**.



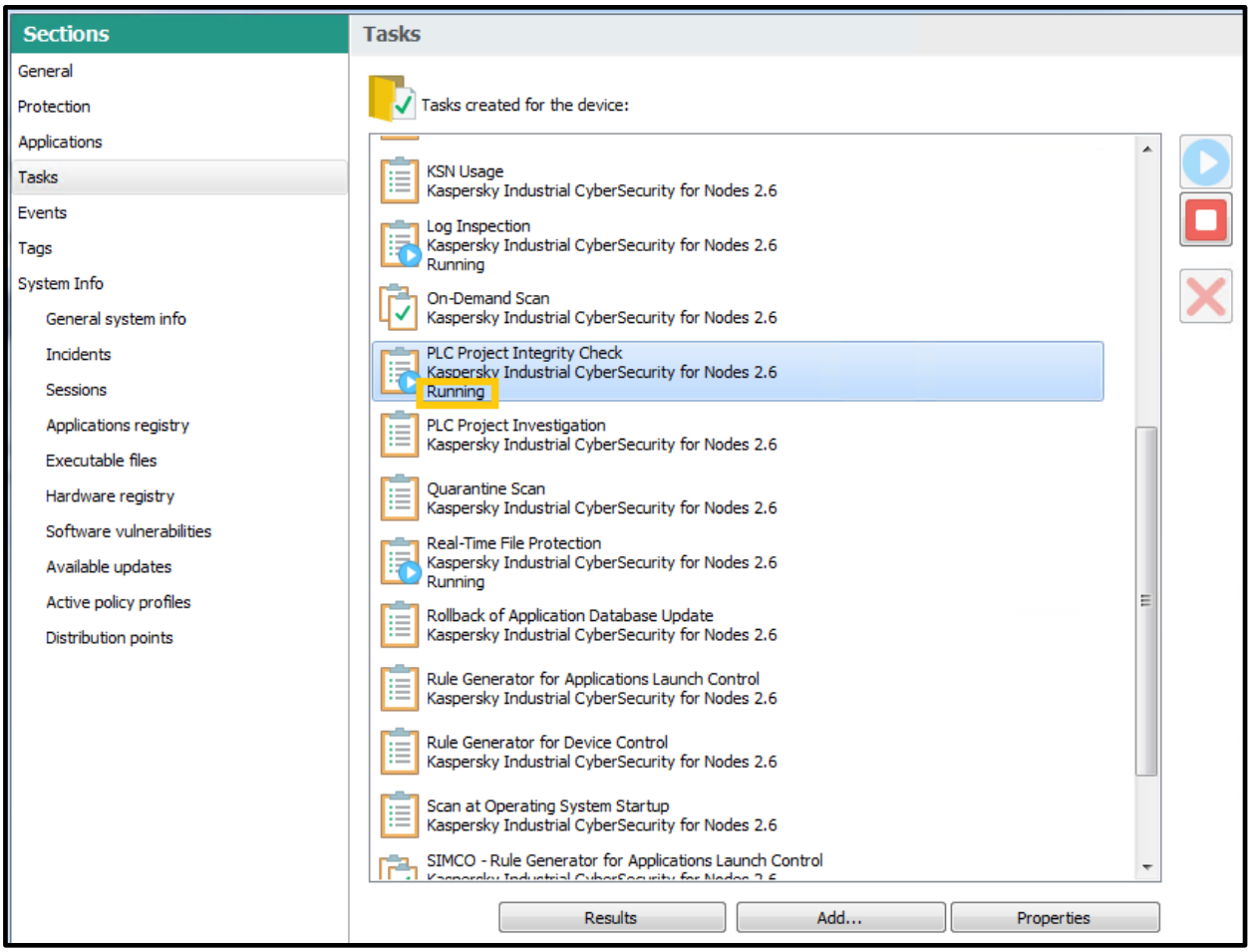
17. In **Schedule** specify the task **Schedule** settings as shown below. Click **OK** to finalize the task parametrization.



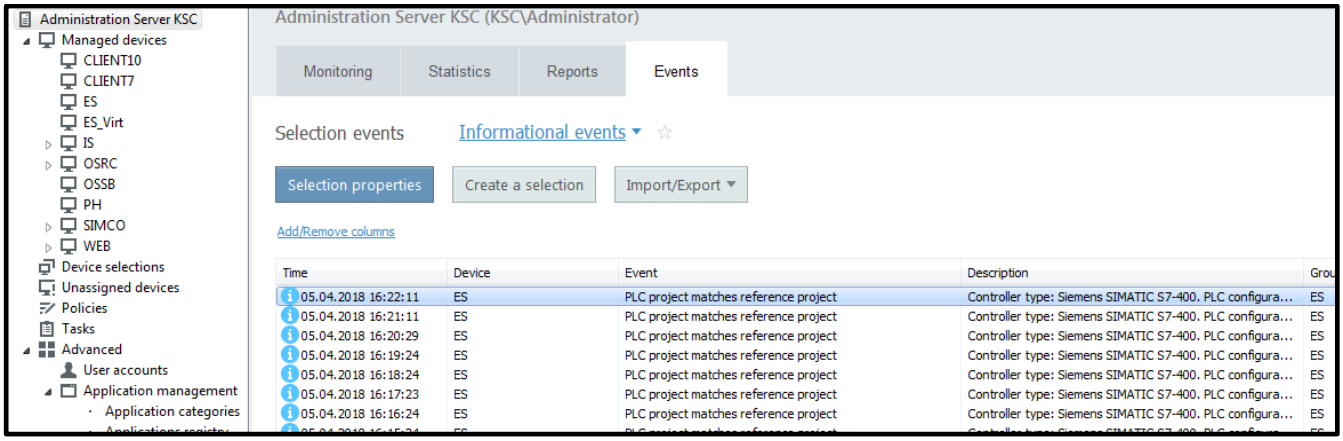
18. Select the **PLC Project Integrity Check** task and click  in order to start it.



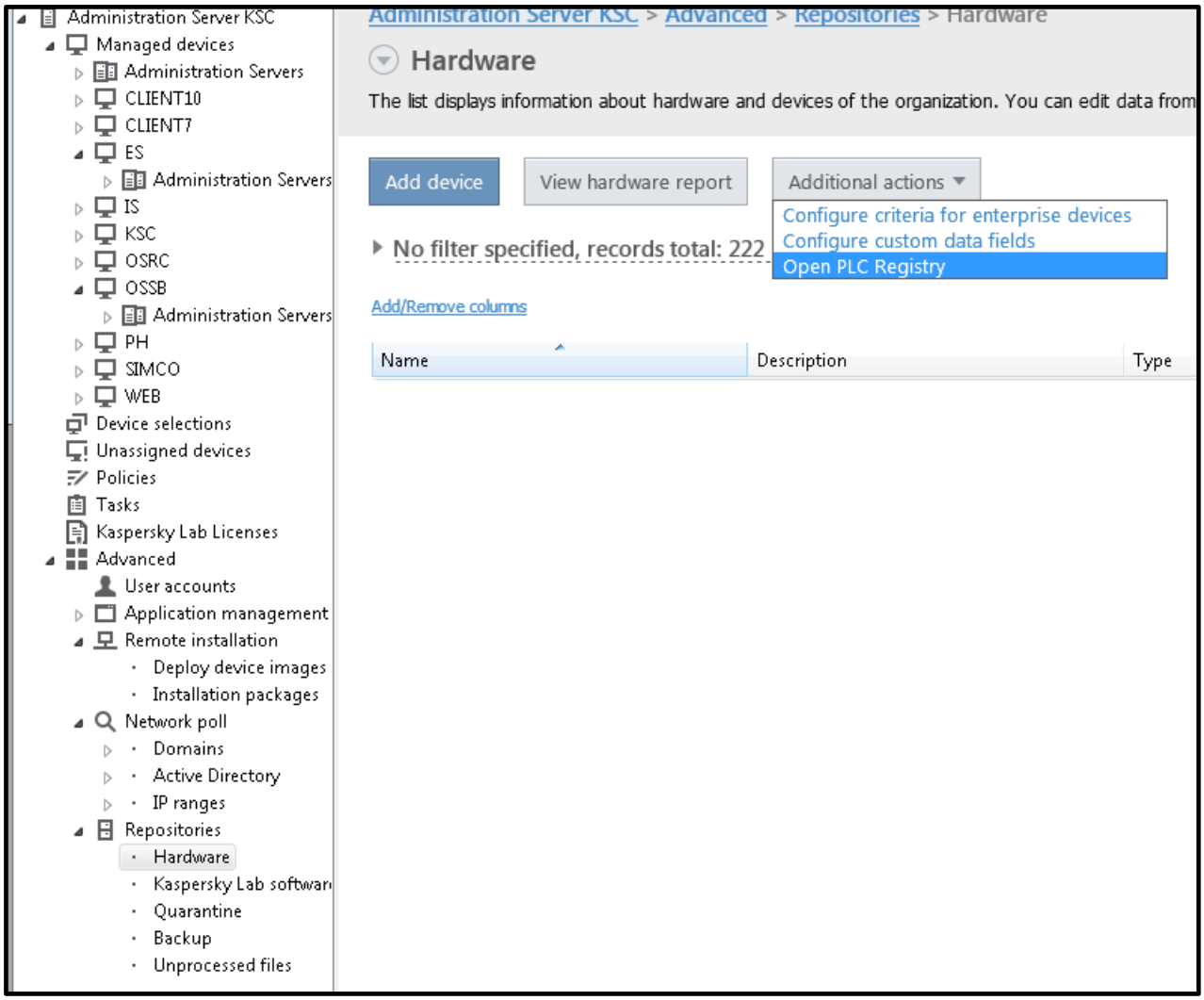
19. Make sure that the task status is now displayed as **Running**. Click **OK** to exit the **ES Properties** window.



20. Subsequently, you will be able to track PLC polling results if you go to **Administration Server** and switch to the **Events** tab.



21. Later on, during system operation, you may need to edit the PLC settings. Rather than manipulating with the **PLC Project Investigation** task, you can go to **Advanced->Repositories->Hardware** and select **Open PLC Registry** hidden in **Additional actions**.



