

kaspersky

How to integrate Kaspersky Industrial CyberSecurity 3.0 into common process control infrastructure

Step-by-step installation and configuration guide

08.11.2021

Contents

What this document is about	2
Who would find this document useful	2
What is KICS.....	2
KICS software components	2
Distribution package composition	4
System requirements	5
Installation and configuration steps	6
Installation of KSC on a management PC	6
Initial configuration of KSC	14
Remote installation of KLnagent onto target computers	25
Installation of the KICS for Nodes management plugin	34
General configuration of the security policy for KLnagent	36
Configuring KICS for Nodes instances	39
Import of the generic policy for KICS for Nodes	40
Settings of KICS for Nodes generic policy	43
Remote installation of KICS for Nodes onto target computers via KLnagent	52
Remote installation of Hotfix onto target computers via KLnagent	65
Initial update of antivirus databases	72
Performing On-Demand Scanning on target hosts	87
Execution of the Generate Rules for Application Launch Control task	95
Setting up Application Launch Control whitelisting	102
Setting up Device Control whitelisting	105
Setting up Network Threat Protection	111
Setting up File Integrity Monitor	113
Setting up PLC Integrity Checker	113
Enabling optional password protection	123
Installing optional KICS for Nodes management console	125
Uninstalling KICS for Nodes and KLnagent.....	132
FSTEK certification for KICS for Nodes installations within the territory of Russia	138
Recommendations	139

What this document is about

This document provides detailed instructions on how to install and configure **Kaspersky Industrial CyberSecurity 3.0** in accordance with the most common requirements of the process control infrastructure. It will guide you through several sequential steps of the product installation and its subsequent configuration.

Who would find this document useful

The following audience may find the document interesting:

- Specialists involved in industrial cybersecurity.
- Process operating staff.
- Automation system or process control 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**. It enables robust protection of automatic control systems against a broad variety of cybersecurity threats, whether they are known or “zero-day”. The solution 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 referred to as **KSC**). It is an administration tool, which enables management of the **KICS** components in a centralized and user-friendly manner.

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

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

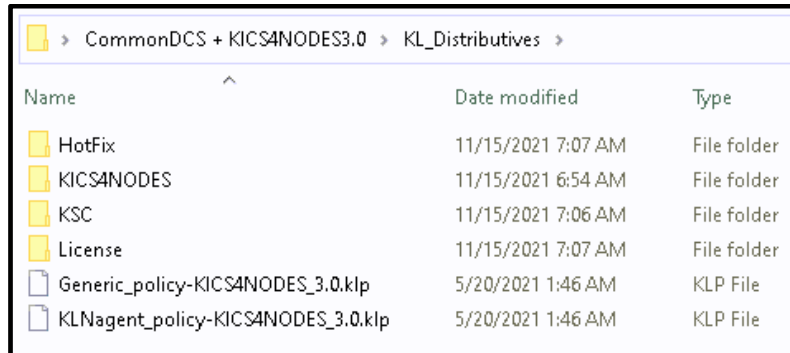
- **Application launch control.** It restricts the execution of files and scripts according to the user-defined white list.
- **Device control.** It restricts the connection of peripheral devices to the protected host. It solely deals with USB-interface storage devices such as USB memory sticks, USB 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 an on-demand search for malicious objects in locations specified by users.
- **Virus database updater.** It is essential for keeping the anti-virus database up to date.
- **Untrusted host blocker.** It blocks the network access to shared folders from the side of those remote hosts that show malicious activity.
- **Anti-cryptor.** It prevents malicious encryption activities. 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.** **KICS for Nodes 3.0** 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 the consistency of a control program, executed by the monitored PLC. It reacts to any modification of a process control algorithm. At present, this module supports **SIMATIC S7-300**, **S7-400(H)**, **MODICON M340** and **MODICON M580** series controllers.
- **Network Attack Blocker.** It can be regarded as a host-based **IPS**. Its operation is based on regularly updated patterns of network attacks. The module is able to function either in the active mode or notification-only mode.

Please note, that the **Firewall management** feature, also provided by **KICS for Nodes 3.0**, 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 configuration techniques.

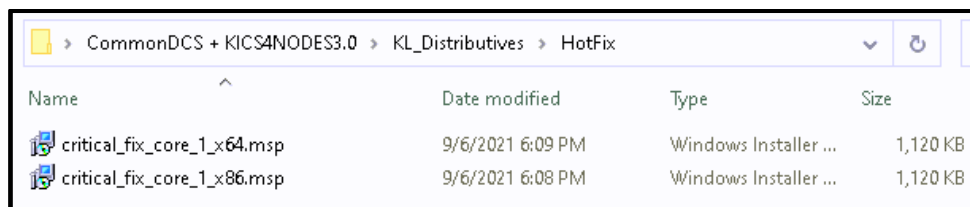
Distribution package composition

Prior to starting the product installation, please check the contents of the **KICS for Nodes** distribution package and make sure you have obtained all the necessary files. The distribution package, as a rule, includes the following items.



Name	Date modified	Type
HotFix	11/15/2021 7:07 AM	File folder
KICS4NODES	11/15/2021 6:54 AM	File folder
KSC	11/15/2021 7:06 AM	File folder
License	11/15/2021 7:07 AM	File folder
Generic_policy-KICS4NODES_3.0.klp	5/20/2021 1:46 AM	KLP File
KLNagent_policy-KICS4NODES_3.0.klp	5/20/2021 1:46 AM	KLP File

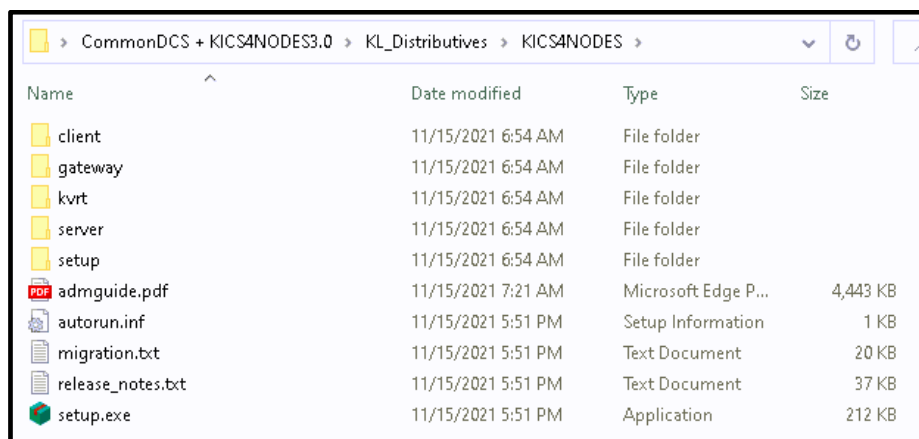
The **HotFix** folder is optional. If it exists, it contains the most recent **Hotfix** for **KICS for Nodes 3.0** that has successfully been tested for compatibility with your model/version of the control system. The **Hotfix** may contain critical patches and in most cases its installation is compulsory¹.



Name	Date modified	Type	Size
critical_fix_core_1_x64.msp	9/6/2021 6:09 PM	Windows Installer ...	1,120 KB
critical_fix_core_1_x86.msp	9/6/2021 6:08 PM	Windows Installer ...	1,120 KB

The **KICS4NODES** folder contains the **KICS for Nodes 3.0** installation files as well as **KICS for Nodes 3.0** administrator's guide. The **client** subfolder contains the **KICS for Nodes 3.0 management console**. The installation of **KICS for Nodes 3.0 management console** is optional though. The **server** folder contains the **administration plugin for KSC**.

You can view the online version of the **KICS for Nodes** manual at <https://support.kaspersky.com/KICS4Nodes/3.0/en-US/147896.htm>



Name	Date modified	Type	Size
client	11/15/2021 6:54 AM	File folder	
gateway	11/15/2021 6:54 AM	File folder	
kvrt	11/15/2021 6:54 AM	File folder	
server	11/15/2021 6:54 AM	File folder	
setup	11/15/2021 6:54 AM	File folder	
admguide.pdf	11/15/2021 7:21 AM	Microsoft Edge P...	4,443 KB
autorun.inf	11/15/2021 5:51 PM	Setup Information	1 KB
migration.txt	11/15/2021 5:51 PM	Text Document	20 KB
release_notes.txt	11/15/2021 5:51 PM	Text Document	37 KB
setup.exe	11/15/2021 5:51 PM	Application	212 KB

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



The **KSC** folder contains the **Kaspersky Security Center** installation package (version 13.1). The **KSC** product manuals are available online at <https://support.kaspersky.com/KSC/13/en-US/5022.htm>

Name	Date modified	Type	Size
 ksc_13_13.1.0.8324_full_en.exe	11/15/2021 6:56 AM	Application	442,022 KB

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

 License	15.04.2019 13:02	File folder
 572BFFDC.key		

The **Generic_policy-KICS4NODES_3.0.klp** file is a preconfigured set of security settings specific to your particular model and version of the control system. These predefined settings, optimized by **Kaspersky** experts as a result of a compatibility research, significantly facilitate the **KICS for Nodes** deployment process. The similar file (**KLNagent_policy-KICS4NODES_3.0.klp**) aids the **KLNagent** configuration. These files are utilized by **KSC**.

 Generic_policy-KICS4NODES_3.0.klp	5/20/2021 1:46 AM	KLP File
 KLNagent_policy-KICS4NODES_3.0.klp	5/20/2021 1:46 AM	KLP File

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/13.1/en-US/96255.htm>.

Every to-be-secured station, hosting **KICS for Nodes**, should be compliant with the system requirements as specified in <https://support.kaspersky.com/KICS4Nodes/3.0/en-US/175048.htm>.

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 protected 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**). Please note that the stand-alone installation of **KICS for Nodes** is not overviewed here because it is hardly a suitable option to build up a highly-scalable, easy-to-maintain solution.

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 for **KSC**.
- Import of the security policy for the network agent **KLnagent** from a file.
- Import of the DCS-specific security policy for **KICS for Nodes** from a file.
- Remote installation of **KICS for Nodes** onto target computers via **KLnagent**.
- Remote installation of the provided **Hotfix**² onto target computers via **KLnagent**. Please note that in some specific cases no **Hotfix** should be installed at all and this deployment step should be omitted. Please refer to the section “FSTEK certification for KICS for Nodes installations within the territory of Russia”.
- Optional remote installation of **KICS for Nodes management console**.
- Initial update of antivirus databases.
- Starting up the **On-Demand virus scan** task to inspect target computers.
- Setting up **Application Launch Control** and **Device Control** whitelisting and fine-tuning the DCS-specific security policy.
- Optional configuration of **PLC Integrity Checker** providing that there are supported **PLCs** available on your production site.

Installation of KSC on a management PC

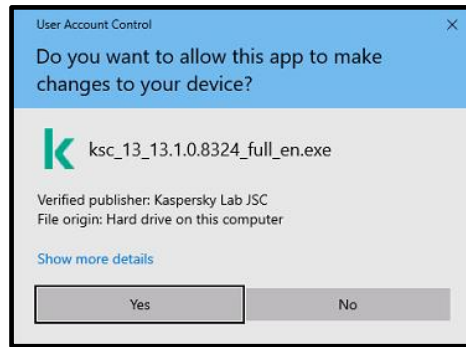
The **KSC** deployment is preceded by the installation of **MS SQL Server 2016 Express Edition** or a later version (for small and medium-size control systems including less than 100 nodes). The **MS SQL** installer is available at https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-52470555DB90/ENU/SQLEXPRESS_x64_ENU.exe. However, for the larger systems we recommend installing full functional **MS SQL Server**.

Please perform the following operations:

1. Log in on your **KSC** computer using an account with administrative privileges.

² As of the date we are revising this document, **Hotfix 3** is the most recent version. However, we strongly recommend that you use the **Hotfix** which was supplied to you as a part of the installation package (and no other version), even if a newer **Hotfix** version has come out.

2. Install **MS SQL Server Express Edition** or **MS SQL Server** depending on your system scale. Follow Microsoft installation guideline.
3. Copy **ksc_13_13.1.0.8324_full_en.exe** from the supplied distribution package to the desktop and launch it as administrator.
4. Acknowledge the file execution if requested.



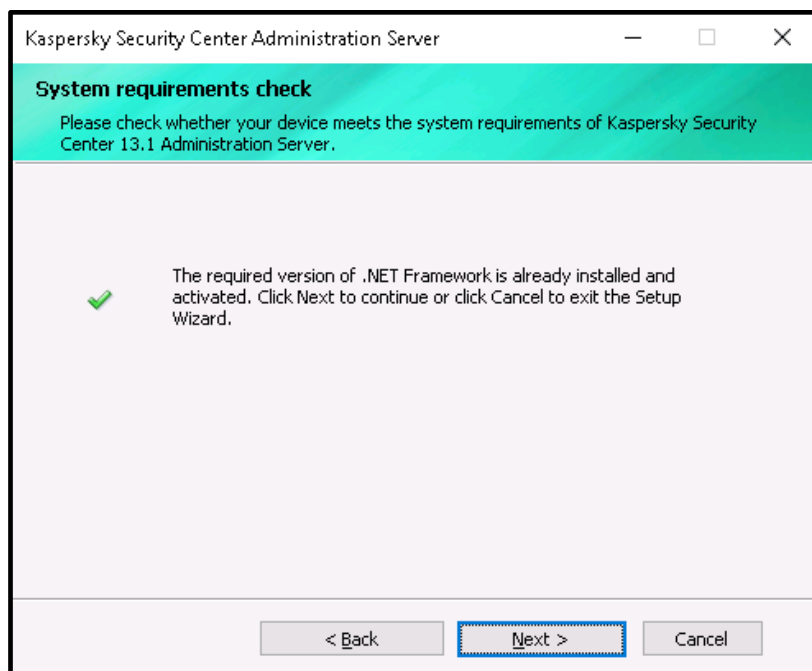
5. The following component selection window should pop up.



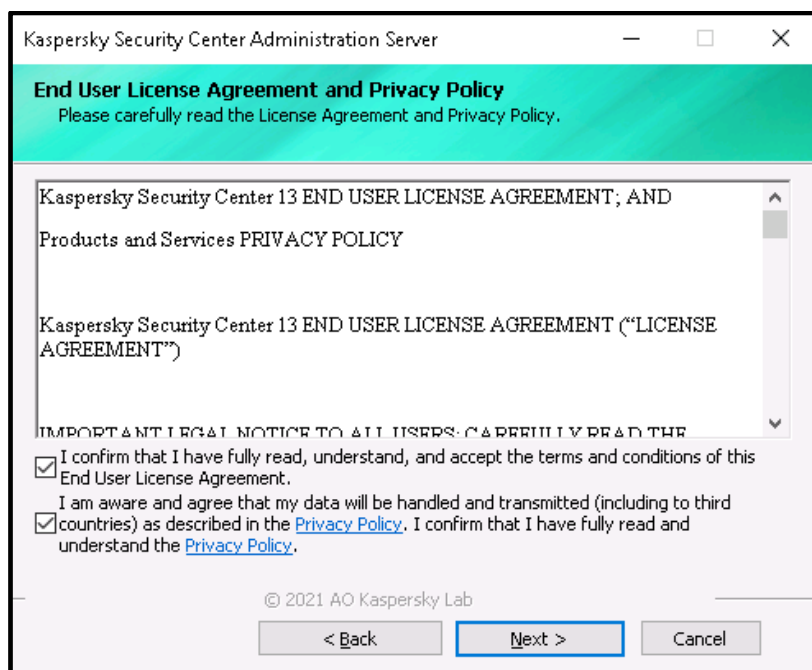
6. Choose **Install Kaspersky Security Center 13.1**. Wait for some minutes while the installation package is being uncompressed and the installation is being prepared.
7. The following setup wizard should appear. Click **Next >**.