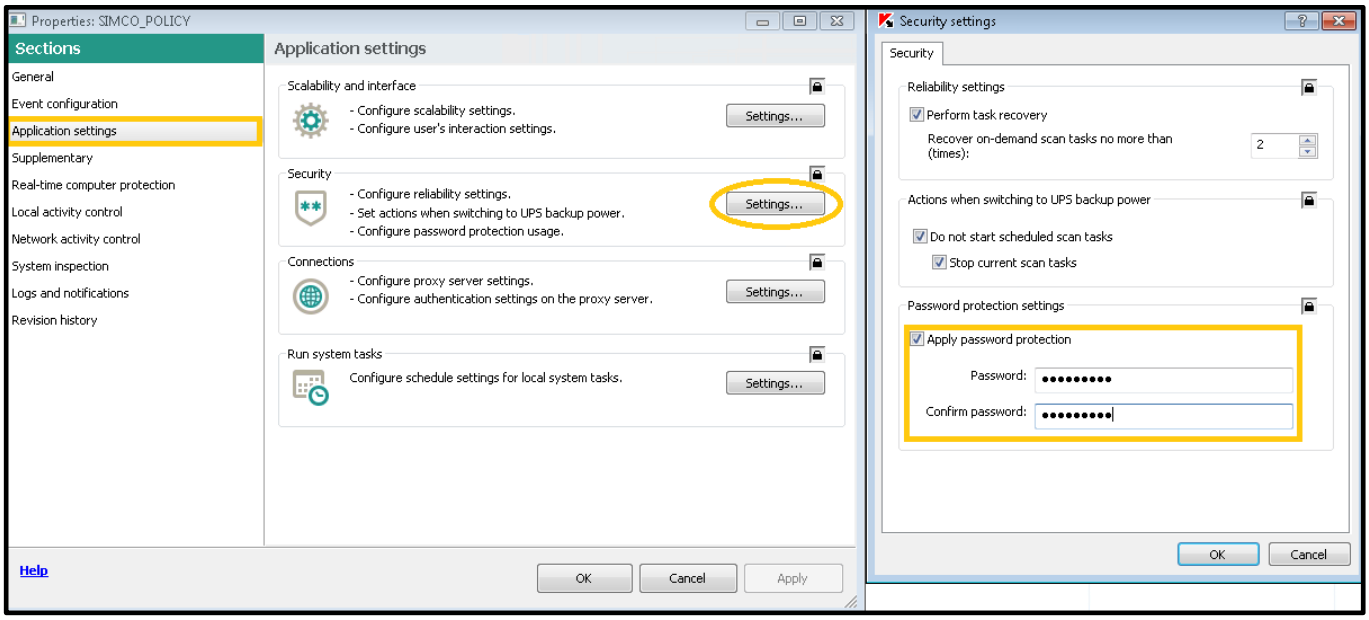
This completes the **KICS for Nodes** parametrization for a single host. For multiple hosts you should proceed in a similar manner by making use of group security policies and group tasks.

Enabling optional password protection

By default, any local user having administrative privileges is allowed to uninstall or modify **KICS for Nodes** without referring to **KSC**. Such users can also launch the **KICS for Nodes management console** locally (providing that it is installed) and manipulate with the protection settings at their discretion (unless these settings are overridden and locked by the **KSC** policy). In order to prevent this, additionally, you can enable the **KICS for Nodes** password protection, which restricts the software removal/modification as well as management console access.

Please perform the following steps.

1. Go to the **SIMCO** node and switch to the **Policies** tab.
2. Locate your active policy applied to **SIMCO**. Right-click it and in the context menu go to **Properties**.
3. Go to **Application settings** and press **Settings…** located on the Security and reliability panel.



4. In the **Security settings** window that pops up go to the **Password protection settings** panel, check **Apply password protection** and enter your password twice.
5. Enable each of the three Locks and press **OK**.
6. Press Apply and then **OK** in the parent window.
7. Wait until the policy changes are applied to the **SIMCO** host.

After this, any **KICS for Nodes** removal/modification attempt performed by a local user on a local machine will prompt him/her to enter a correct password. Starting **KICS for Nodes management console** locally (providing that it is installed) will also require entering a valid password.

Installing optional KICS for Nodes management console

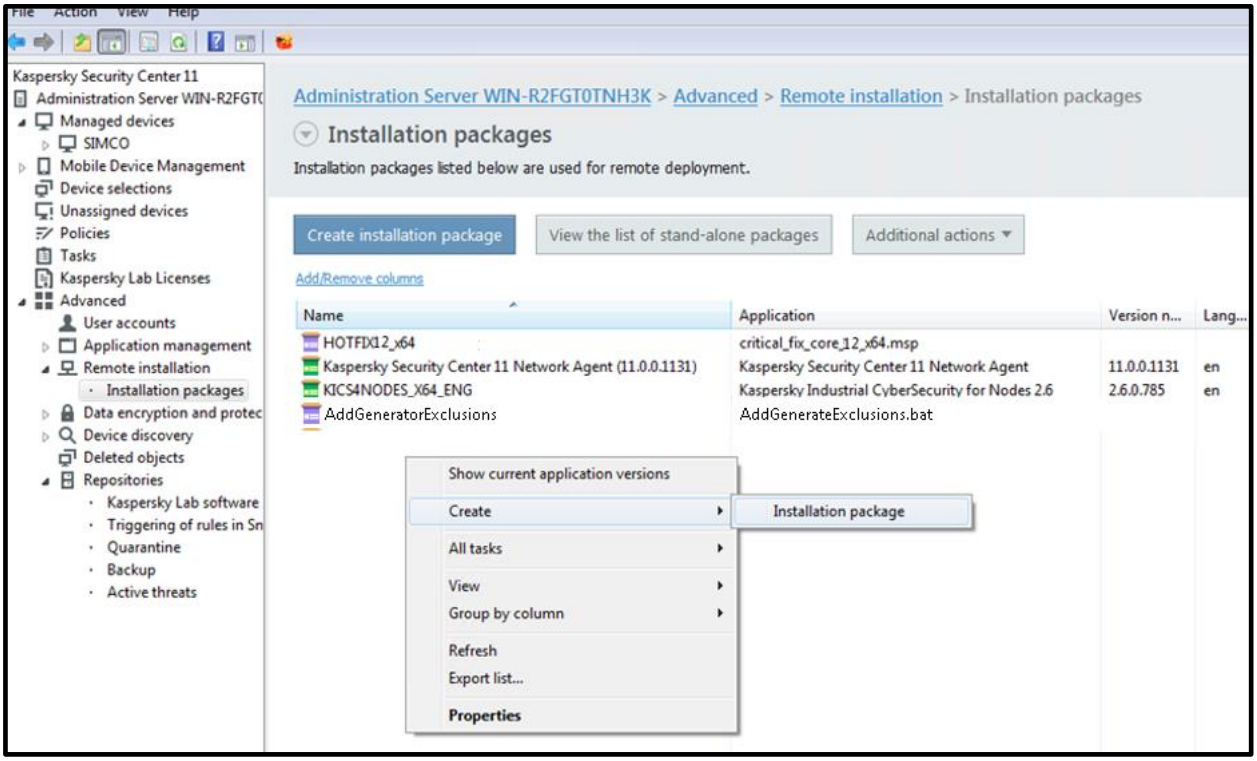
The console is optionally installed on target (managed) computers and it enables local management of a **KICS for Nodes** instance. It might also be useful for local computer diagnostics and troubleshooting.

At the same time, the local management capabilities can be centrally restricted by applying locks on side of the **KSC** policy. Additionally, the mechanism of management console password protection can be activated in order to prevent unauthorized local users from manipulating with **KICS for Nodes** settings (please refer to section “Enabling optional password protection” for details).

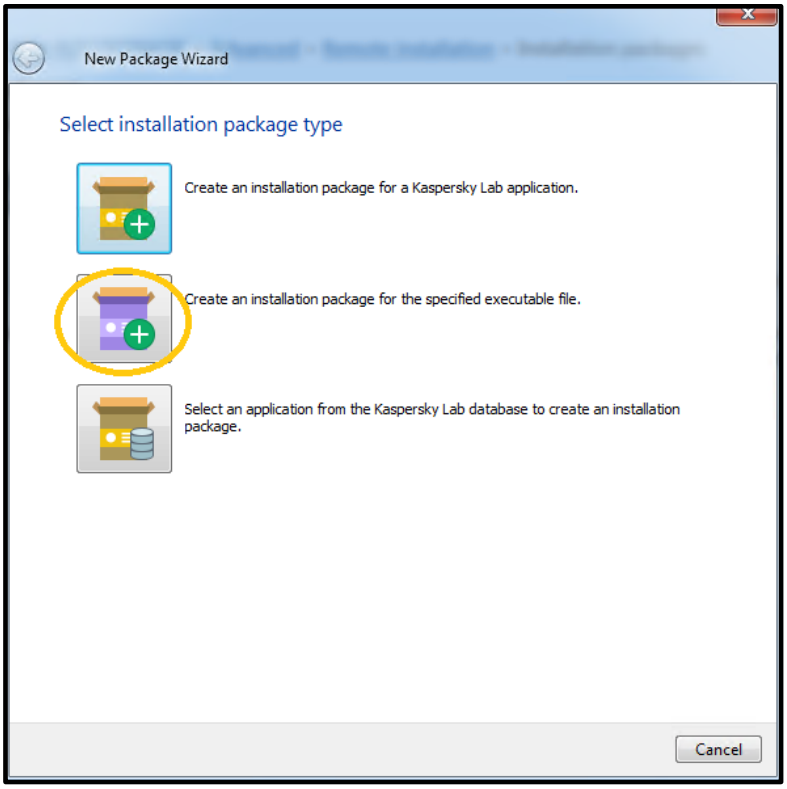
The good thing is that you can install the **KICS for Nodes management console** on one machine and use it to manage a **KICS for Nodes** instance installed on another machine. However, this will require you to open **UDP/TCP 135** ports on both the source and target machines. By default, the console attempts to get connected to the local machine.

In order to install the **KICS for Nodes management console** on a remote node please go through the following steps.

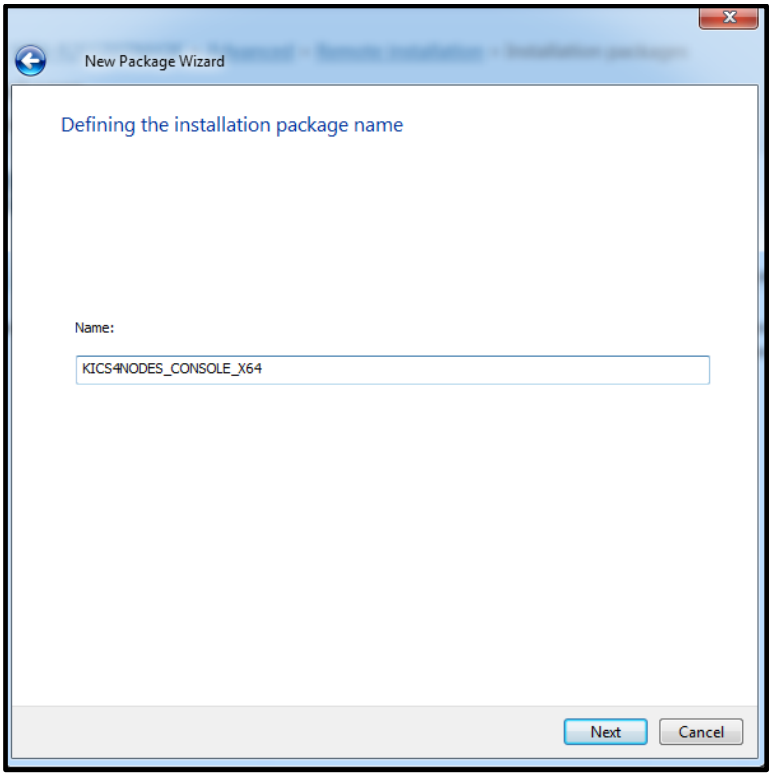
1. Go to **Administration Server->Advanced->Remote Installation**. Right-click on any spare area of the installation packages list. In the context menu choose **Create->Installation package**.



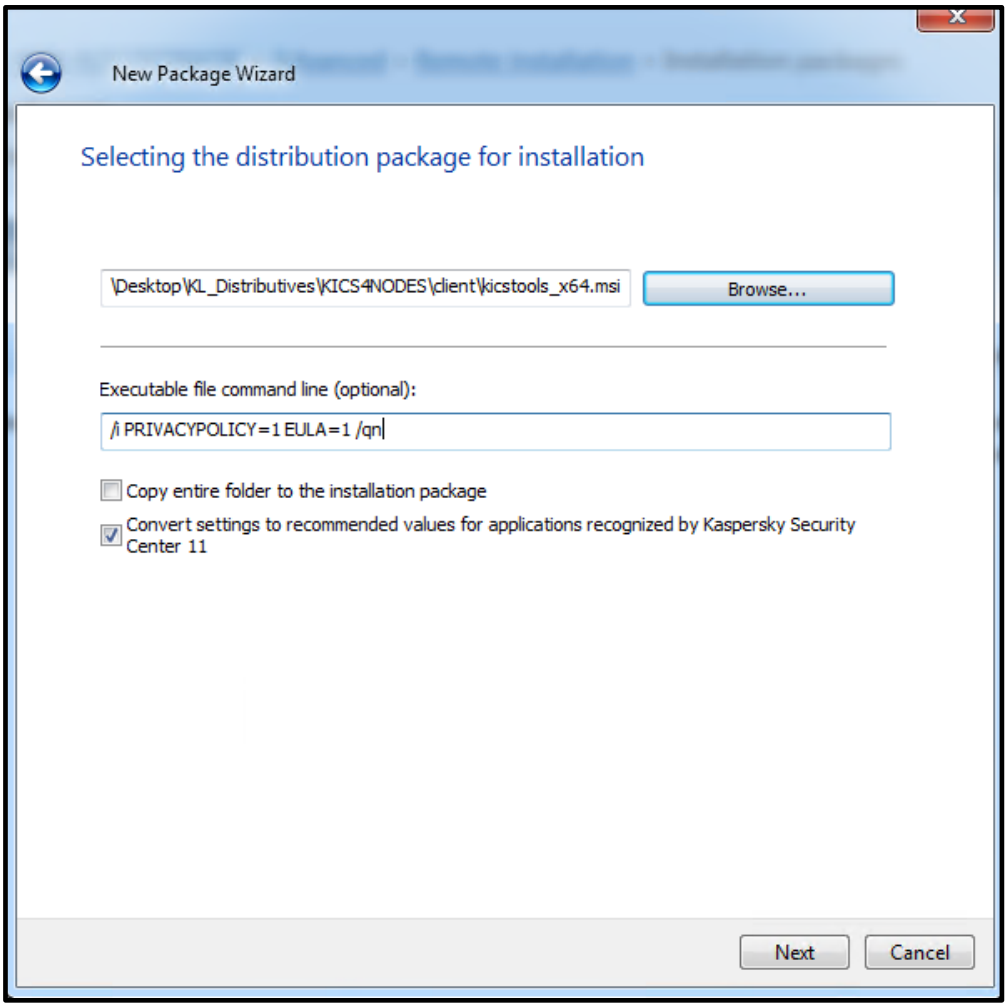
2. In the **Select installation package type** window, click **Create installation package for specified executable file** as shown below.



3. Name this new installation package as **KICS4NODES_CONSOLE_X64**. Click **Next**.

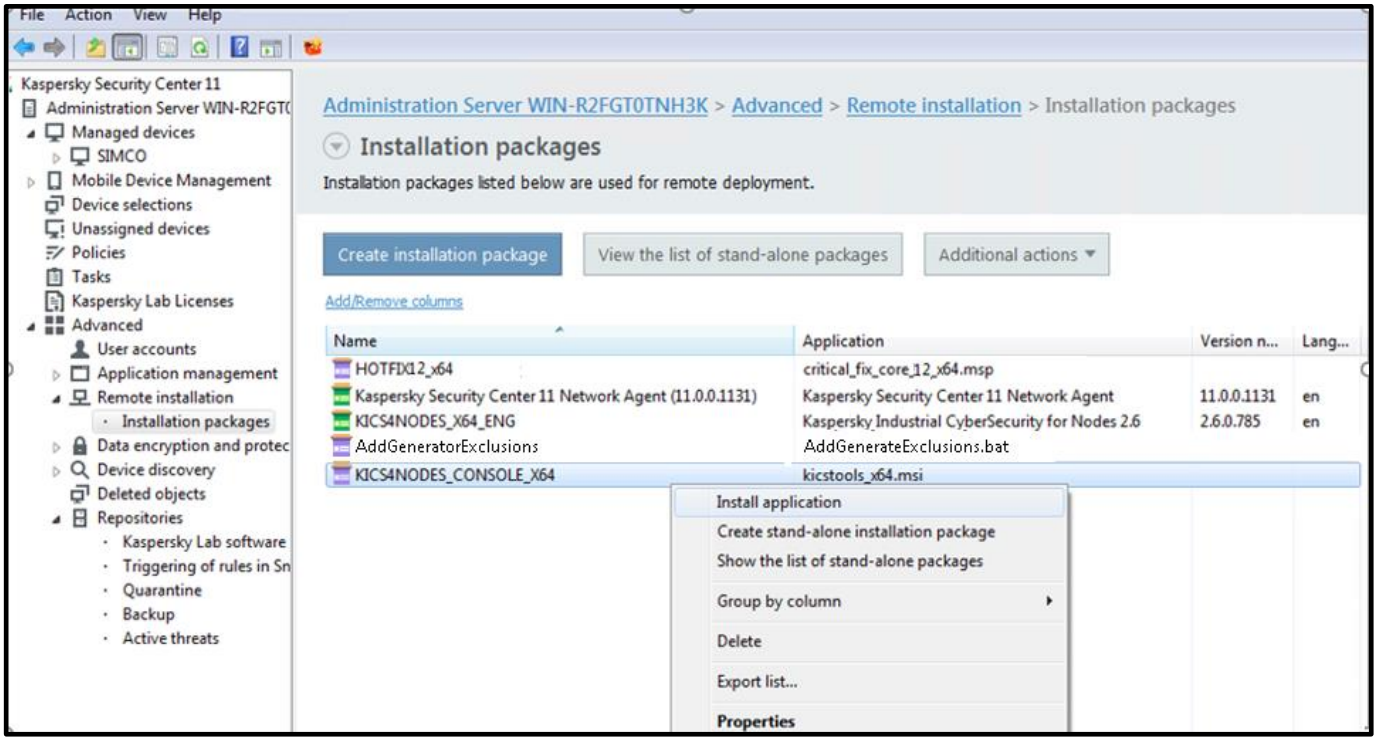


4. In the **Selecting the distribution package for installation** window, browse to the **kicstools_x64.msi** [12]file (supplied as a part of the **KICS for Nodes 2.6** distribution package) and select it. Specify the command line options as shown below. Click **Next**. Then click **Finish** in the finalization window.

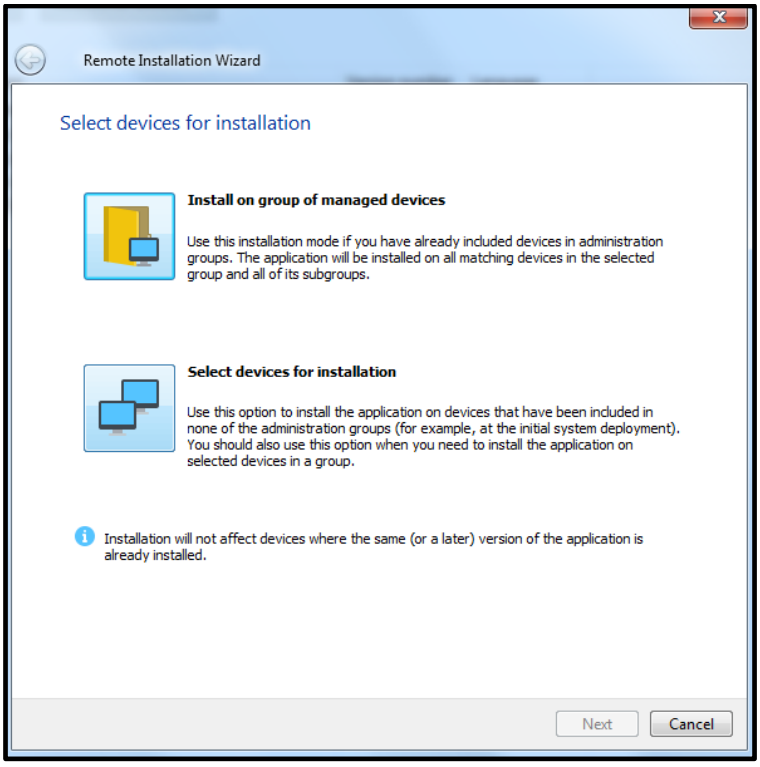


[12] In case of a 32-bit operating system of a target node **kicstools_x86.msi** should be selected