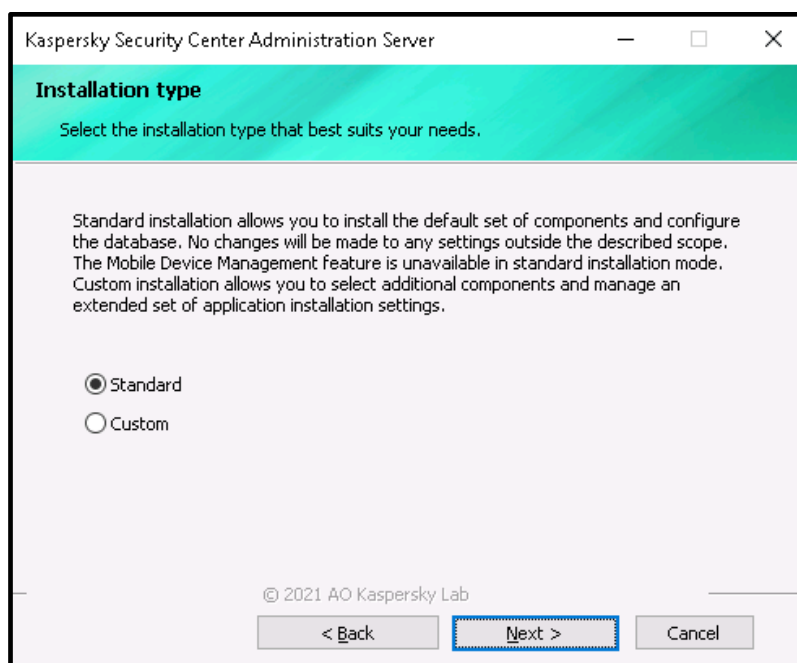
- Please make sure that the system has passed the requirements check and press **Next >**. Otherwise follow the hint on how to install **.NET**.



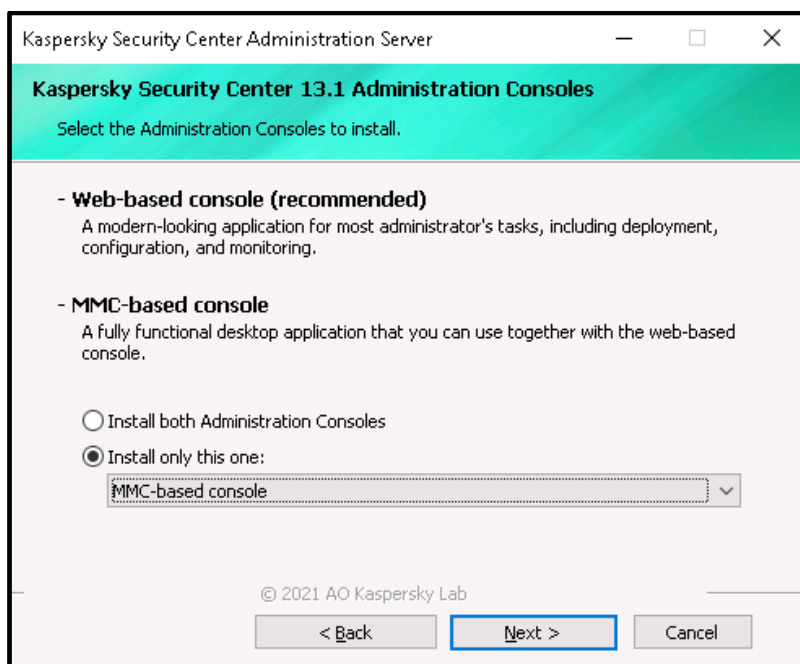
- Accept the terms of the **License Agreement** and **Privacy Policy**. Click **Next >**.



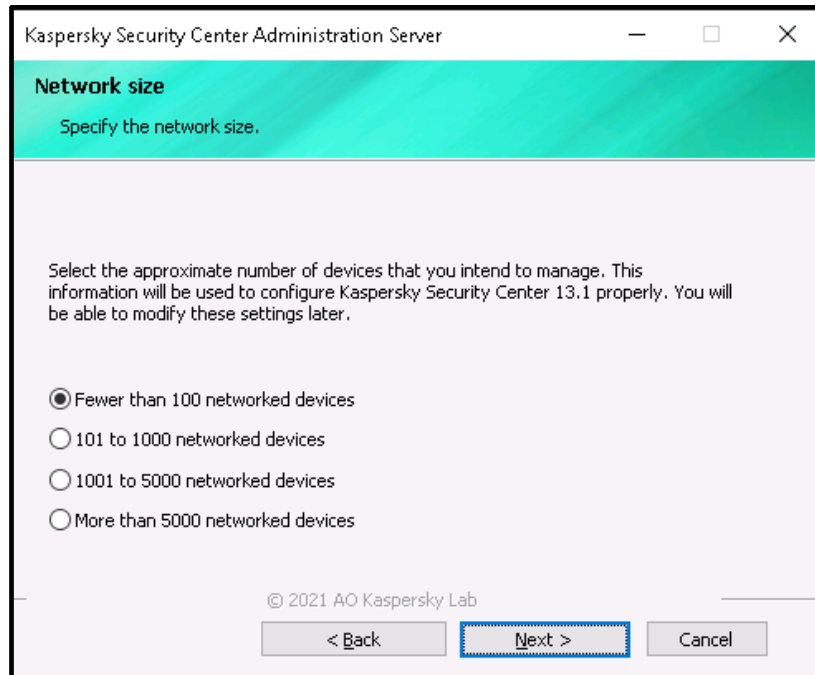
10. Select **Standard** as an installation type and click **Next >**.



11. Specify the component selection as shown in the screenshot below. Click **Next >**.

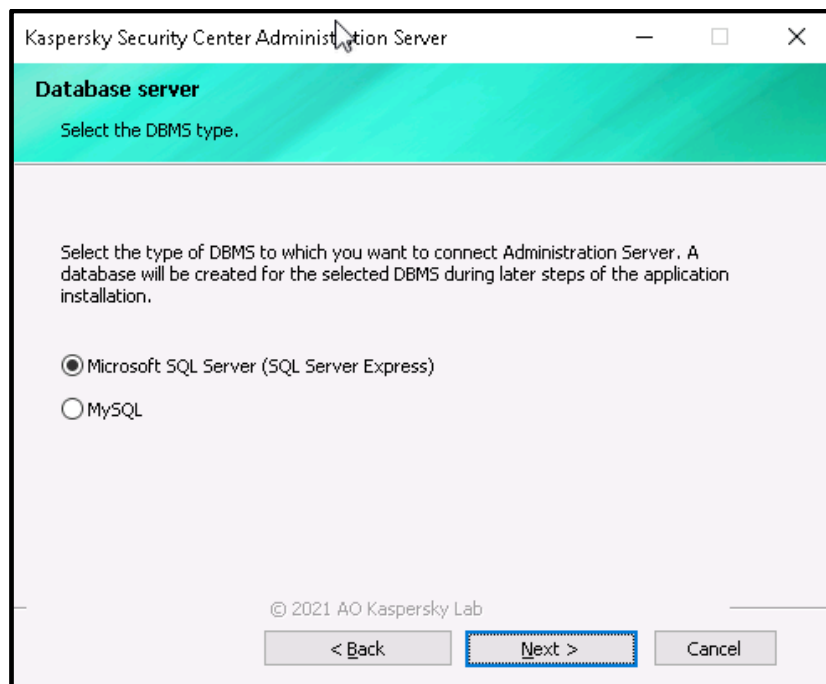


12. Select **Fewer than 100 network devices** (this option normally fits most of the industrial installations) and click **Next >**.



The screenshot shows the 'Network size' configuration window. The title bar reads 'Kaspersky Security Center Administration Server'. The window has a teal header with the title 'Network size' and the instruction 'Specify the network size.' Below this, a text block explains: 'Select the approximate number of devices that you intend to manage. This information will be used to configure Kaspersky Security Center 13.1 properly. You will be able to modify these settings later.' There are four radio button options: 'Fewer than 100 networked devices' (selected), '101 to 1000 networked devices', '1001 to 5000 networked devices', and 'More than 5000 networked devices'. At the bottom, there is a copyright notice '© 2021 AO Kaspersky Lab' and three buttons: '< Back', 'Next >' (highlighted with a blue dashed border), and 'Cancel'.

13. Select the **Database server** type to fit your **SQL** installation. In our case we have installed **SQL Server Express**, so we make the corresponding choice. Click **Next >**.



The screenshot shows the 'Database server' configuration window. The title bar reads 'Kaspersky Security Center Administration Server'. The window has a teal header with the title 'Database server' and the instruction 'Select the DBMS type.' Below this, a text block explains: 'Select the type of DBMS to which you want to connect Administration Server. A database will be created for the selected DBMS during later steps of the application installation.' There are two radio button options: 'Microsoft SQL Server (SQL Server Express)' (selected) and 'MySQL'. At the bottom, there is a copyright notice '© 2021 AO Kaspersky Lab' and three buttons: '< Back', 'Next >' (highlighted with a blue dashed border), and 'Cancel'.

14. Select the **SQL Server** instance using the **Browse...** button, leave the automatically filled fields intact and click **Next >**.

Kaspersky Security Center Administration Server

Connection settings
Specify the Microsoft SQL Server settings.

1) Make sure that the relevant version of Microsoft SQL Server is installed.
You can download Microsoft SQL Server 2014 Express SP2 (recommended) or another supported version from the [Microsoft website](#). Other versions of Microsoft SQL Server are available on [this website](#).

2) Specify the Microsoft SQL Server settings:

SQL Server instance name: PCS7-KSC\SQLEXPRESS **Browse...**

Database name: KAV

© 2021 AO Kaspersky Lab

< Back Next > Cancel

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

Kaspersky Security Center Administration Server

SQL Server Authentication mode
Choose the authentication mode.

Choose the authentication mode that you want to use for connection to Microsoft SQL Server. If you select SQL Server Authentication, you are prompted to enter the account and confirm the password.

☒ Microsoft Windows Authentication mode

☐ SQL Server Authentication mode

Account:

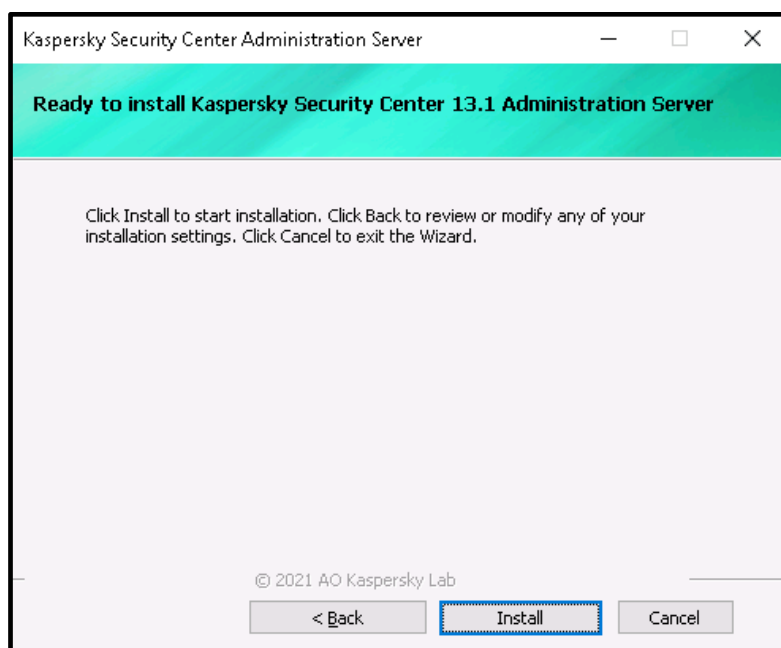
Password:

Confirm password:

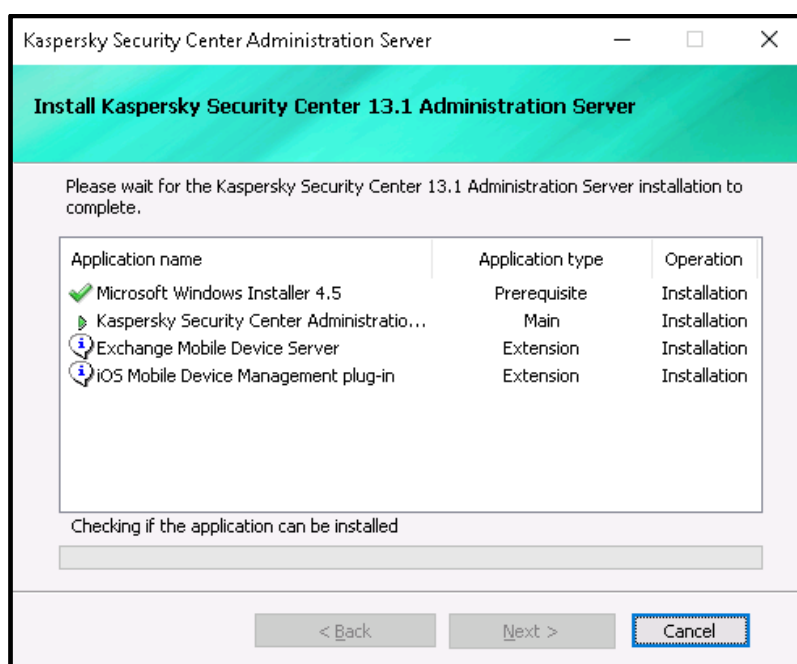
© 2021 AO Kaspersky Lab

< Back Next > Cancel

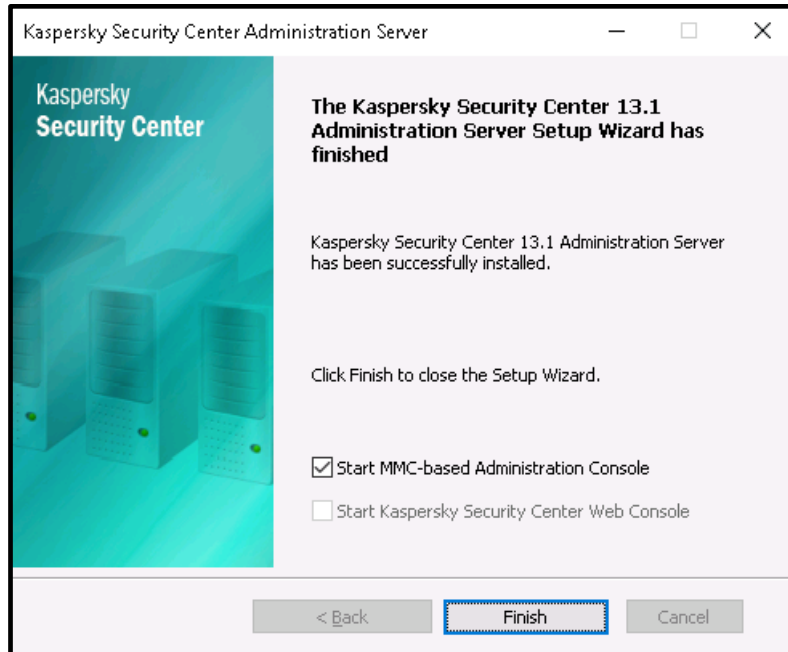
16. Confirm the installation start in the **Ready to install...** window by clicking **Install**.



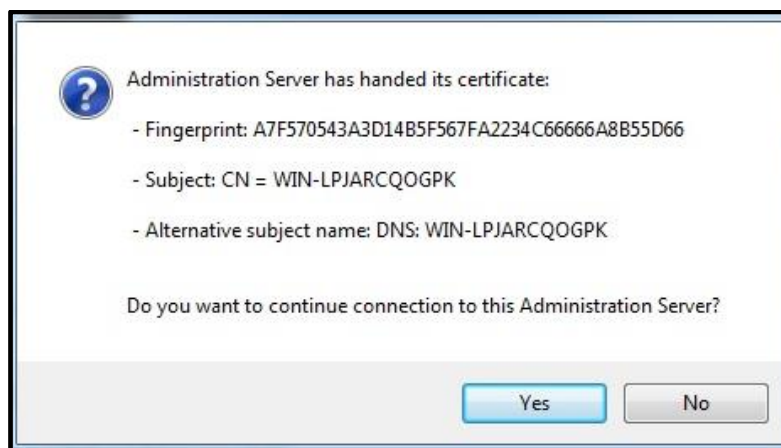
17. Wait until the installation process is completed. Throughout the installation its progress is displayed in the following window.