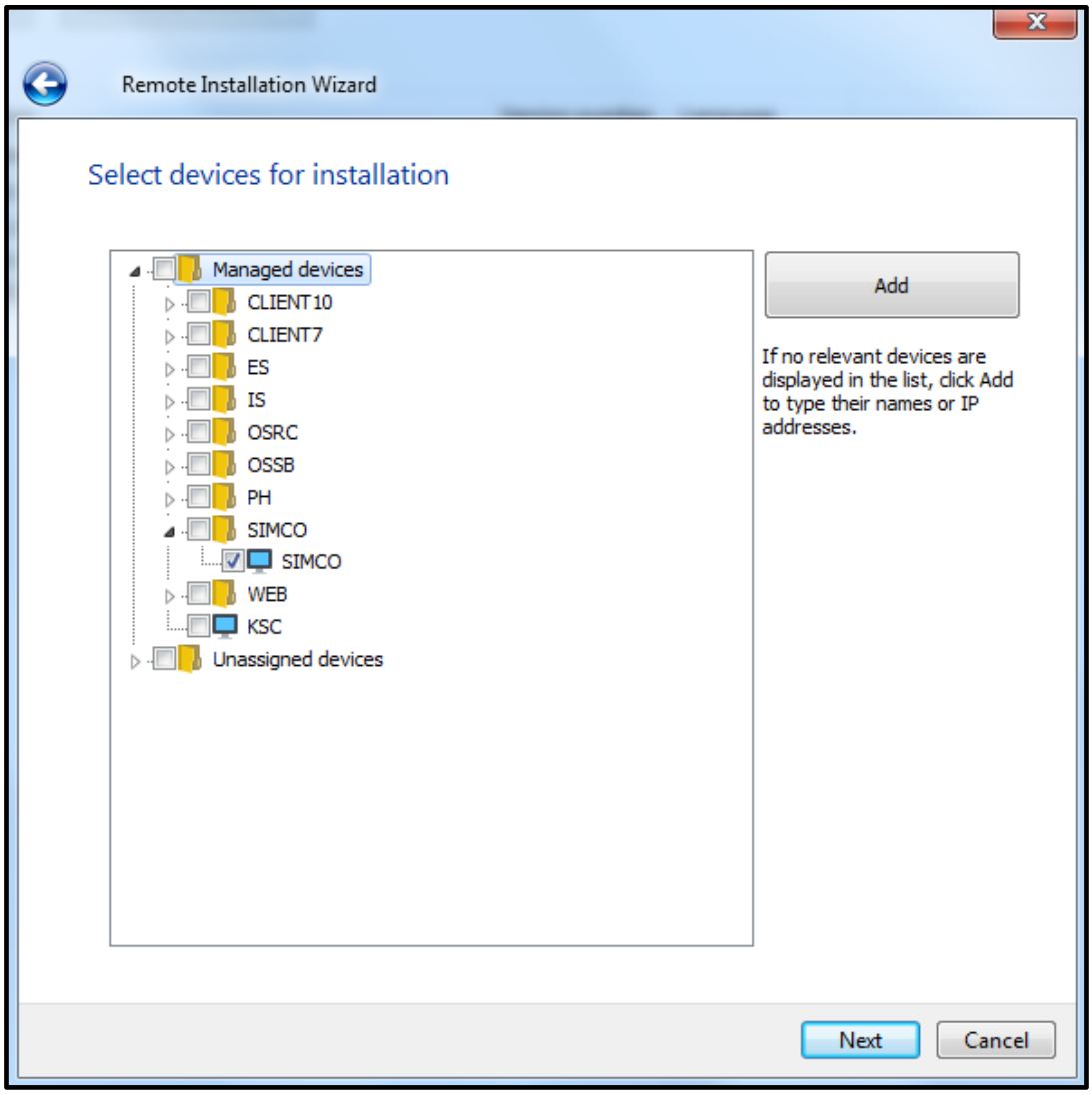
5. Select the just created installation package, right-click it and in the context menu select **Install application** as shown below.



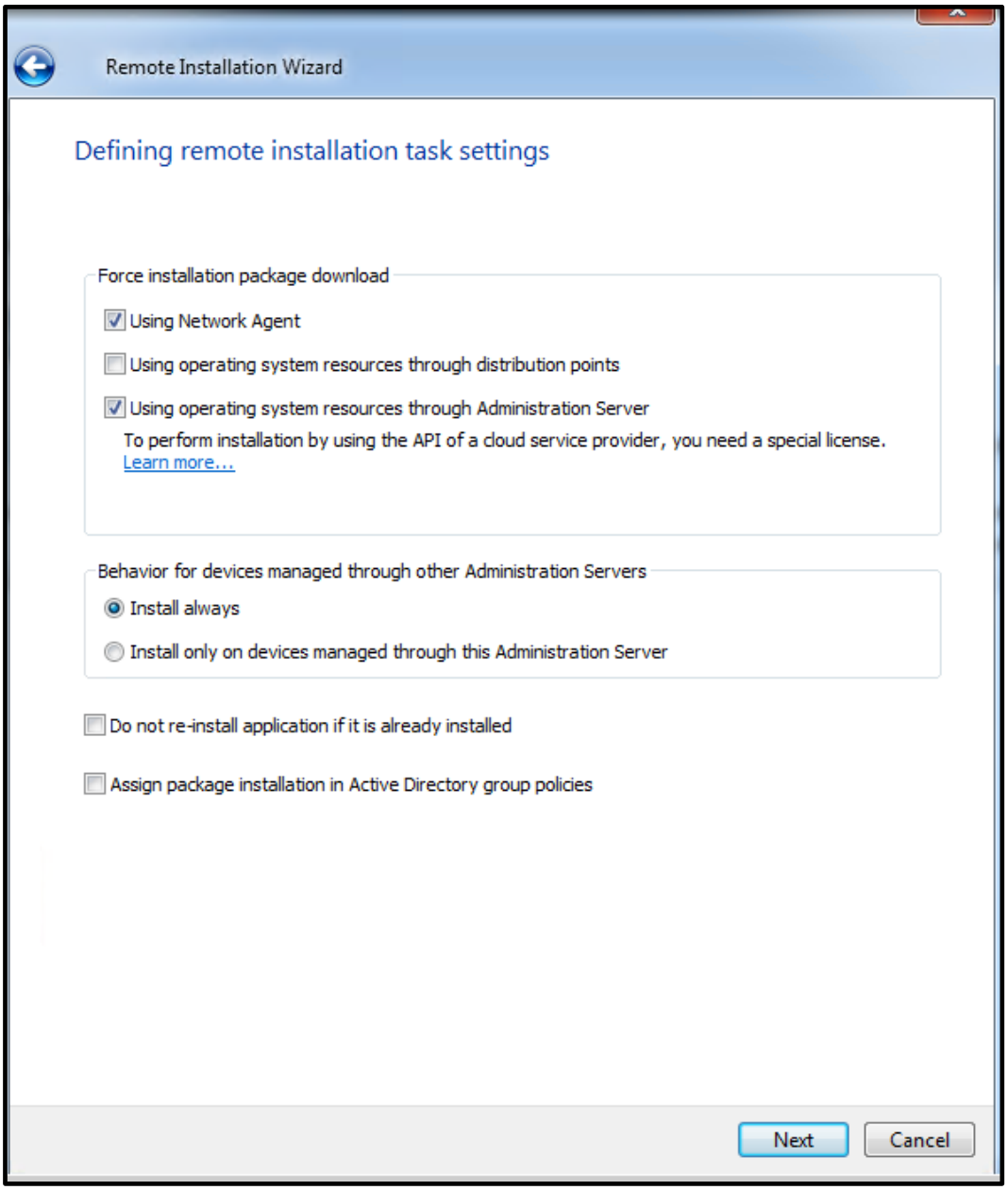
6. In the **Select devices for installation** window, click **Select devices for installation**.



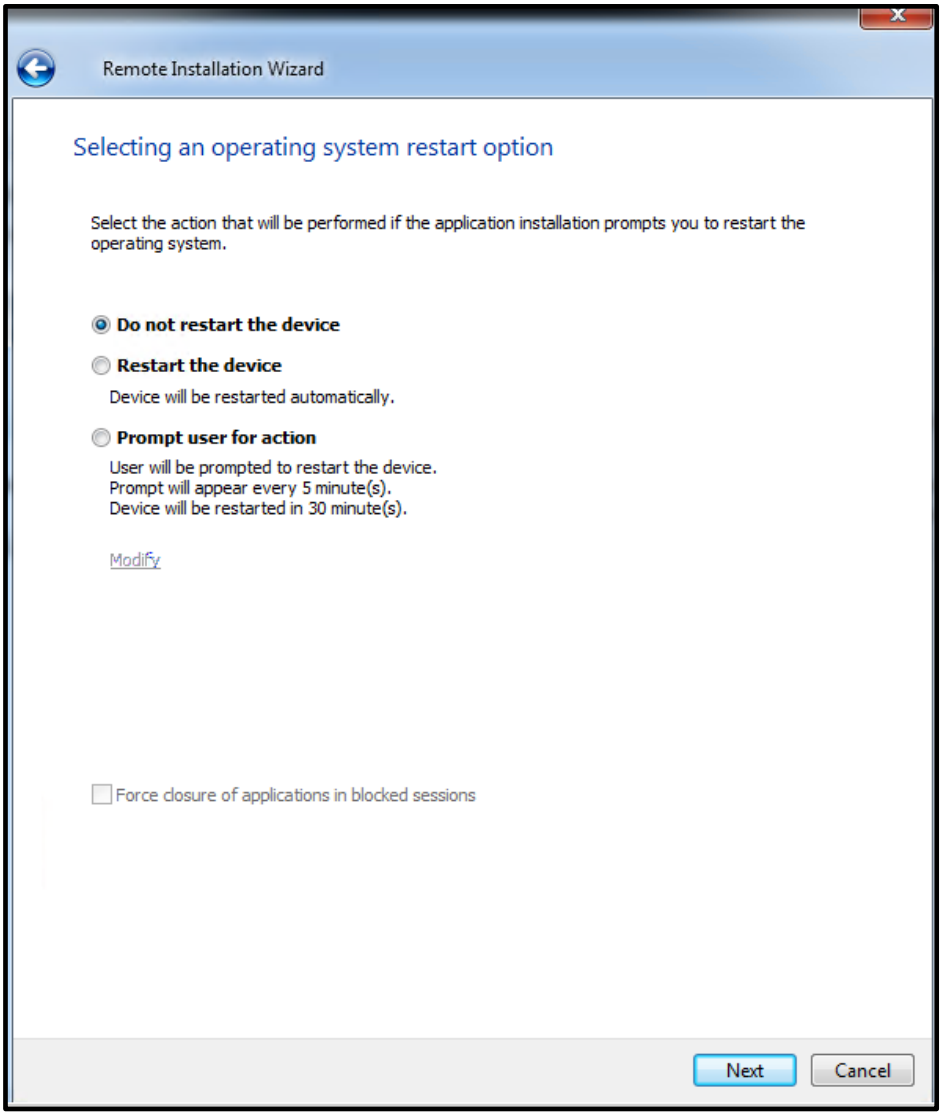
7. Check particular devices for installation. In our case, it will be **SIMCO**. Click **Next**.



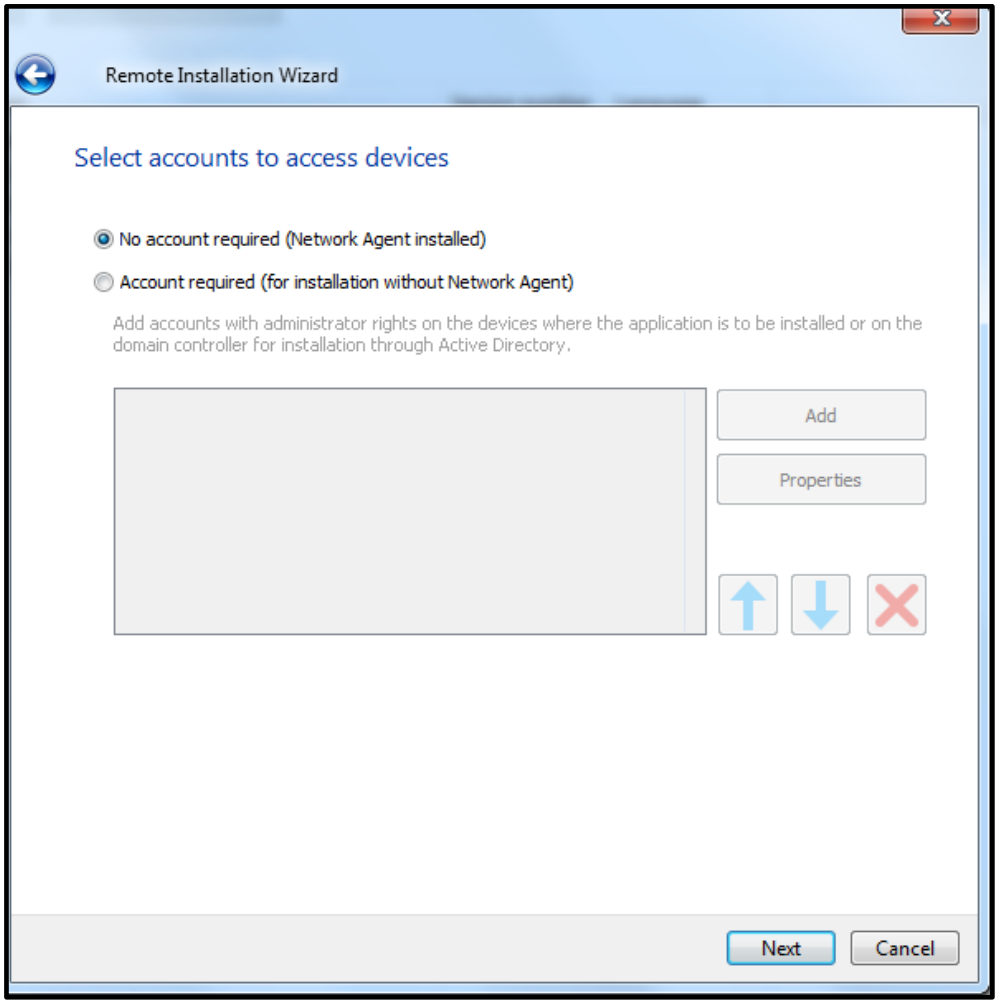
8. In the **Defining** remote **installation task settings** window specify the settings as shown below. Click **Next**.