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



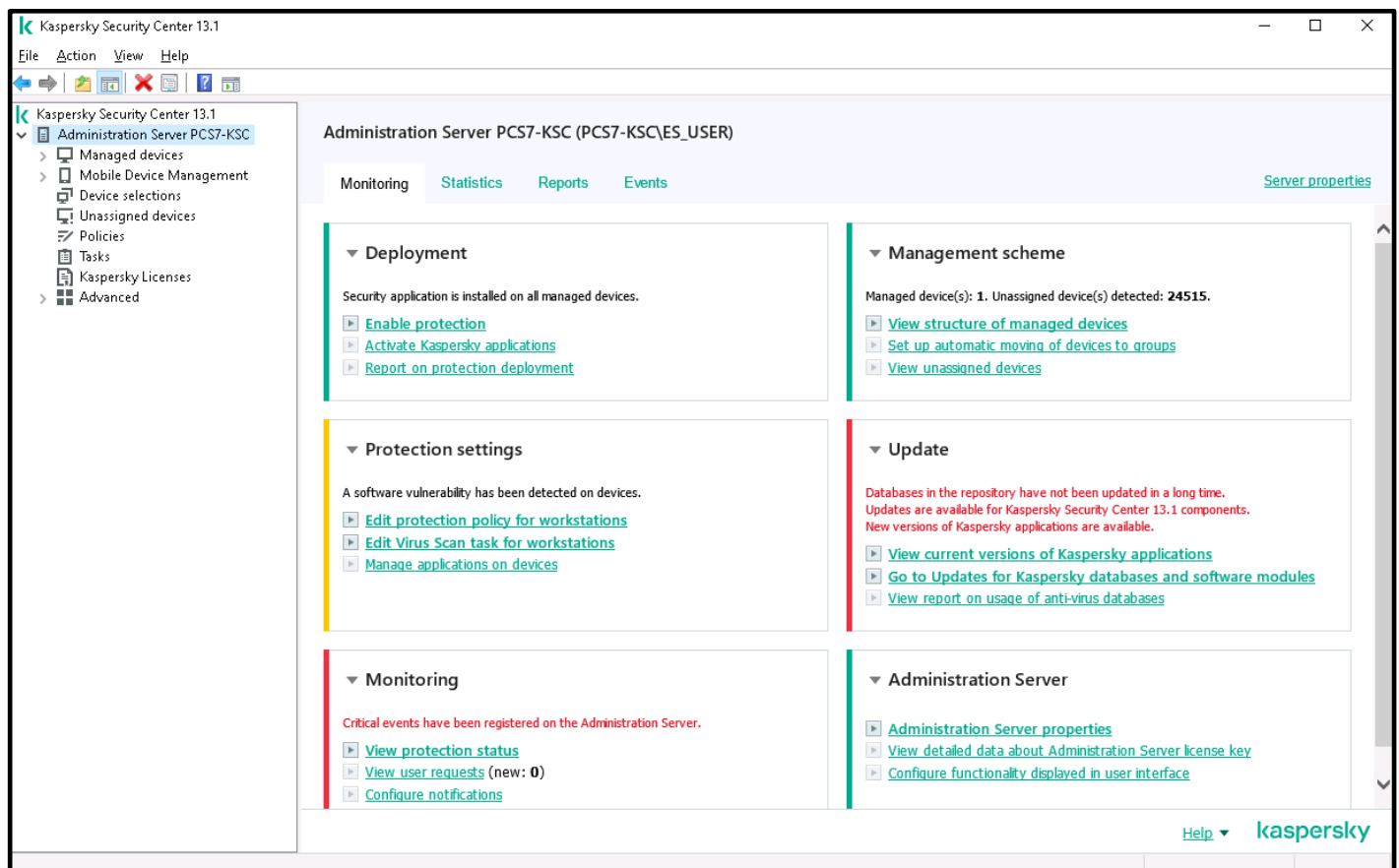
19. Press **Yes** in the following window in order to launch **Administration Console** and make it establish an encrypted connection to the server. This finalizes the **KSC** installation.



Initial configuration of KSC

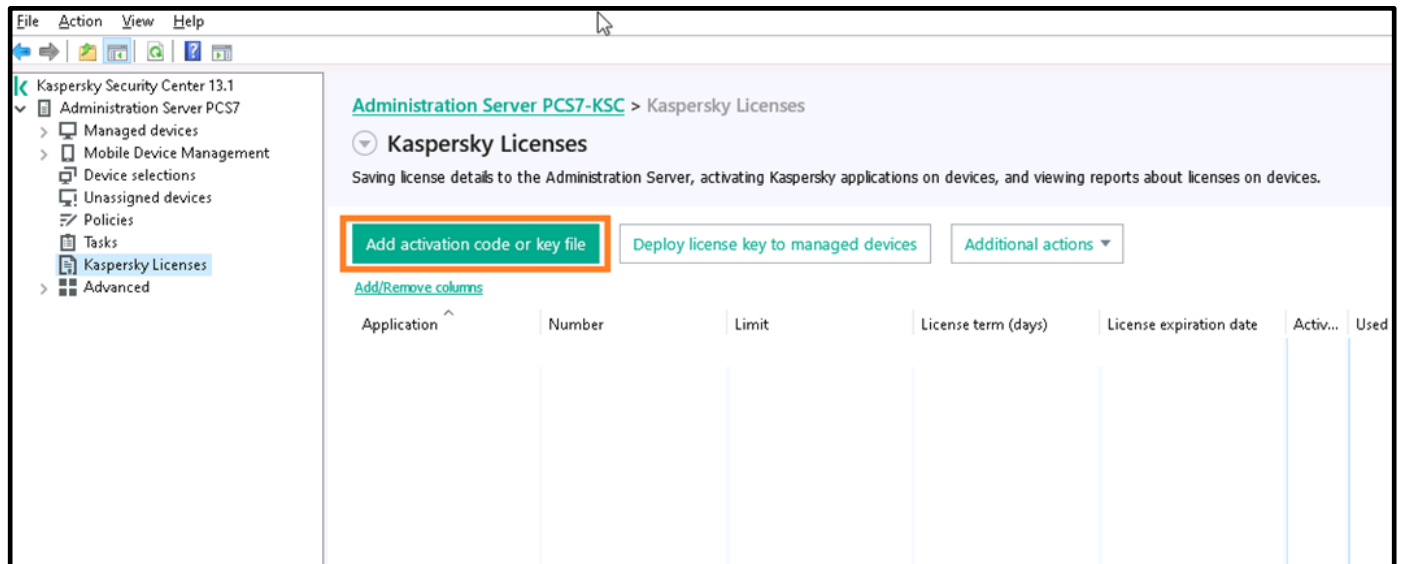
The **KSC Administration Console** automatically starts up after the **KSC** server core components are installed³. Please perform the following operations to apply primary settings to **KSC**:

1. Cancel the **KSC Administration Server Quick Start Wizard** if it has emerged. We are not going to use it.
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. Switch over to the **Monitoring** tab, click **Activate Kaspersky applications** to view the list of installed licenses.

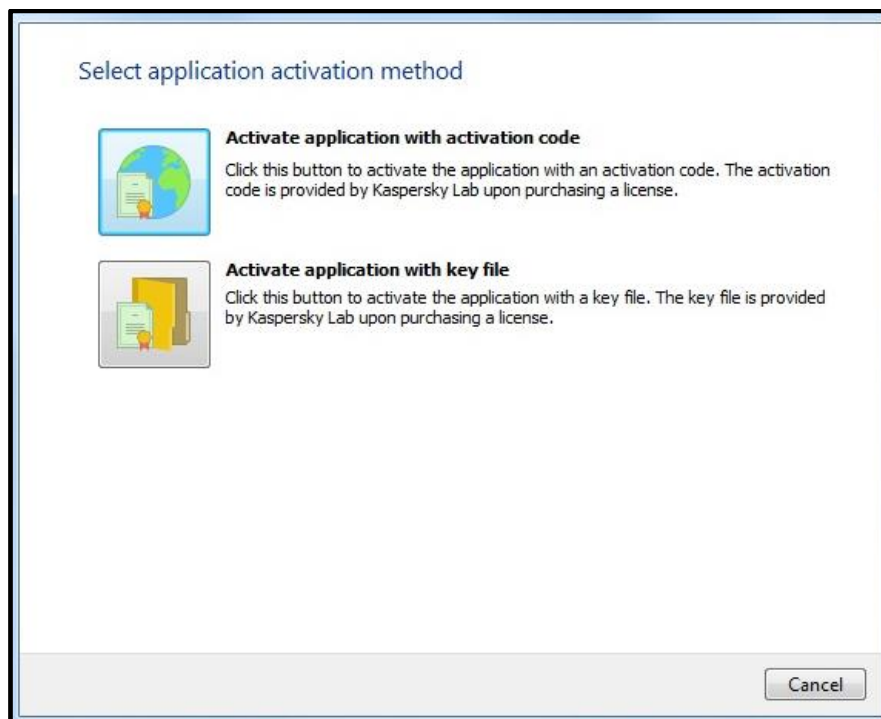


³ The other way of calling **KSC Administration Console** is using the **Kaspersky Security Center 13** shortcut located on the **Start** menu.

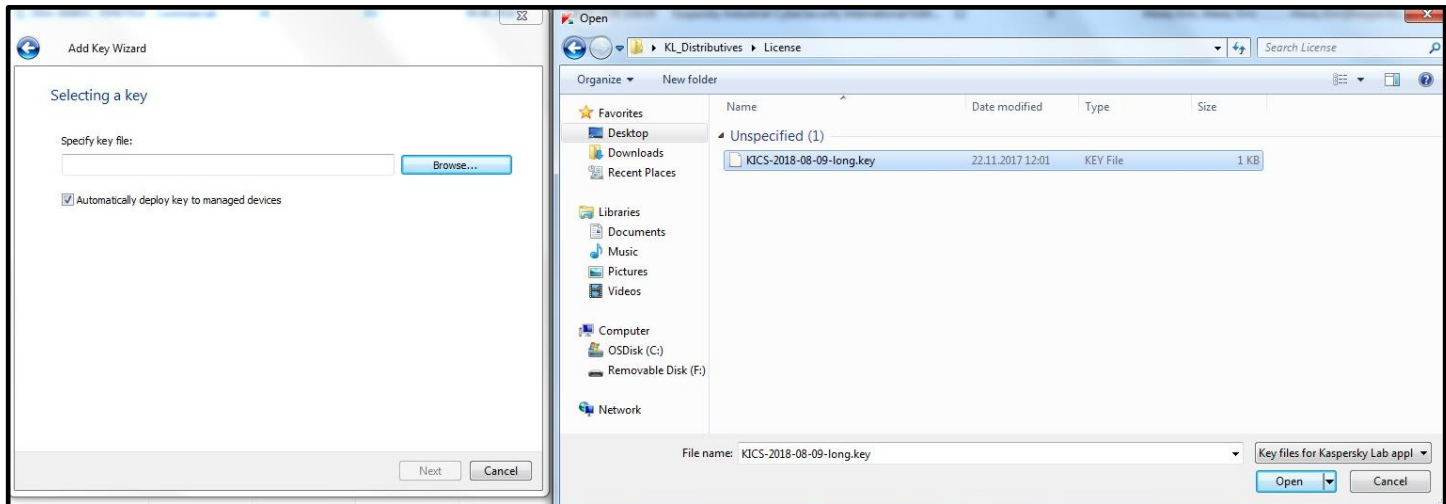
- Apparently, the list of installed licenses is initially blank. Press the **Add activation code or key file** button as highlighted below.



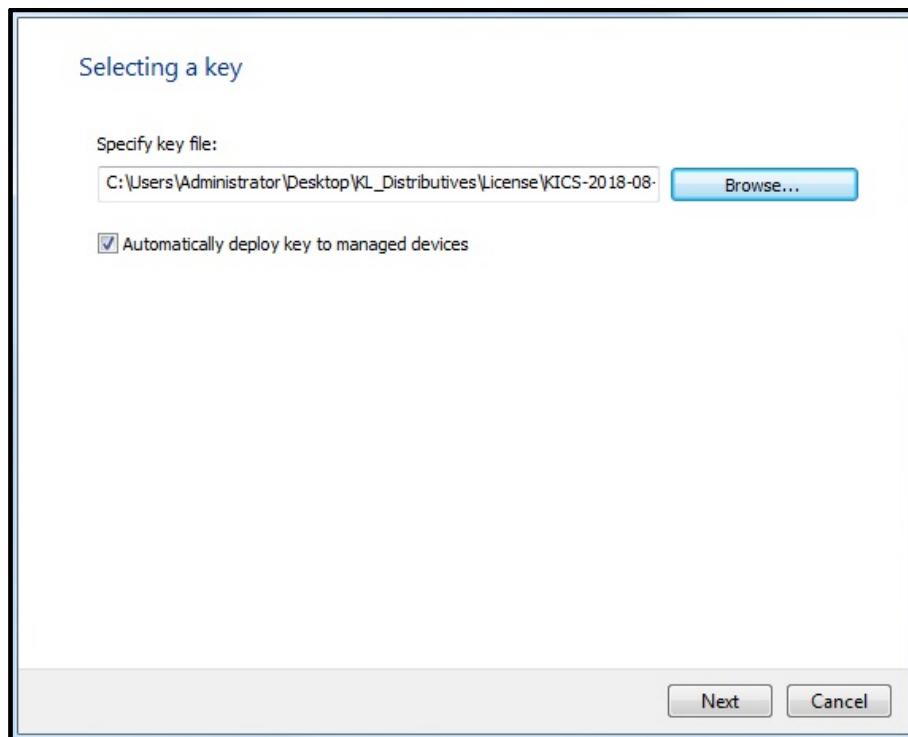
- This starts up the **Add Key Wizard** as shown in the picture below. Most likely, you have got a license key from **Kaspersky**, which requires no Internet for verification. Choose **Activate application with a key file**.



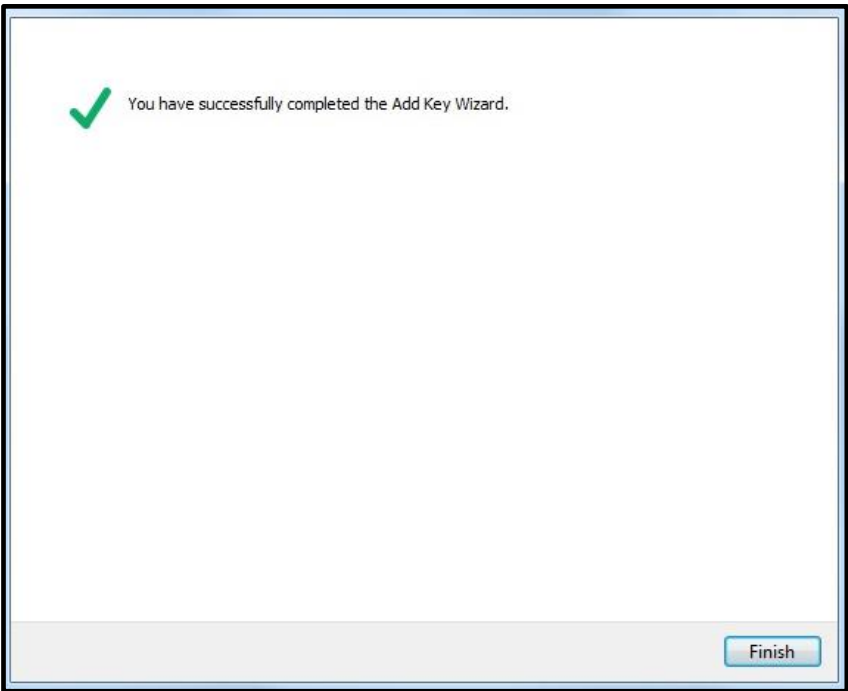
5. In the **Selecting a key** window, check **Automatically deploy key to managed devices** and press **Browse** to locate the key-file supplied. The key file is normally supplied with the distribution package and should have the extension ***.key**.



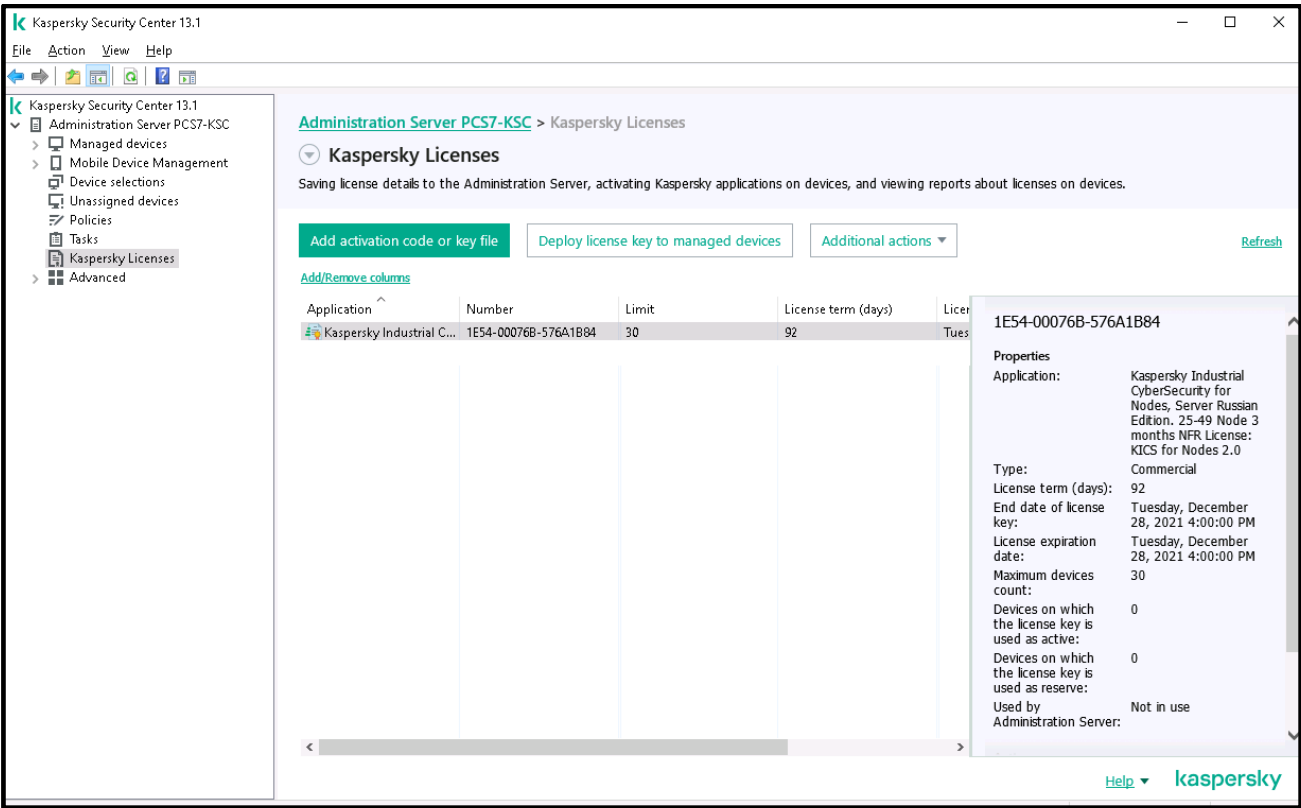
6. After you have picked the appropriate key-file, press **Next**.



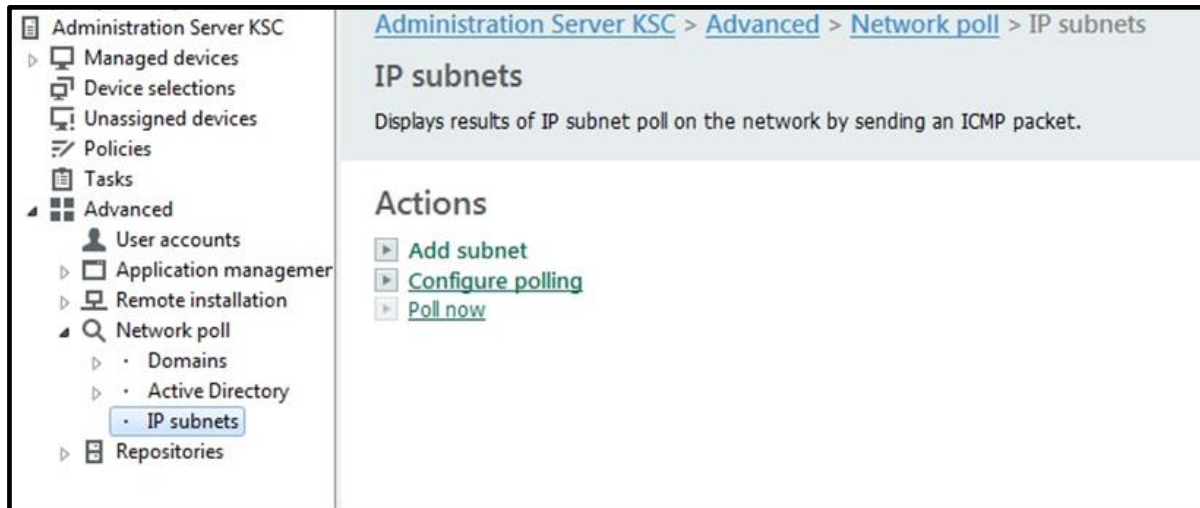
7. Please **Finish** to complete adding your key file.



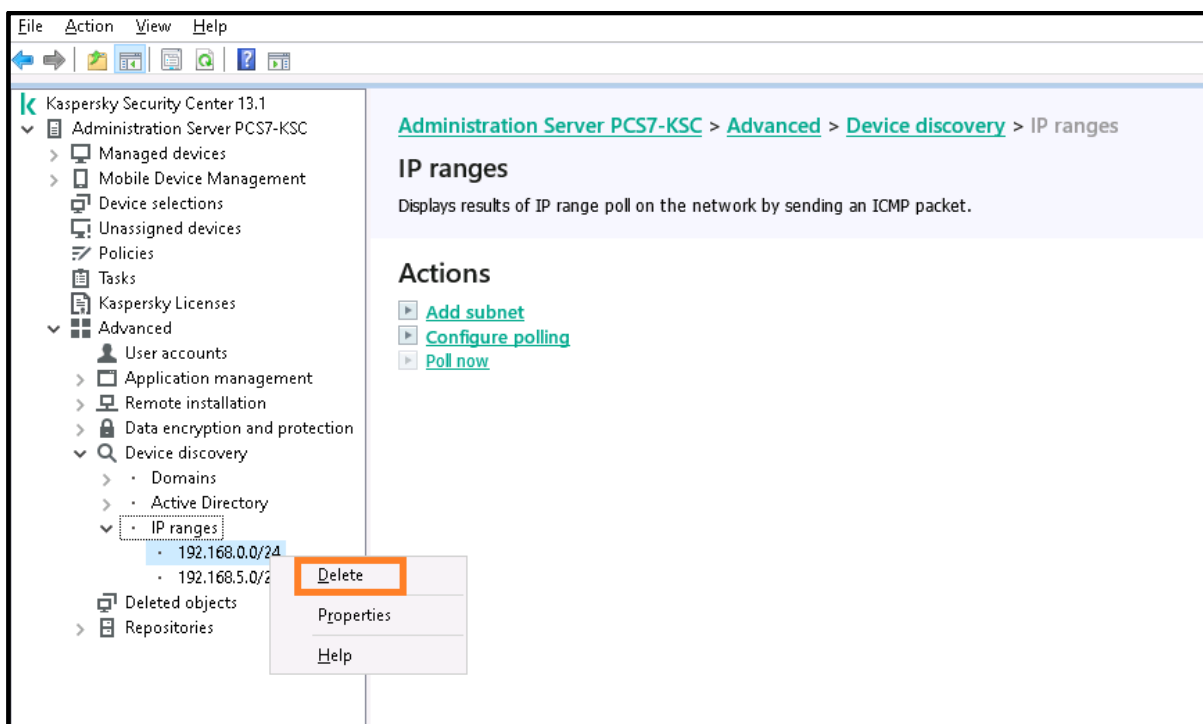
8. If the selected key file is valid, it should emerge on the list of installed licenses as shown below. Study the license terms carefully.



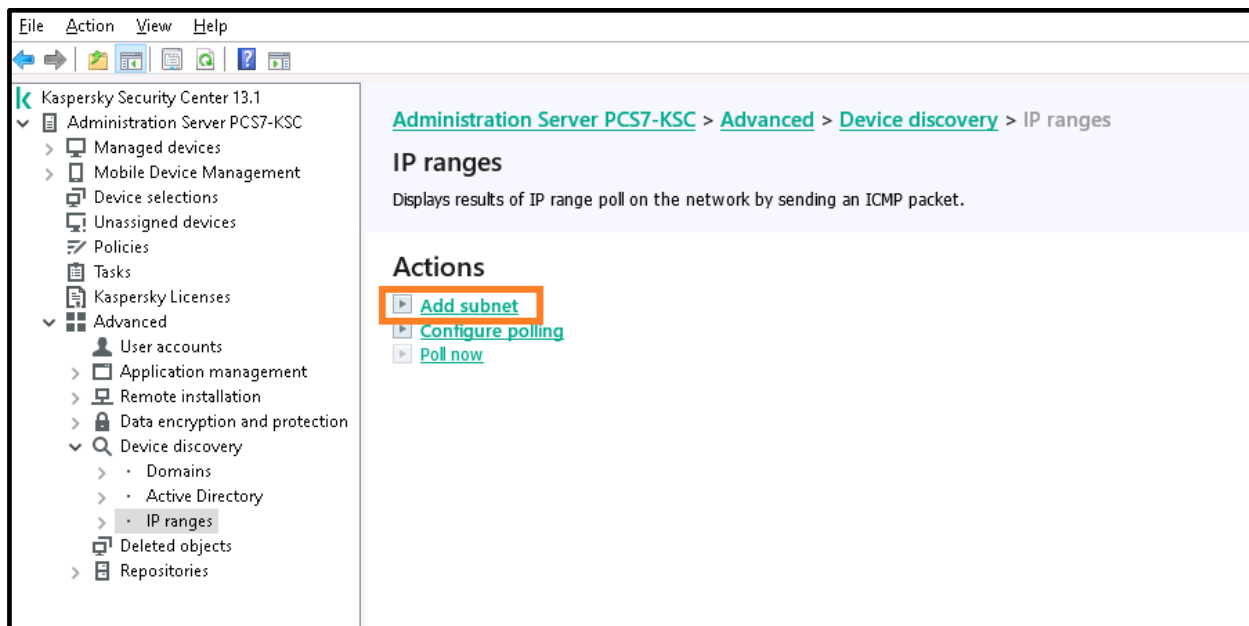
- Using the navigation tree in the left-hand pane, now we go to the **Administration Server->Advanced->Network Poll->IP subnets** hierarchical node. Click **Add subnet** as shown below to expand the list of automatically detected subnets.



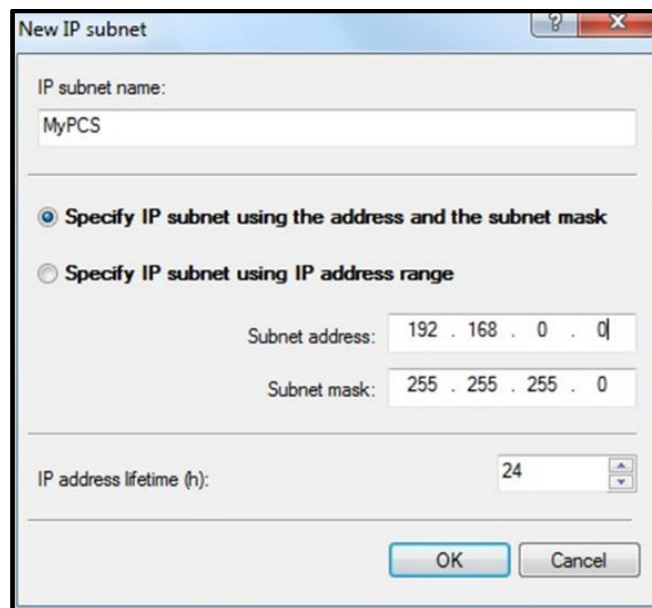
- In our case, we have a couple of NICs installed on the same **KSC** machine. They belong to different subnets. We suggest starting from scratch. Let us first delete all the automatically discovered subnets using the right-click menu as shown below.



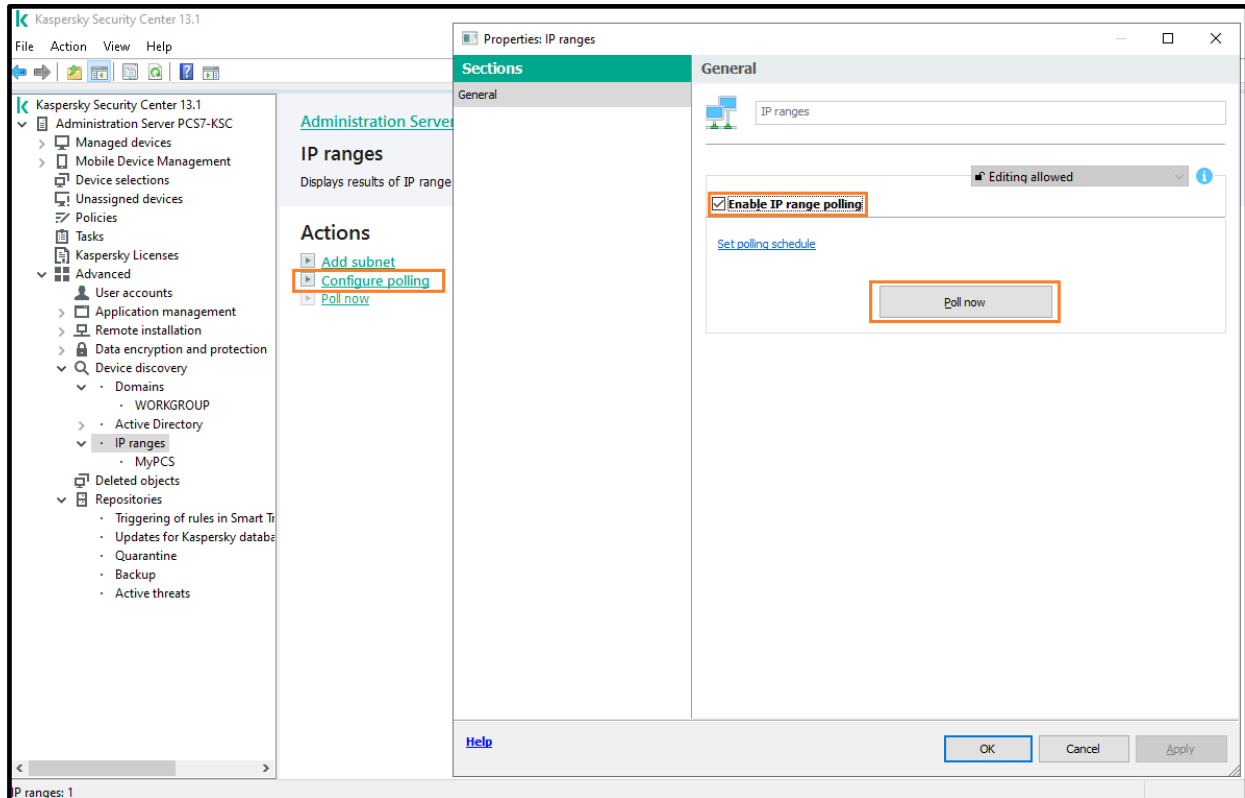
11. Now let us add the monitored subnet(s) we are interested in. So, click **Add subnet** in the right-hand pane.



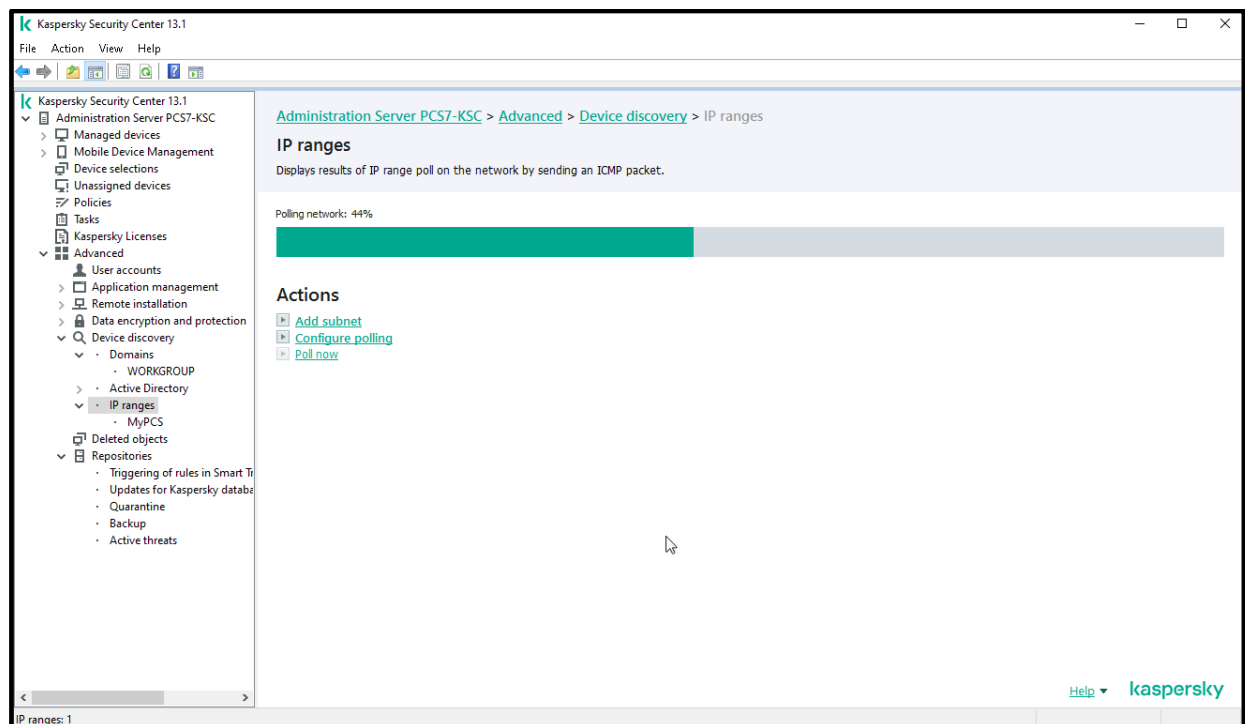
12. In the window that appears, specify the network polling details. In our case, we have named our control system network “MyPCS” and specified the IP subnet (192.168.0.0/24) that will be polled. Click **OK** when done.