9. In the **Selecting an operating system restart option** window select **Do not restart the device** and click **Next**.

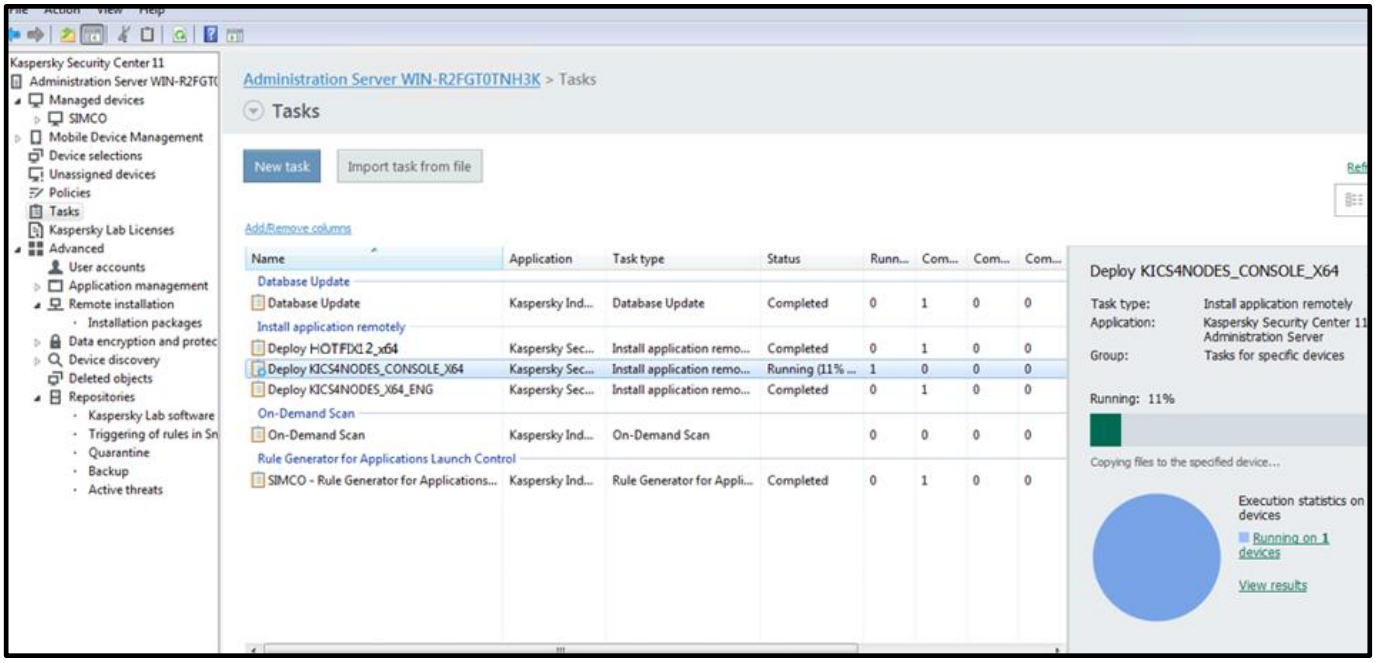


10. In the **Select accounts to access devices** select **No account required (Network Agent installed)**. Click **Next**.



11. In the **Starting installation** windows that follows, click **Next** and finally **Finish**. Actually, we have created the task that will launch **kicstools_x64.msi** on a target host.

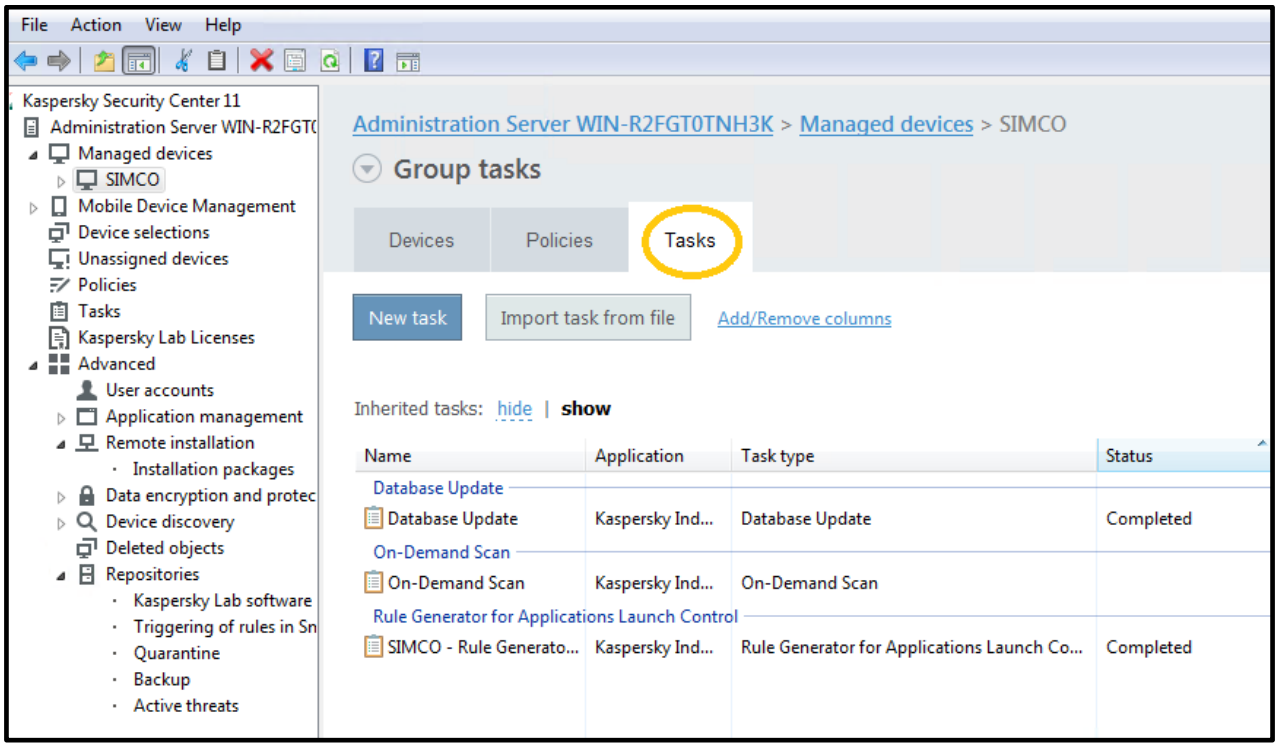
12. Now you are automatically redirected to the **Administration Server->Tasks** node and you can see the just created **Deploy KICS4NODES_CONSOLE_X64** task running. Wait for its completion.



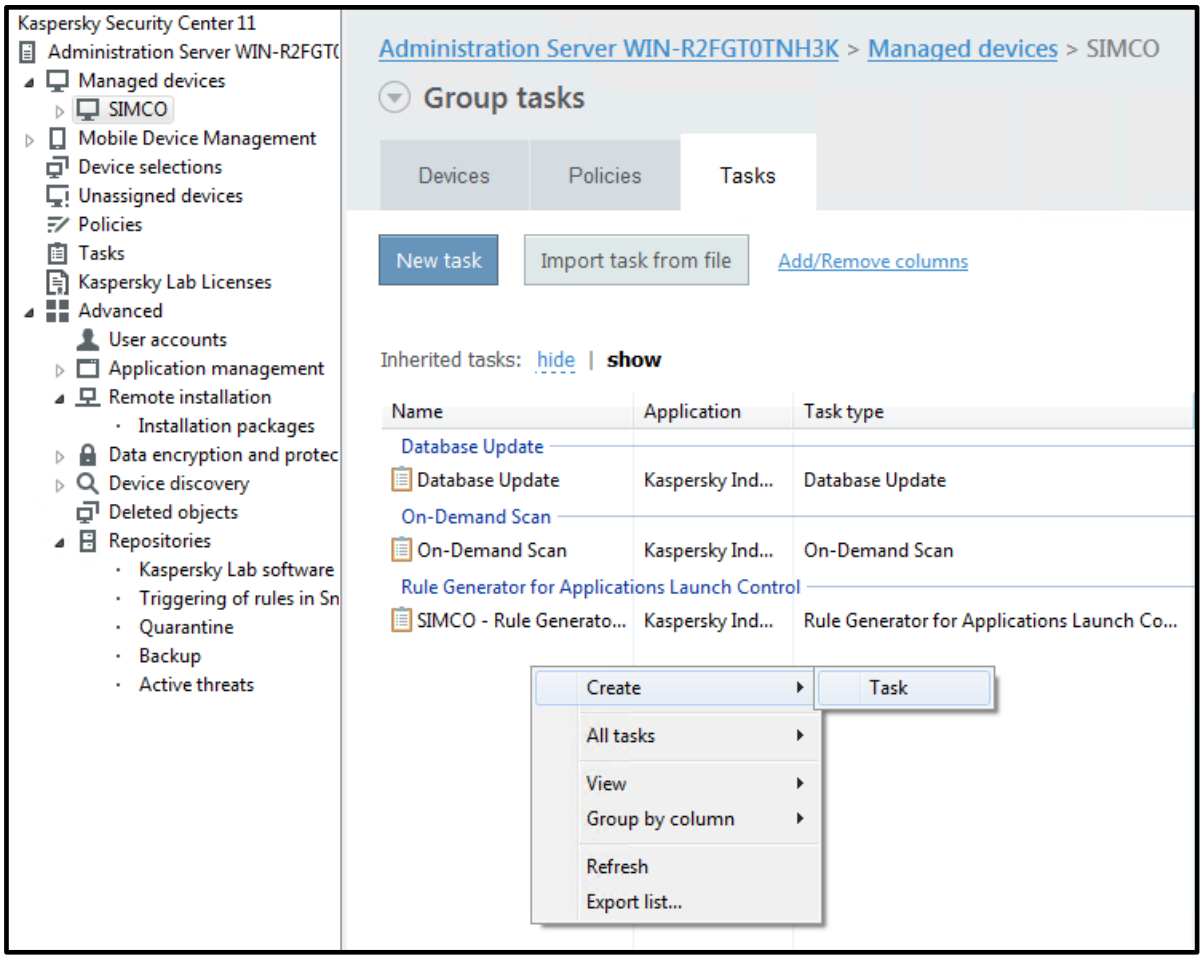
Uninstalling KICS for Nodes and KLnagent