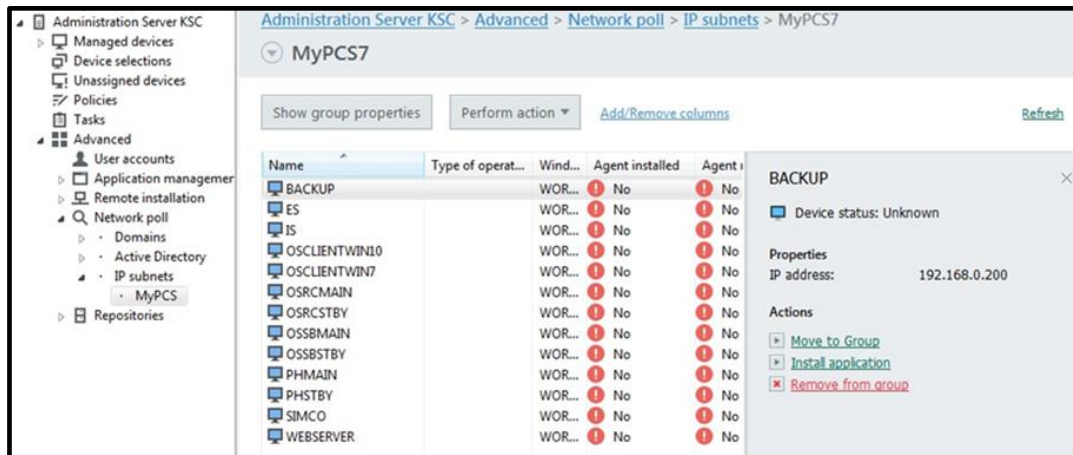
- Click **Configure Polling** in the right-hand pane. The following window should appear. Check **Enable IP subnets polling** and press the **Poll now** button. Click **OK** to close the popup window.



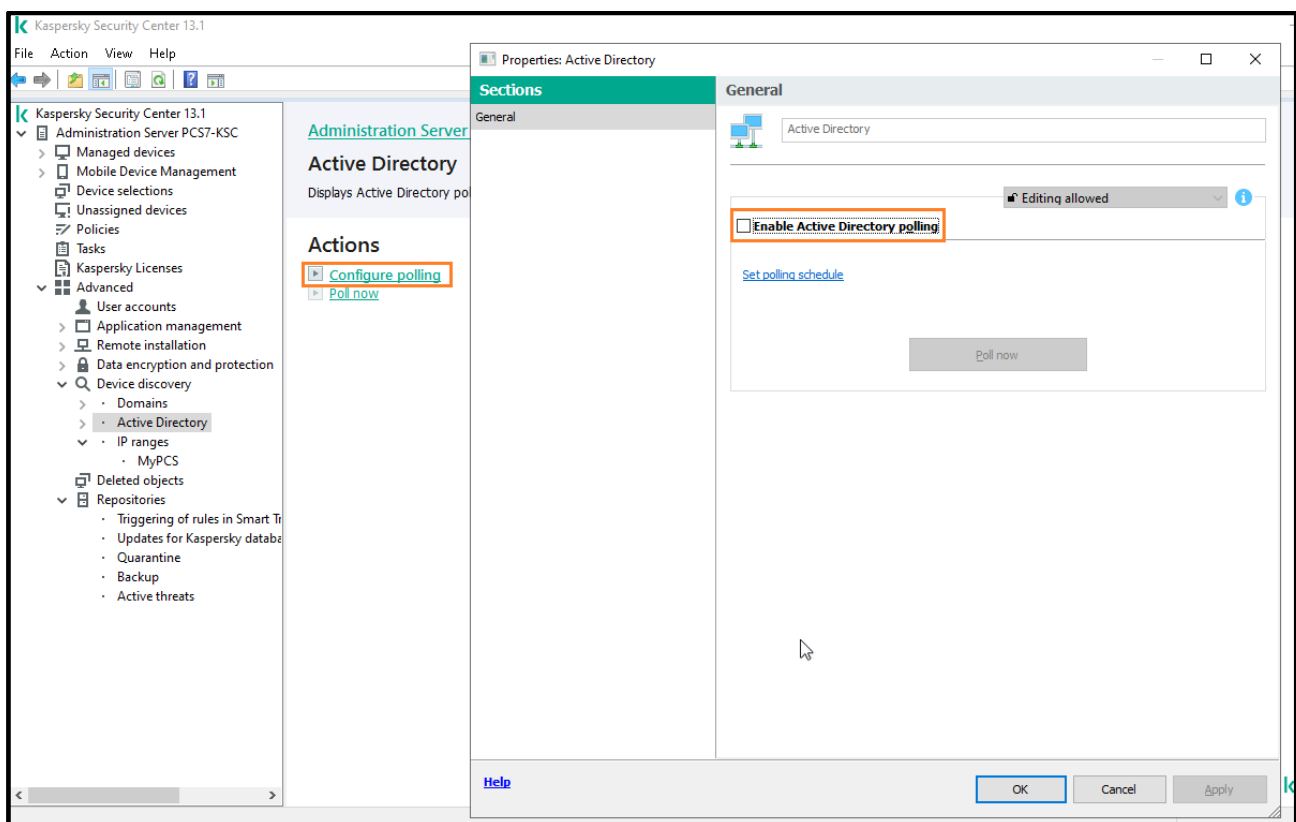
- Wait for some time until the polling process is complete. The polling time depends on the scale of your network. You can track percentage of completion by viewing the progress bar as shown below.



15. 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.

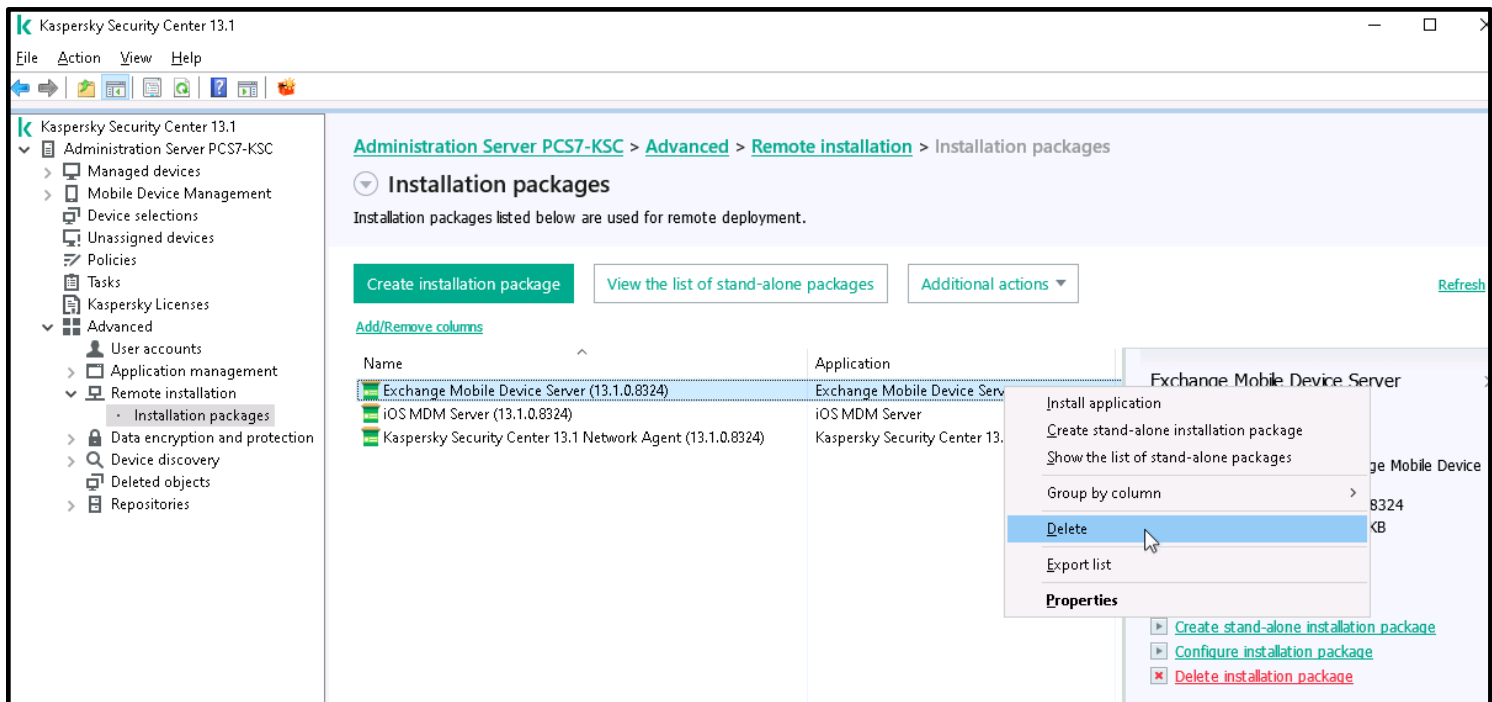


16. In our case, we are going to proceed with the **SIMCO** host only. However, it is easy to replicate the same configuration techniques for multiple hosts⁴ by placing them into respective managed devices groups.
17. If there is neither a domain structure nor active directory configured on your production site, we suggest that you manually disable network polling for these technologies. For example, the screenshot below guides you how to do it for **Active Directory**.

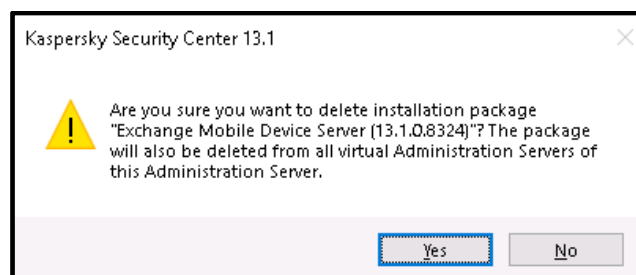


⁴ Please note that in this document the terms “device”, “host” and “target computer” have the same meaning and are interchangeable.

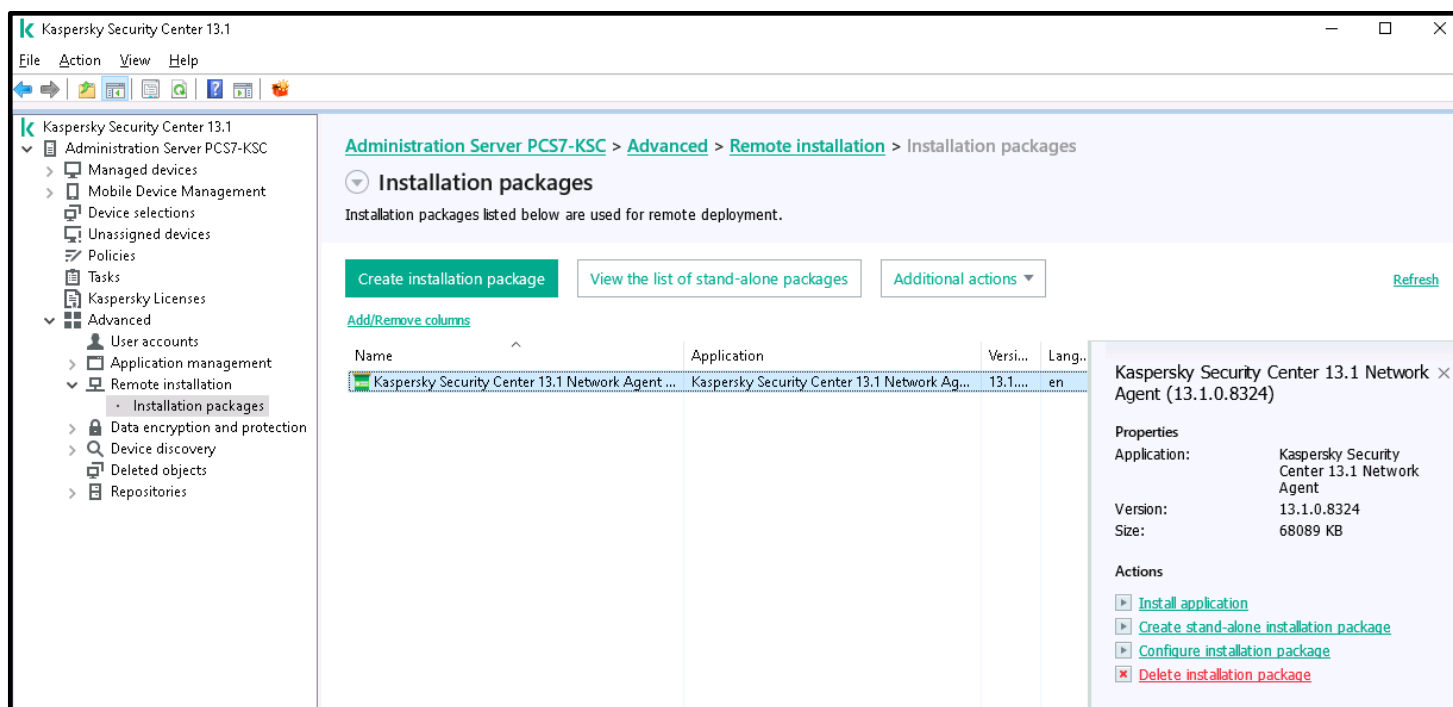
18. Using the left-hand pane navigation tree, now we go to the **Administration Server->Advanced->Remote Installation->Installation packages** hierarchical node.
19. It is advised to remove from the repository all the default packages **apart from Kaspersky Security Center 13.1 Network Agent**. The latter will be required for the remote installation of **KICS for Nodes**.
20. For every redundant package call the context menu and choose **Delete** as shown below.



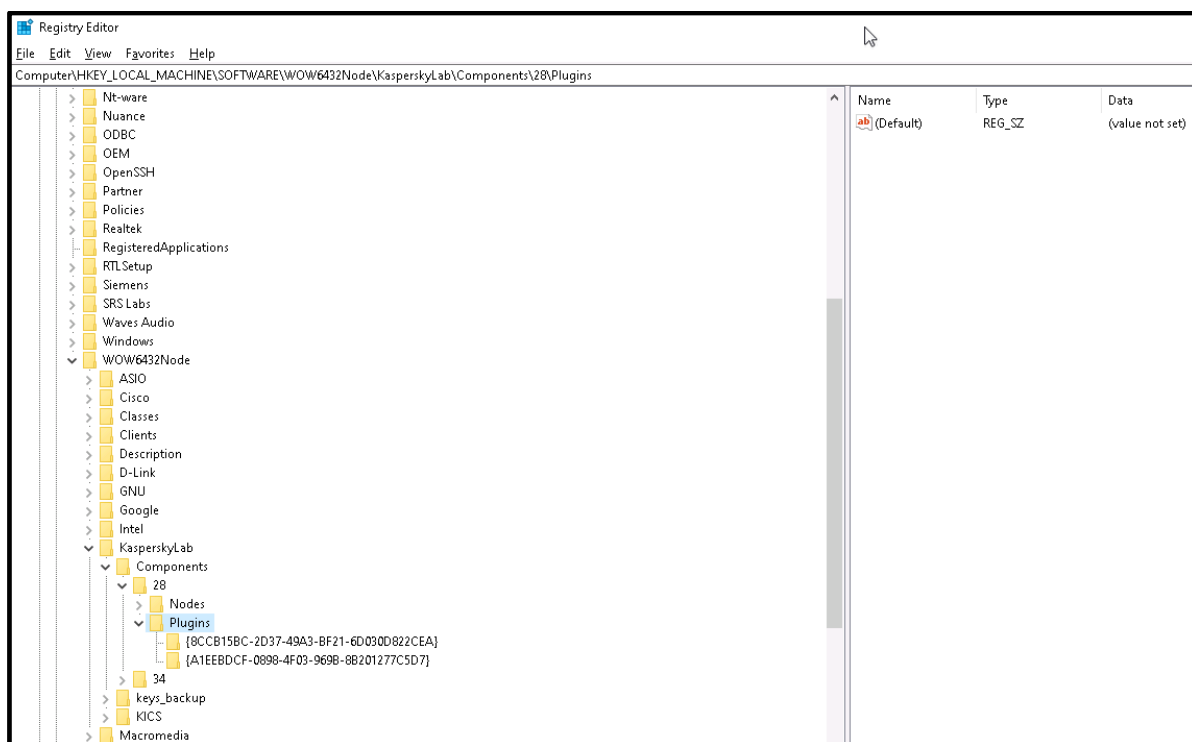
21. For every software package, that is to be deleted, confirm its removal by pressing **Yes** in the confirmation window.



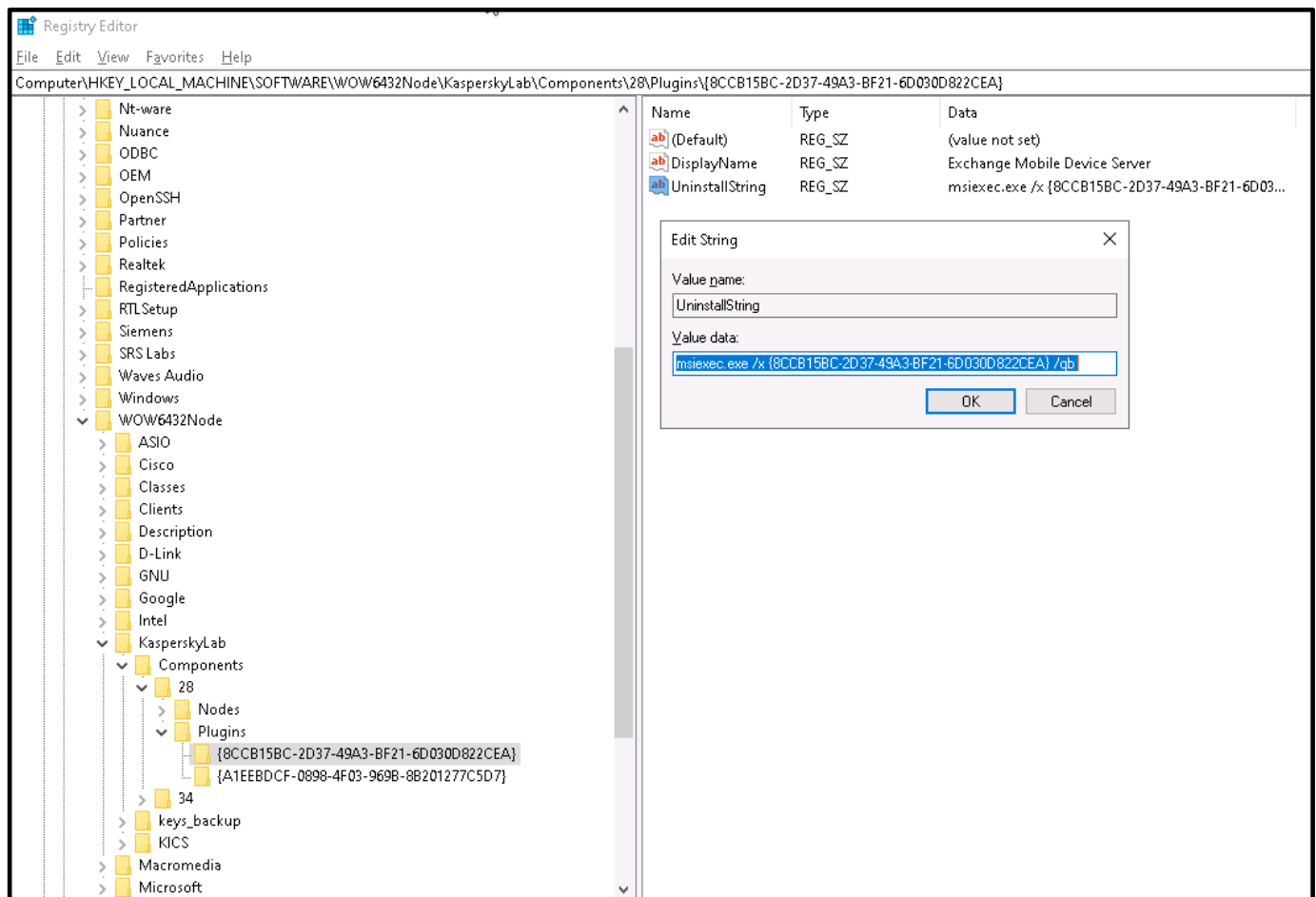
22. As mentioned before, you should end up with just one software package as shown below.



23. The last thing left for us to do with the primary configuration of **KSC** is to uninstall unnecessary plugins. So, we call **Regedit.exe** and navigate into the following branch: **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Components\28\Plugins** (as shown below). The branch should contain two sub nodes, each relates to an individual **KSC** plugin.



24. Select either of the two nodes and locate the **UninstallString** key. Copy its value to clipboard.



25. Run **Cmd.exe** as administrator and paste the copied value into the command line. Execute it.



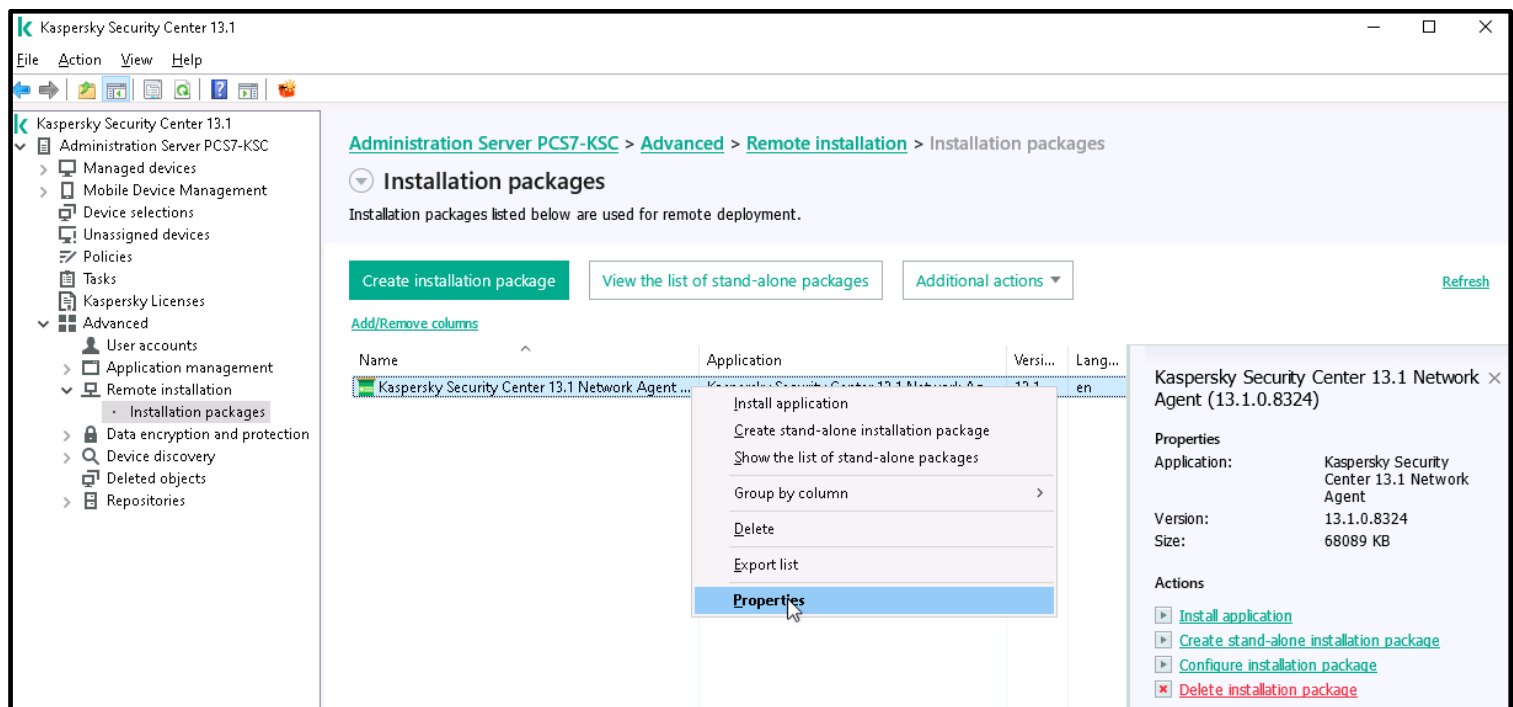
26. Now repeat the same with the other registry node. Close the **Registry Editor** and restart the **KSC Administration Console** to make changes come into effect.

Remote installation of KLnagent onto target computers

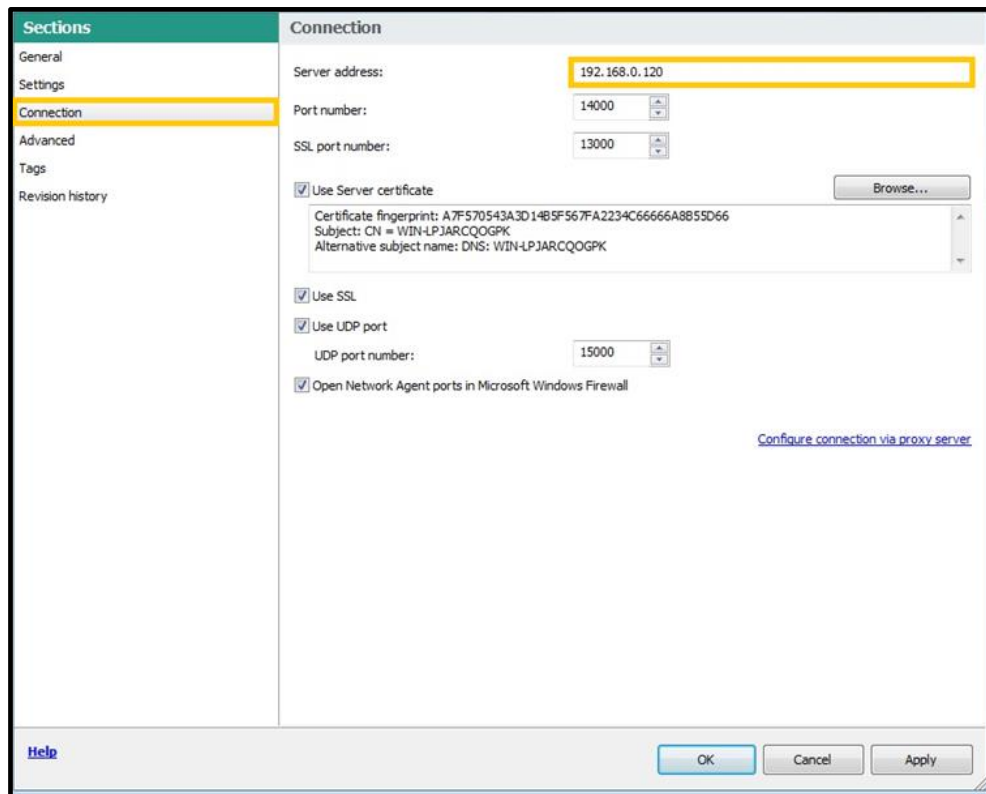
In order to make a host remotely manageable by **KSC**, we need to install the network agent **KLnagent** on that host. However, prior to the **KLnagent** installation, it is important to make sure that the **KSC** computer has network access to the administrative shares located on the **SIMCO** device (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 to jump to step 3 right away.

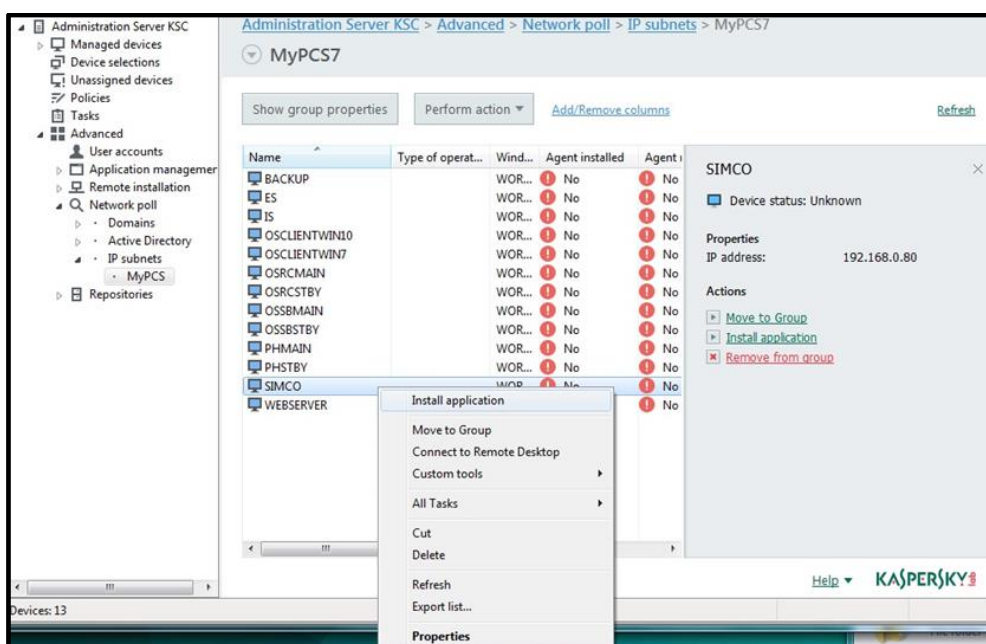
1. Go to the **Advanced->Remote installation->Installation packages** hierarchical node and right-click on the **Kaspersky Security Center 13 Network Agent installation** package. In the context menu select **Properties**.



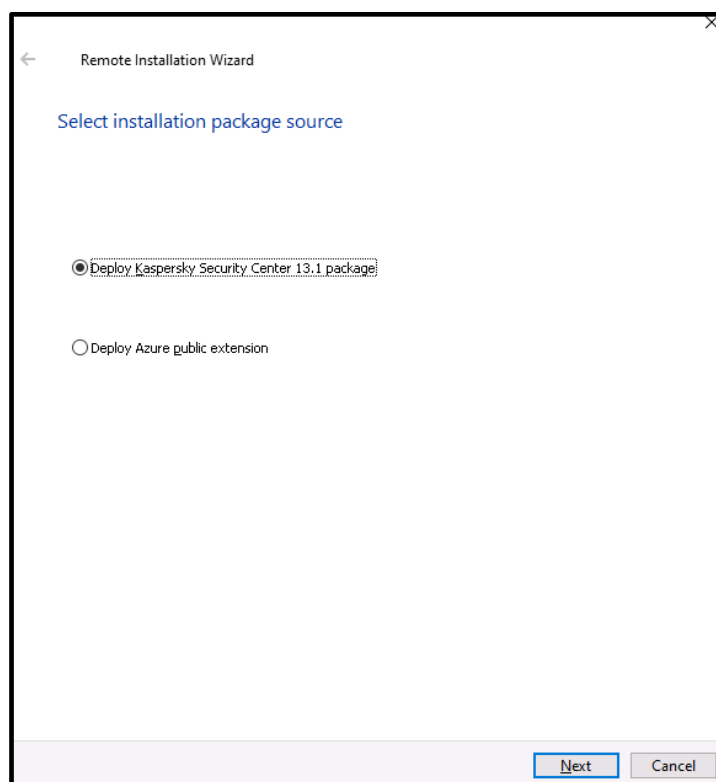
- In the window that appears, go to **Connection**. Find the **Server address**: text field and replace the symbolic name of the **Kaspersky Security Center** server with its explicit IP address. The other settings should look as shown below. Press **Apply** and **OK** to close the window.