We hope that you will not encounter a situation inducing you to do this. However, if it is necessary you can perform software removal without even having to shut down your control system runtime.
Please perform the following compulsory steps to get the protection software removed from your computer (we are still referring to our **SIMCO** host as an example):

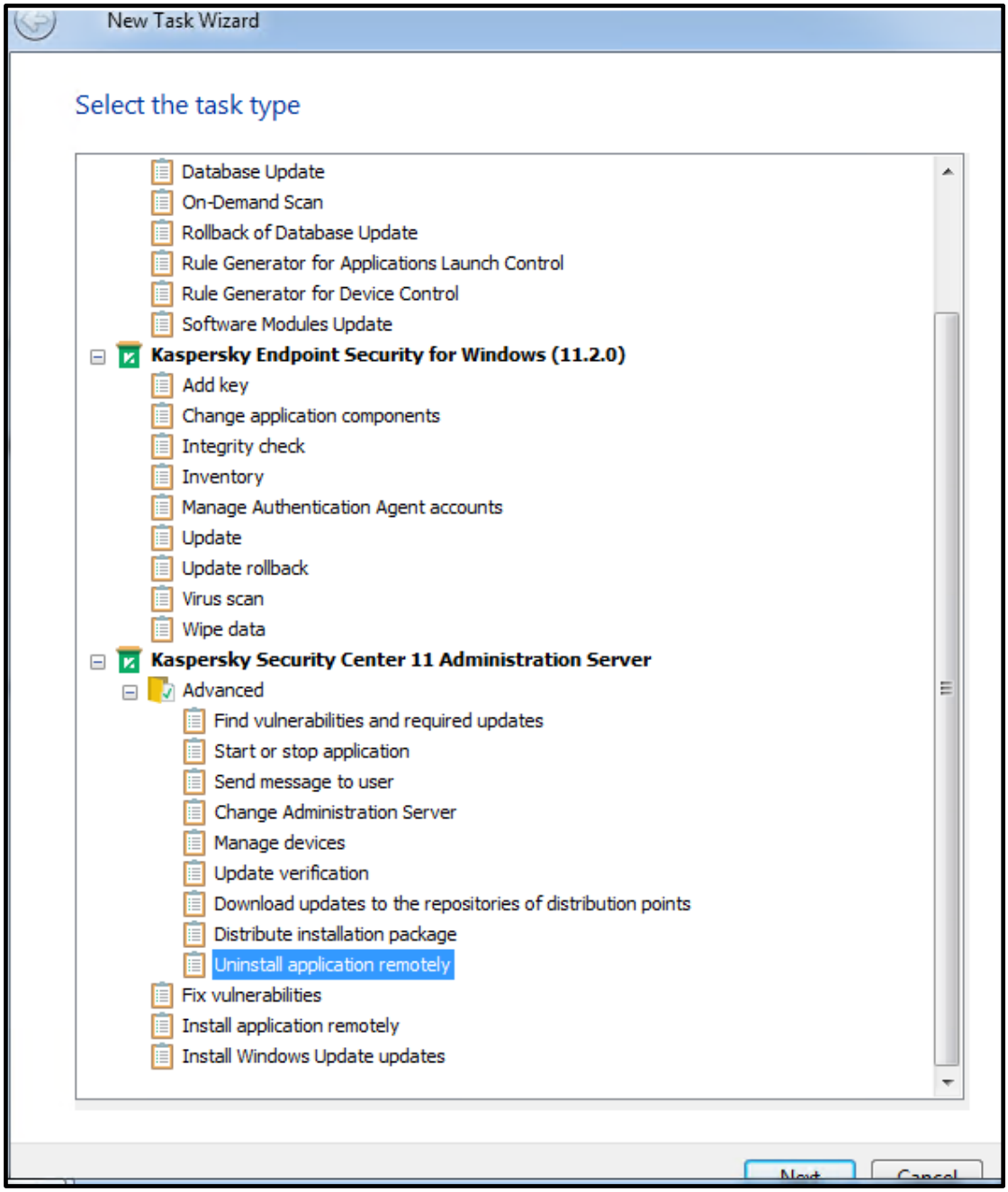
1. Go to the **SIMCO** node and switch to the **Tasks** tab as shown below.



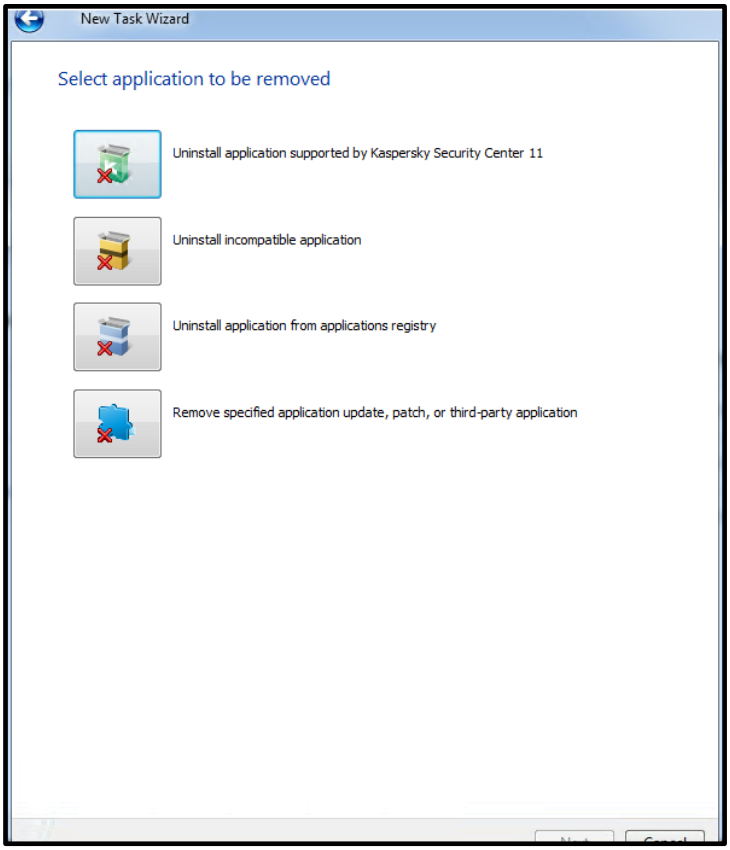
2. Right-click on any spare area of the **Tasks** list; in the context menu choose **Create->Task**.



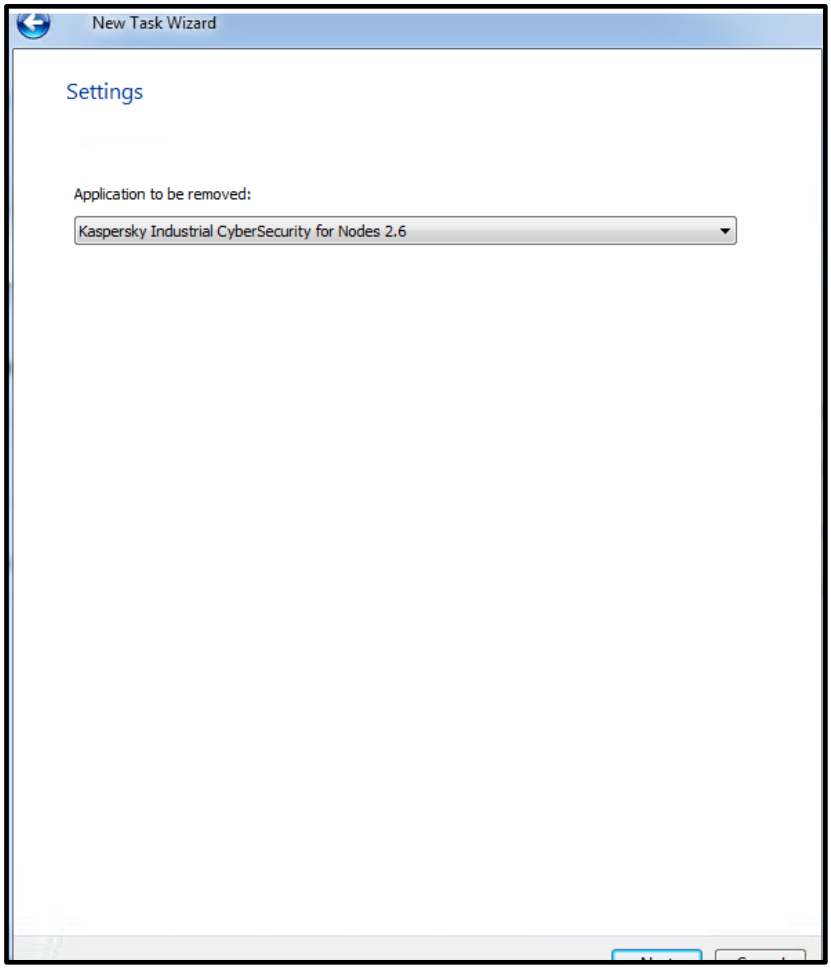
3. In the **New task wizard** window that appears, select **Kaspersky Security Center 11 Administration Server->Advanced->Uninstall application remotely** as shown below. Click **Next**.