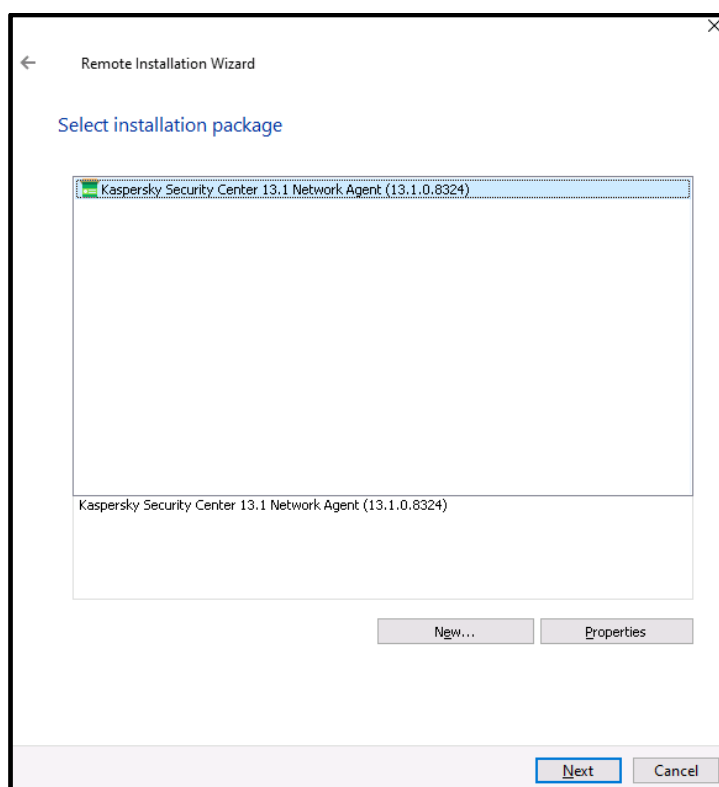
- Now, proceed to **Advanced->Network Poll->IP subnets**. From the list of the discovered devices select the one you want to install **KLnagent** on. In our example, it is **SIMCO**. Right-click on the target host and select **Install Application** in the context menu as shown below.



4. In the **Remote Installation Wizard** select **Deploy Kaspersky Security Center 13.1** package and click **Next**.



5. In the **Select installation package** window choose **Kaspersky Security Center 13 Network Agent**, which is the only option yet. Click **Next**.



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

Defining remote installation task settings

Force installation package download

☐ Using Network Agent

☐ Using operating system resources through distribution points

☒ Using operating system resources through Administration Server
To perform installation by using the API of a cloud service provider, you need a special license.
[Learn more...](#)

Behavior for devices managed through other Administration Servers

☒ Install always

☐ Install only on devices managed through this Administration Server

☐ Do not re-install application if it is already installed

☐ Assign package installation in Active Directory group policies

Next Cancel

7. Now 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**.

Select user account to access remote device

☐ No account required (Network Agent installed)

☒ Account required (for installation without Network Agent)

Add accounts with administrator rights on the devices where the application is to be installed or on the domain controller for installation through Active Directory.

Account

Administrator

Password:

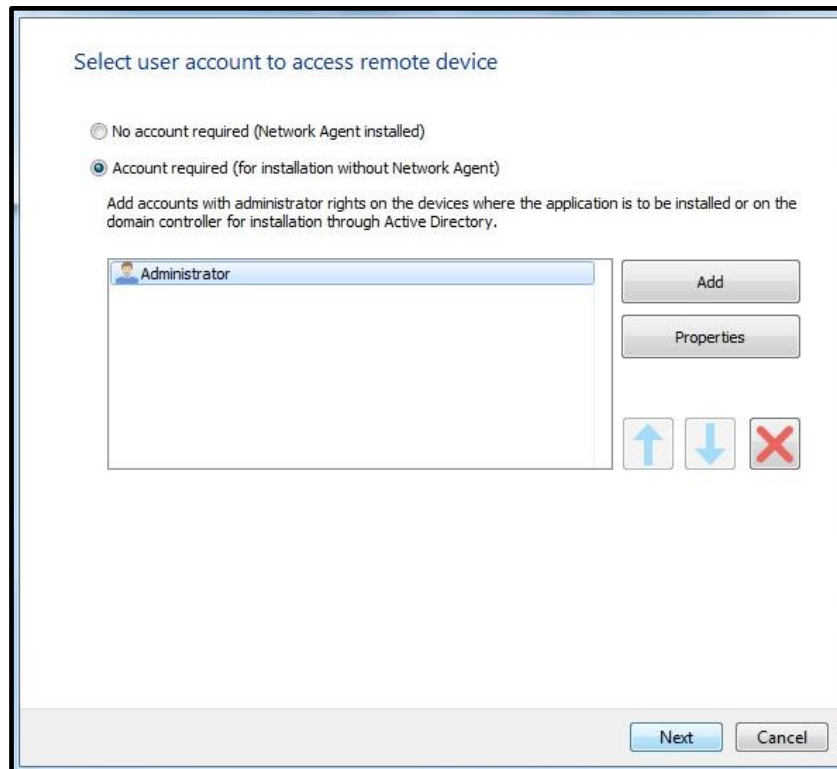
Confirm password:

OK Cancel

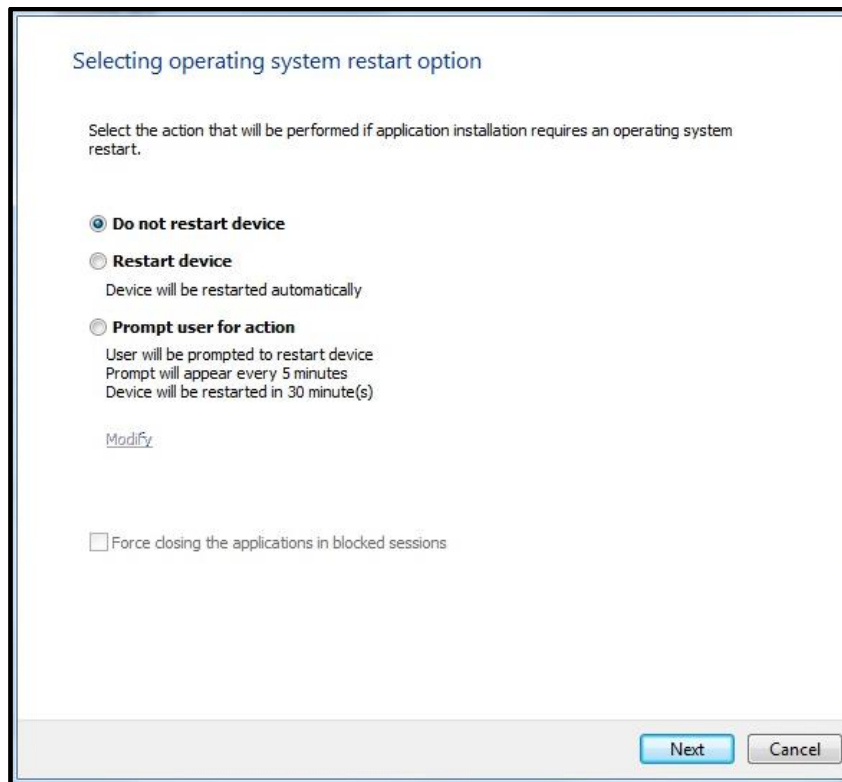
Add Properties

Next Cancel

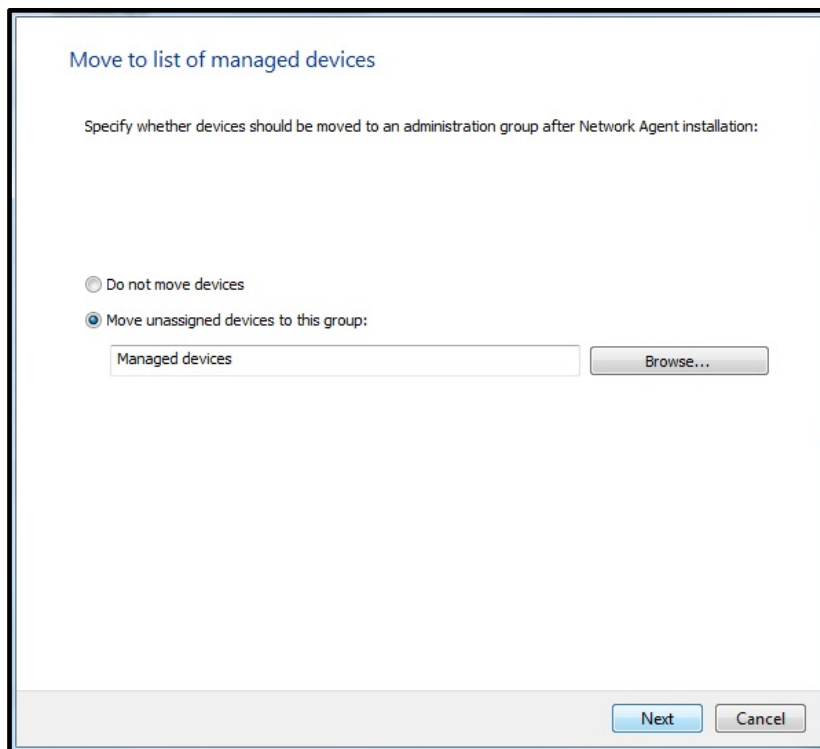
8. When done, click **Next**.



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

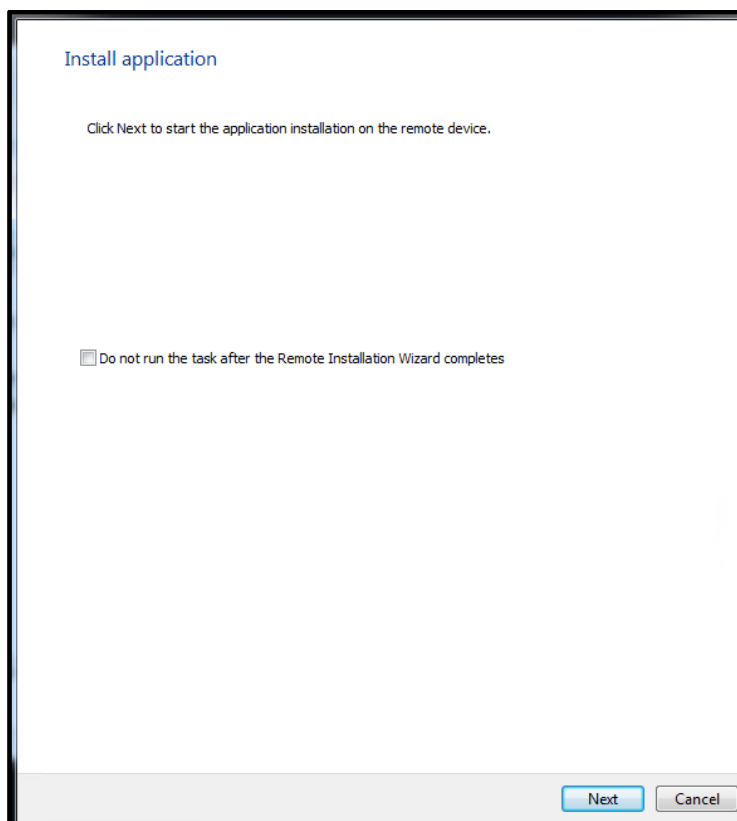


10. Check **Move unassigned devices to this group** and choose **Managed devices** as a destination group.
Click **Next**.



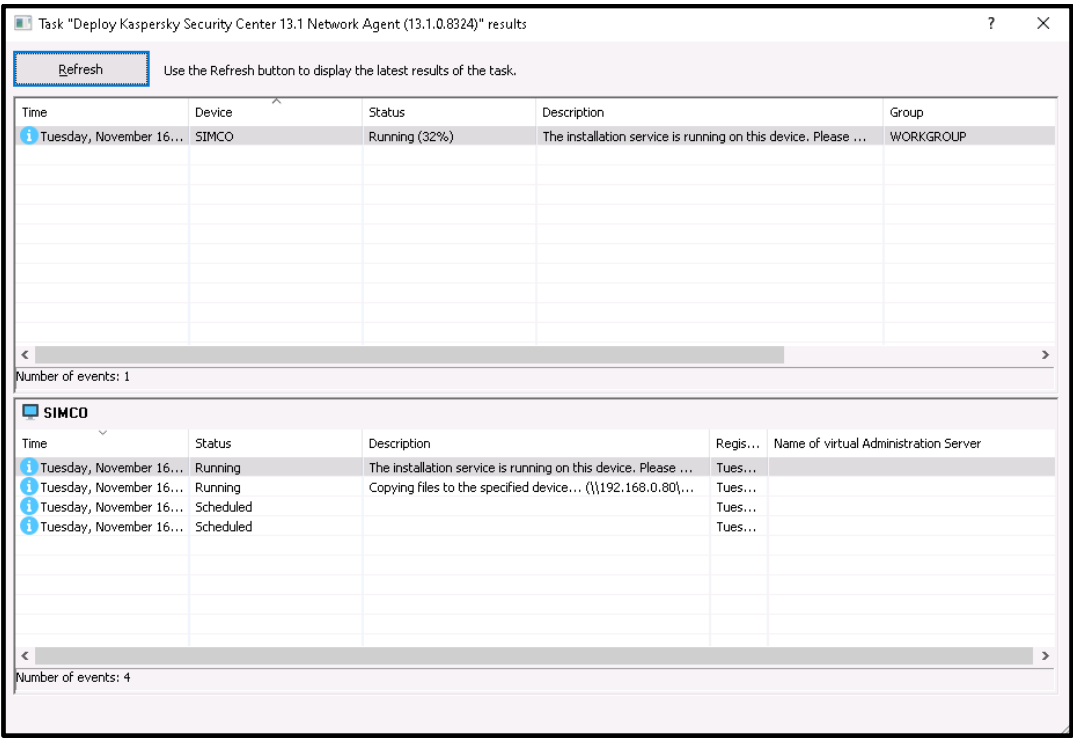
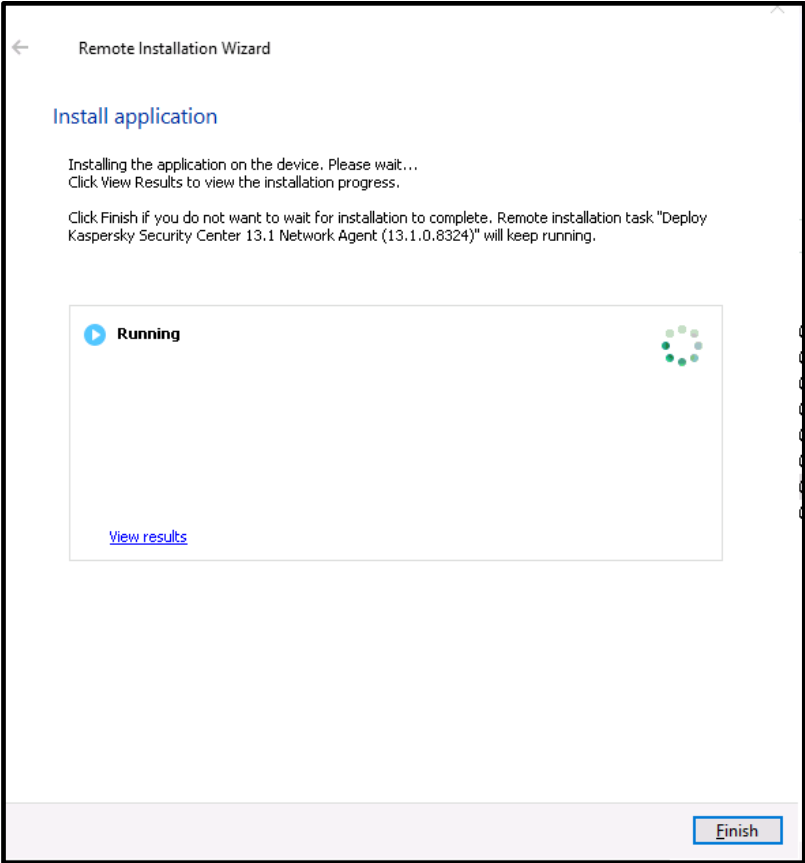
The screenshot shows a dialog box titled "Move to list of managed devices". Inside, there is a text label: "Specify whether devices should be moved to an administration group after Network Agent installation:". Below this, there are two radio button options. The first is "Do not move devices". The second is "Move unassigned devices to this group:", which is selected. Below the selected option is a text box containing "Managed devices" and a "Browse..." button to its right. At the bottom right of the dialog are "Next" and "Cancel" buttons.