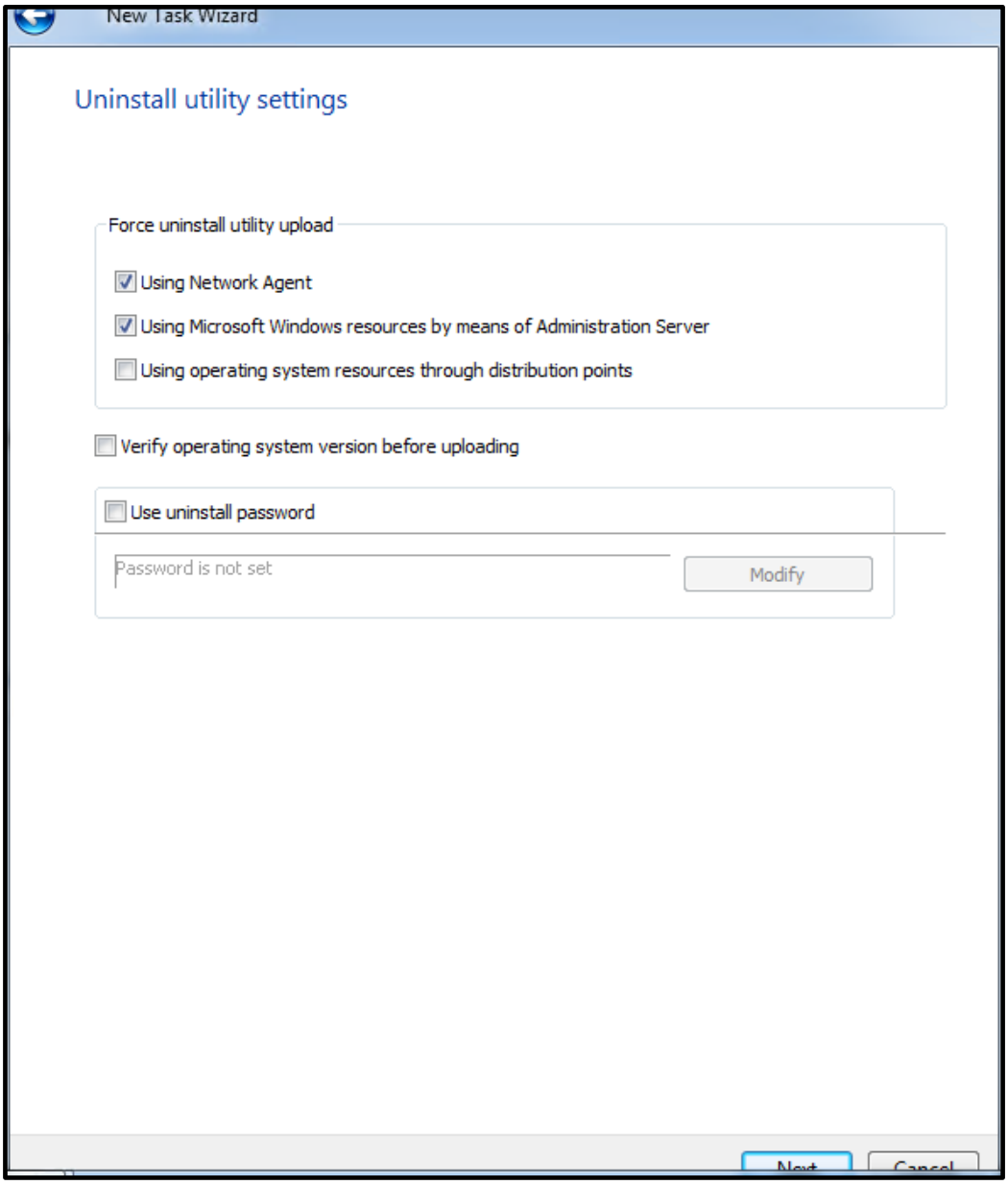
4. In the next window, click **Uninstall application supported by Kaspersky Security Center 11** as shown below.



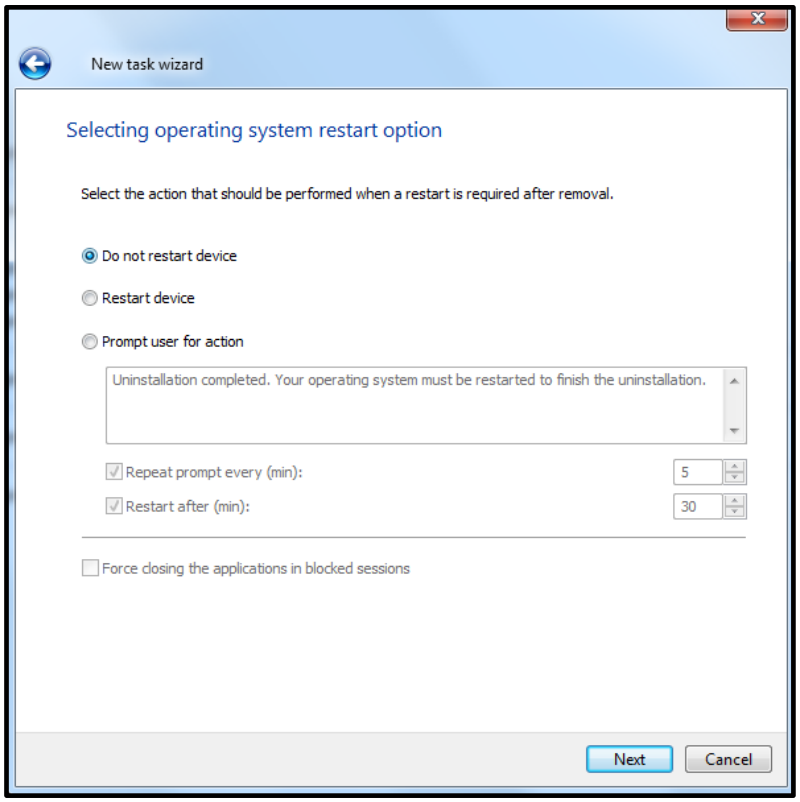
5. In the window that appears, specify **Kaspersky Industrial CyberSecurity for Nodes 2.6** as an application to be removed. Click **Next**.



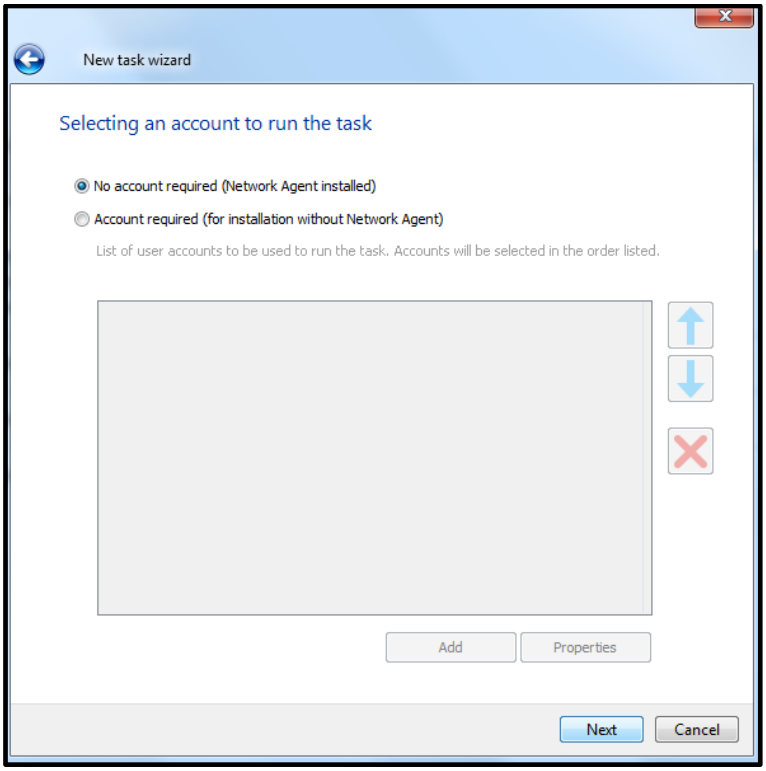
6. In the **Uninstall utility settings** window specify the settings as shown below. Additionally, specify your protection password in the **Uninstall password** field unless you have the password protection disabled (please refer to section “Enabling optional password protection”).



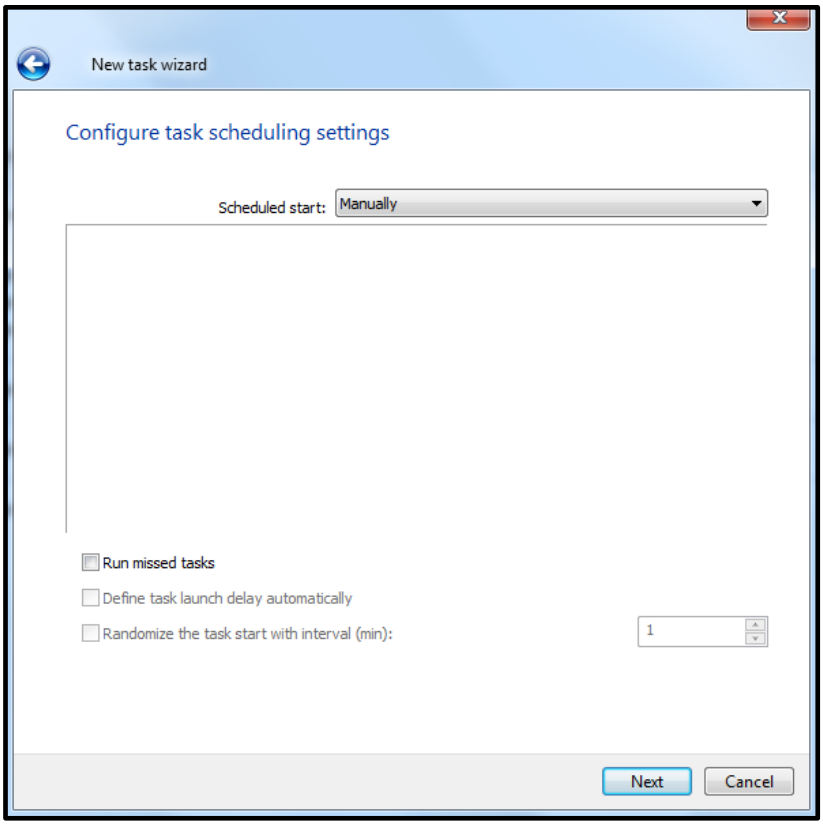
7. In the **Selecting operating system restart option** window specify settings as shown below and click **Next**.



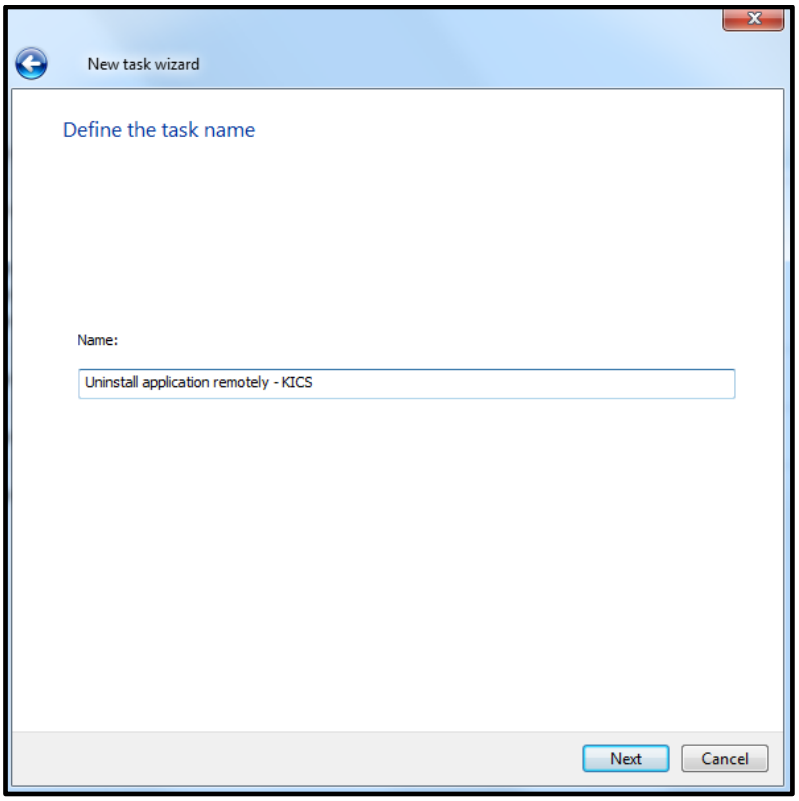
8. In the **Selecting an account to run the task** select **No account required (Network Agent Installed)** as shown below. Click **Next**.



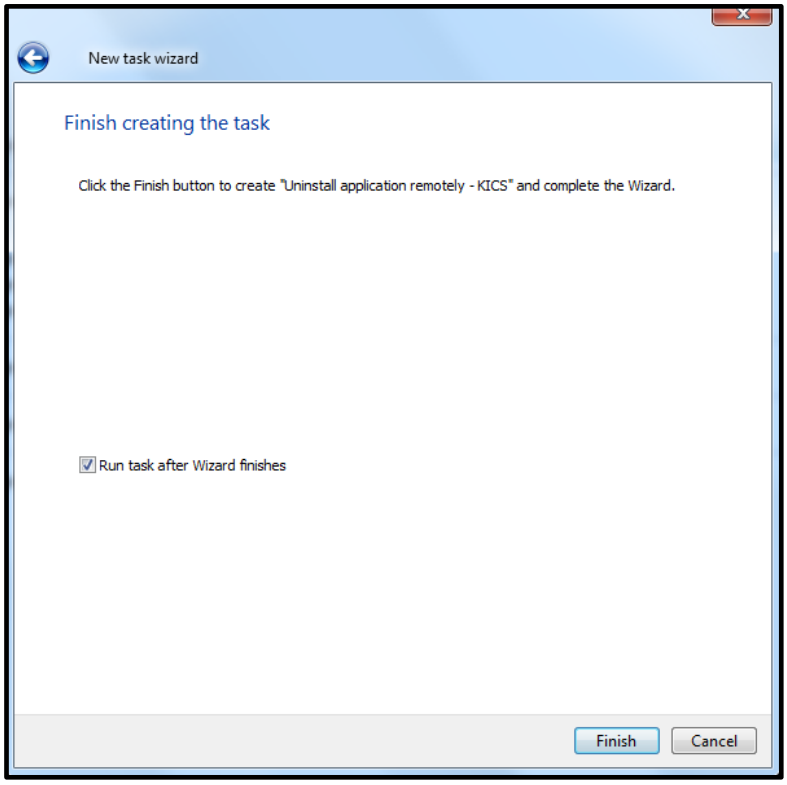
9. In the Configure **task scheduling settings** window specify the settings as shown below. Ckick **Next**.



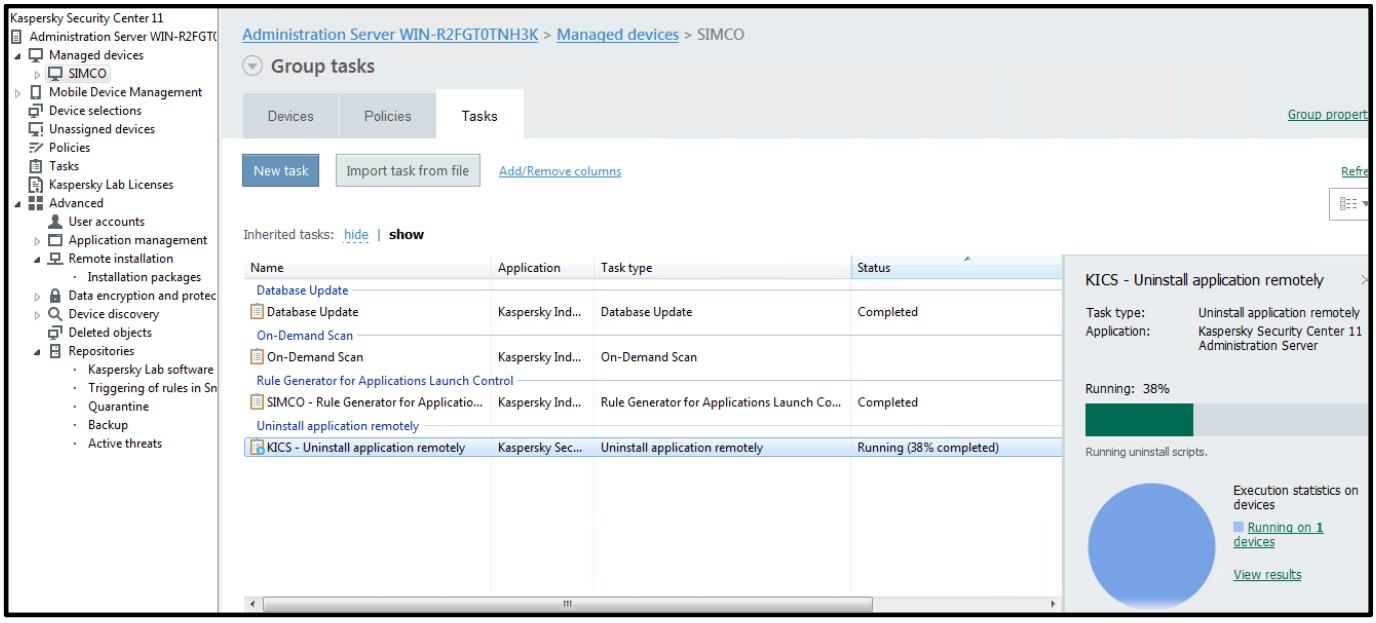
10. Give a name to the task in the following window. Click **Next**.



11. In the Finish **creating the task** window check **Run task after Wizard finishes**. Click **Finish**. This will start **KICS for Nodes** removal immediately.



12. Wait a few minutes until the just created **Uninstall application remotely** task is completed. You can track the progress by observing the progress bar.



13. After you finish uninstalling **KICS for Nodes 2.6**, you may also want to get the management agent **KLnagent** removed from your host (do not uninstall **KLnagent** prior to **KICS for Nodes 2.6**!). In order to get **KLnagent** uninstalled, please perform exactly the same sequence of operations as was described in steps **1-11**.

It is also possible to uninstall **KICS for Nodes** from a computer locally (without operating from **KSC**). Please mind the following nuances in order to get it done:

- **Do not** initiate software removal via Windows **Control Panel-> Programs and Features**!
- Instead, go to the **Start** menu and find the **Modify or Remove Kaspersky Industrial CyberSecurity for Nodes 2.6** shortcut.
- Run **Modify or Remove Kaspersky Industrial CyberSecurity for Nodes 2.6** as administrator.
- Follow all the hints and tips of the uninstallation wizard; they are intuitively clear.
- If you have enabled password protection, you will be required to enter this password to authorize software removal.

FSTEK certification for KICS for Nodes installations within the territory of Russia

FSTEC of Russia forms a federal executive authority implementing national policy, organizing interdepartmental coordination and interaction, and exercising special and control functions in the sphere of state security including information security. The **FSTEK** directives and guidelines are solely valid within the territory of the Russian Federation.

As per **FSTEK** guideline there is a certain category of productions sites (commonly referred to as “critical infrastructure”) that require the compulsory certification of any cybersecurity software for compliance with the **FSTEK** requirements. Plant owners, production executives or security officers are surely aware whether the production area entrusted to them falls under the **FSTEK** regulation. If it is a case, only the certified version of **KICS for Nodes** must be used, which implies that **NO Hotfixes** must be installed on top of the **KICS for Nodes release version (2.6.0.785)** whatsoever.

The corresponding **FSTEK** certificates and compatibility statements can be downloaded from the following web-location: https://support.kaspersky.ru/common/certificates/14567

Recommendations

In order to ensure sufficient reliability and security of your control system operating in conjunction with **KICS for Nodes 2.6**, the following recommendations and prerequisites may be considered:

- Prior to installing **KICS for Nodes,** it is required to remove any other antivirus software from your computer.
- Simultaneous operation of **KICS for Nodes** and **Windows Defender** should be avoided. Please follow the given link to learn how to disable **Windows Defender** permanently https://answers.microsoft.com/en-us/insider/forum/insider_wintp-insider_security/how-to-disable-windows-defender-in-windows-10/b834d36e-6da8-42a8-85f6-da9a520f05f2 (this should only be done if **Windows Defender** remains active despite **KICS for Nodes** installation).
- **KICS for Nodes Firewall management** should not be installed. Alternatively, it is recommended to rely on properly configured **Windows Firewall**.
- After setting **Application Launch Control** to the **Statistics only** mode, it is required to perform a limited time trial run involving regular process supervision and engineering operations on DCS. This documented technique ensures enhanced discovery of dynamically created executable files that did not exist while **the Generate Rules for Application Launch Control** task was executed. Generally, the trial run period must not be less than 12 hours but you can make “fine tuning” of **Application Launch Control** a lot easier by rebooting your computer (as long as it is practically possible). If you encounter any alerted file launches (providing that these files are legitimate), you should add them to the existing white list by looking into **KSC Administration Server->Events**. To get a hint on how to feed **Application Launch Control** with previously unseen executables, please refer to the similar technique described in “Setting up Device Control whitelisting”.

- Although we have never encountered it in practice, some minor probability remains that new virus definitions might affect the operability of the legitimate control system software. Therefore, it is recommended that you should check even minor anti-virus updates on a simulation platform prior to deploying them onto operational workstations or should, at least, first validate such updates on a standby workstation leaving a redundant partner intact throughout such validation (in case of fault-tolerant DCS architecture).
- It is recommended to avoid launching the **Update antivirus databases** task on every DCS station at the same time. The best solution is to adhere to consecutive updates carried out under strict supervision on a host-by-host basis. The same advice is relevant to the **On-demand scanning** and **Find vulnerabilities tasks**.
- Such tasks as **Update antivirus databases, On-demand scanning** and **Find vulnerabilities** obviously consume additional computational resources while they run. That is why these tasks should only be started manually and their execution should be closely supervised. Avoid scheduled or automatic execution of these “heavy duty” tasks!
- Prior to putting your USB device on the **Device Control** white list, we suggest that you do its anti-virus scanning (by using the **On-demand scanning** task, for example).
- It recommended assigning a static IP-address to your **Kaspersky Security Center** machine. When it comes to **KICS for Nodes** configuration, it is also advised to operate with explicit IP-addresses (whenever possible) instead of using domain or NetBIOS names.
- As of the date we are revising this document, **Hotfix 12** is the most recent version. Unless you face the **FSTEK** restrictions pointed out in “**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia”, in all other cases we strongly recommend using **Hotfix 12** and no other version (even if a newer **Hotfix** version has come out).
- If you are induced to follow the **FSTEK** certification requirements and therefore have not installed any product **Hotfixes**, you must **NOT** activate **Application Launch Control** on the engineering workstation (that is normally the one that contains **Simatic Manager**). The protection module can still be enabled on any other workstation or server without any restrictions.

kaspersky

www.kaspersky.com/

www.securelist.com