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

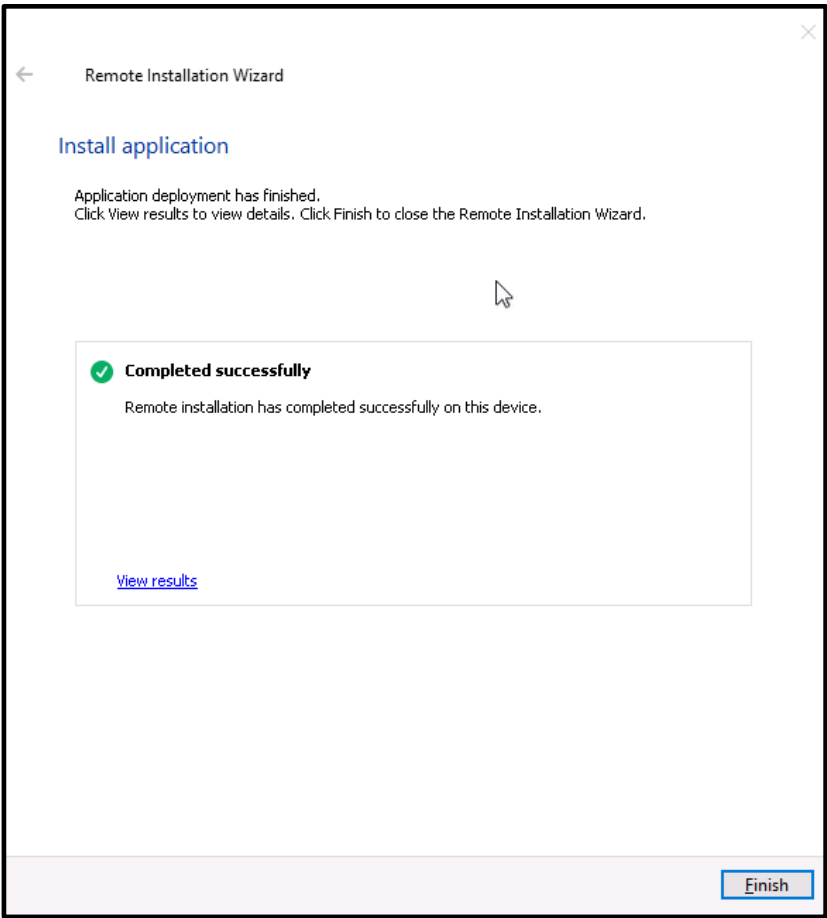


The screenshot shows a dialog box titled "Install application". Inside, there is a text label: "Click Next to start the application installation on the remote device.". Below this, there is a checkbox option: "Do not run the task after the Remote Installation Wizard completes", which is currently unchecked. At the bottom right of the dialog are "Next" and "Cancel" buttons.

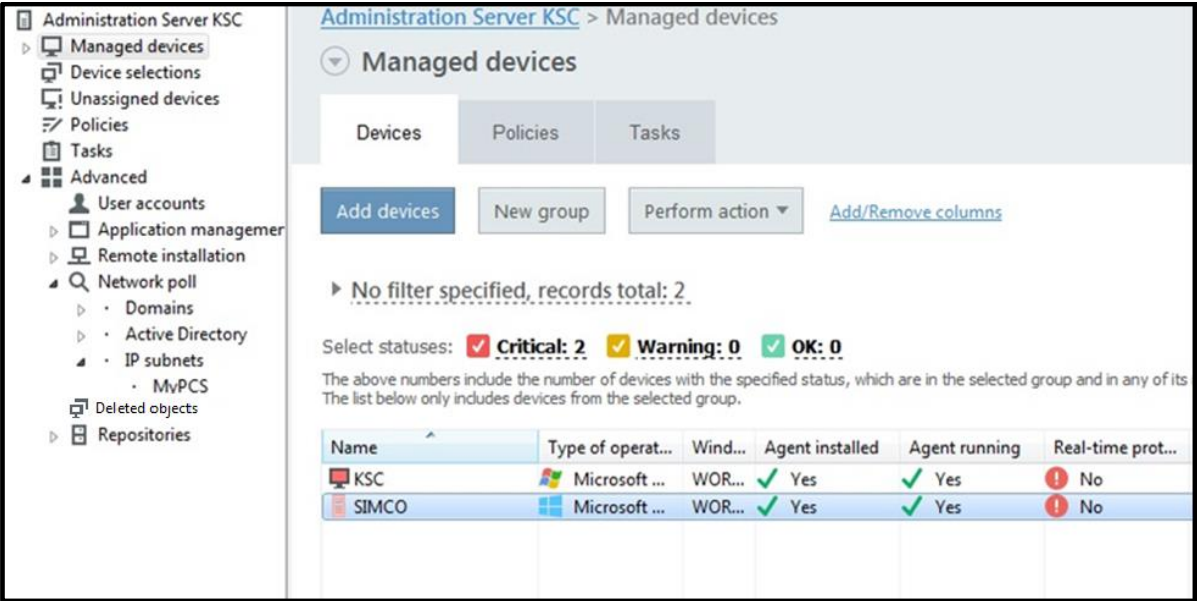
12. Wait until the installation process is complete. It can take up to 10 minutes. You can get more details on the installation progress if you click **View Results**.



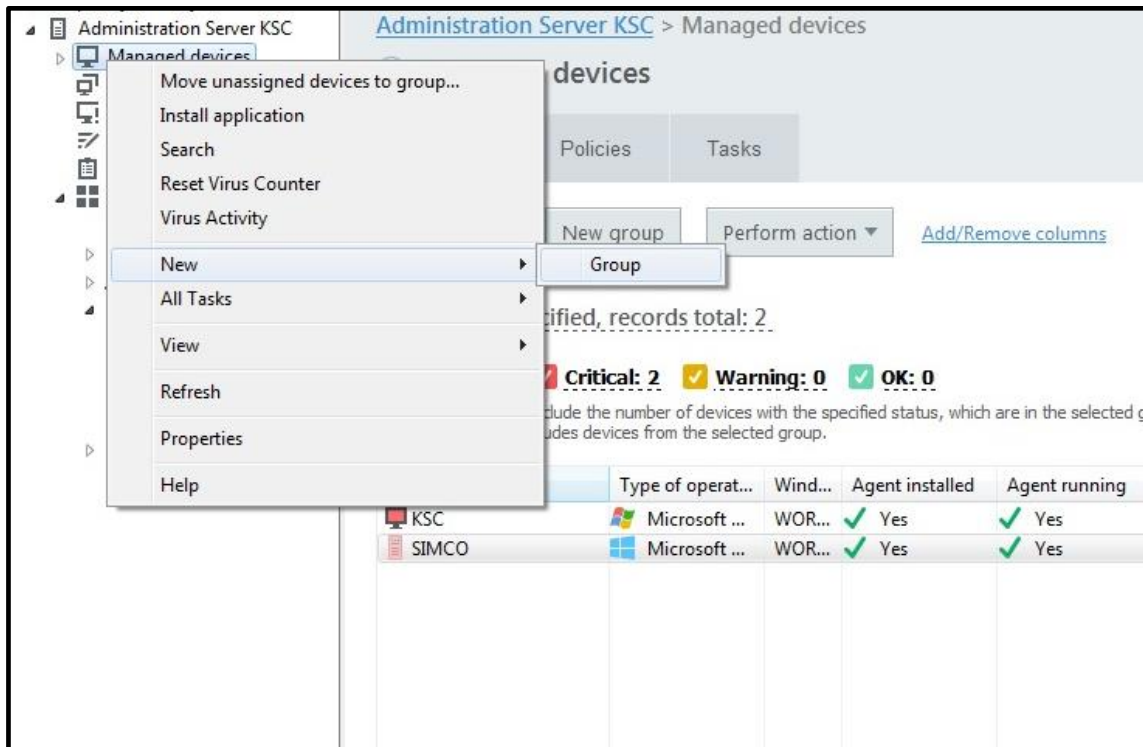
13. When the installation is complete, click **Finish**.



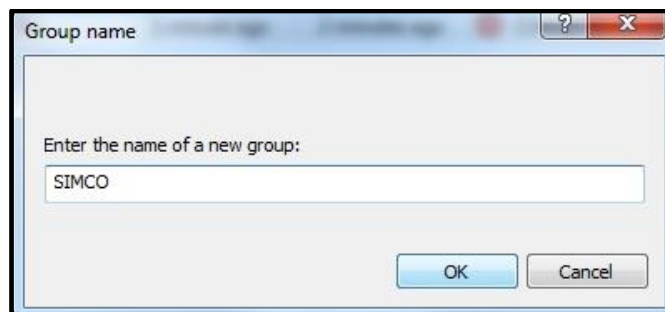
14. Now we go to the **Administration Server->Managed Devices** hierarchical node and switch to the **Devices** tab. Here we should see the host we have recently installed **KLnagent** onto (in our case, **SIMCO**).



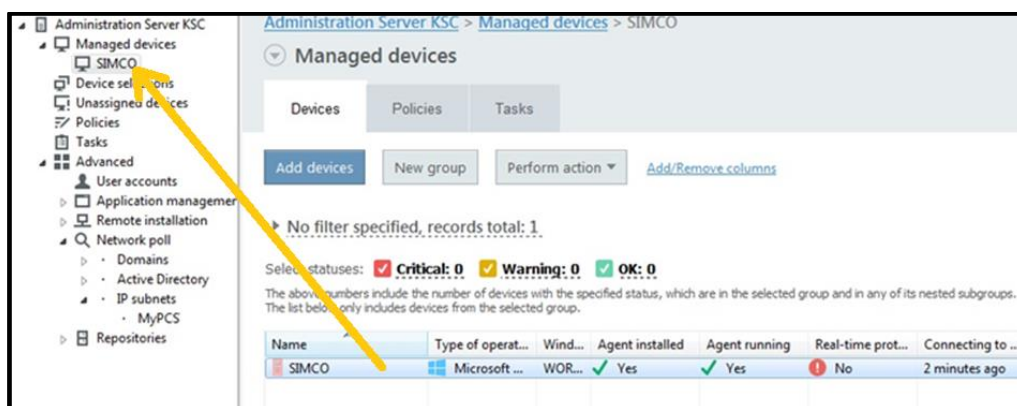
15. Right-click on **Administration Server->Managed Devices** and in the context menu select **New->Group**.



16. Give an intuitively clear name to a new group.



17. 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.



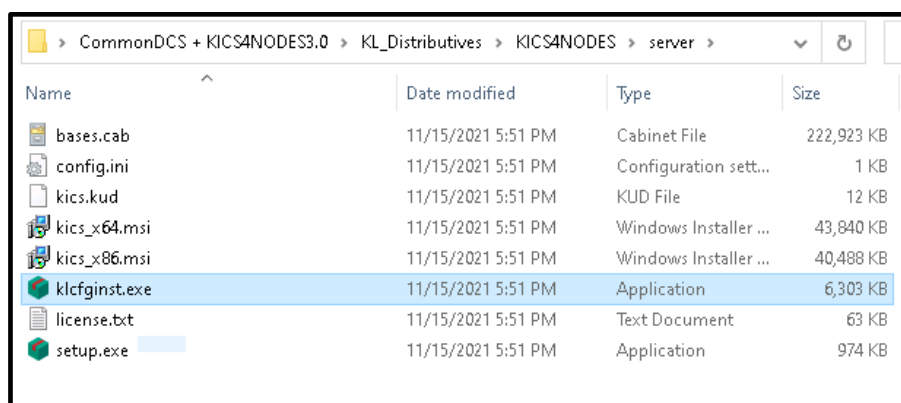
18. Do not forget to disable administrative access to the **C\$, D\$,...,ADMIN\$** shared folders compromising **SIMCO**. Once **KLNagent** has been installed on the target host, all further interactions will be carried out with the help of the network agent.

When it comes to structuring your scope of control system assets, it makes sense to group devices as per their functional purpose or their software composition. For example, if we had a redundant pair of **Process Historians** servers, we would assign both its master and standby units to the same group because redundant devices usually run the identical software. The point is that security policies or management tasks placed into a group affect every device belonging to this group. It is very convenient as similar devices do not need multiple policies and are normally managed in bulk.

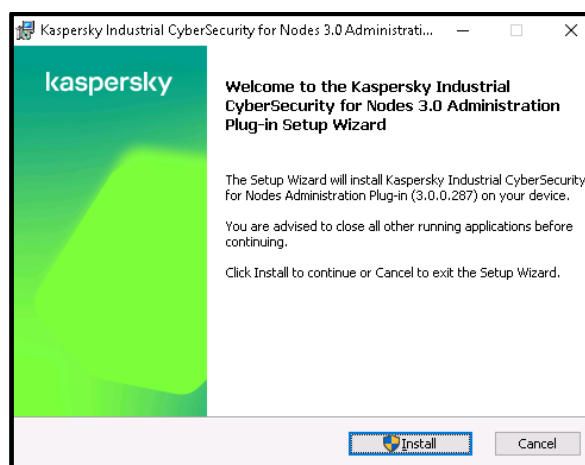
Installation of the KICS for Nodes management plugin

In order to enable remote administration of **KICS for Nodes** instances, we need to supplement **KSC** with **KICS for Nodes management plugin**, which is also part of the software distribution package.

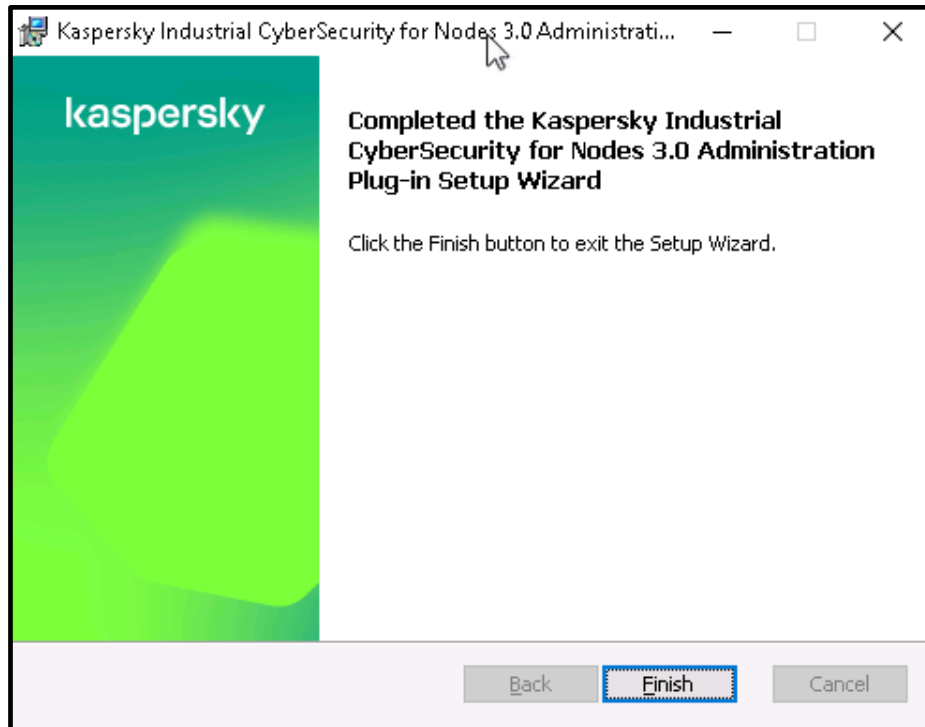
1. Locate **klcfginst.exe** in the **server** folder of the distribution package supplied and launch it.



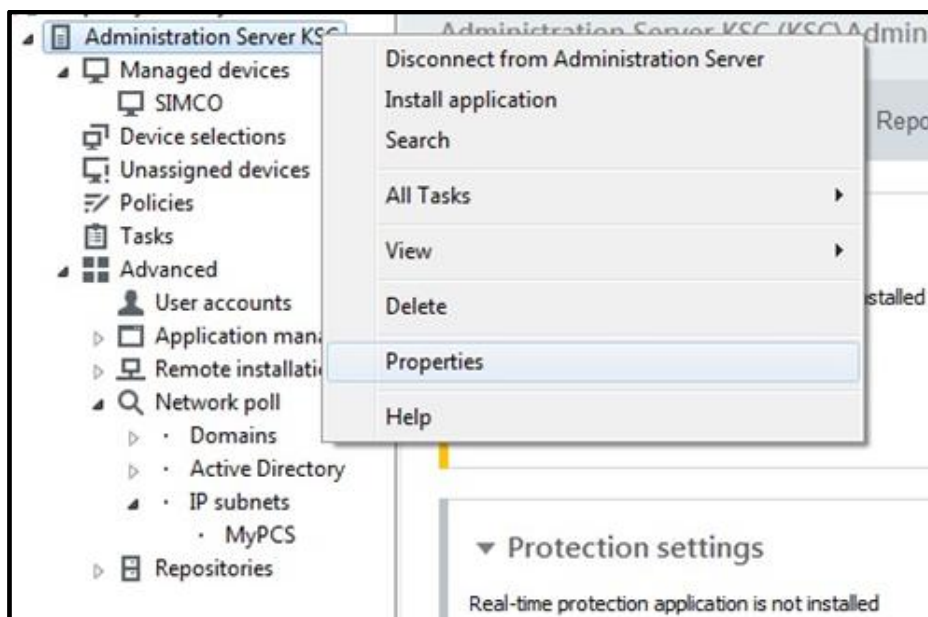
2. In the **Plug-in Setup Wizard** click **Install**. Elevate the user's rights if requested.



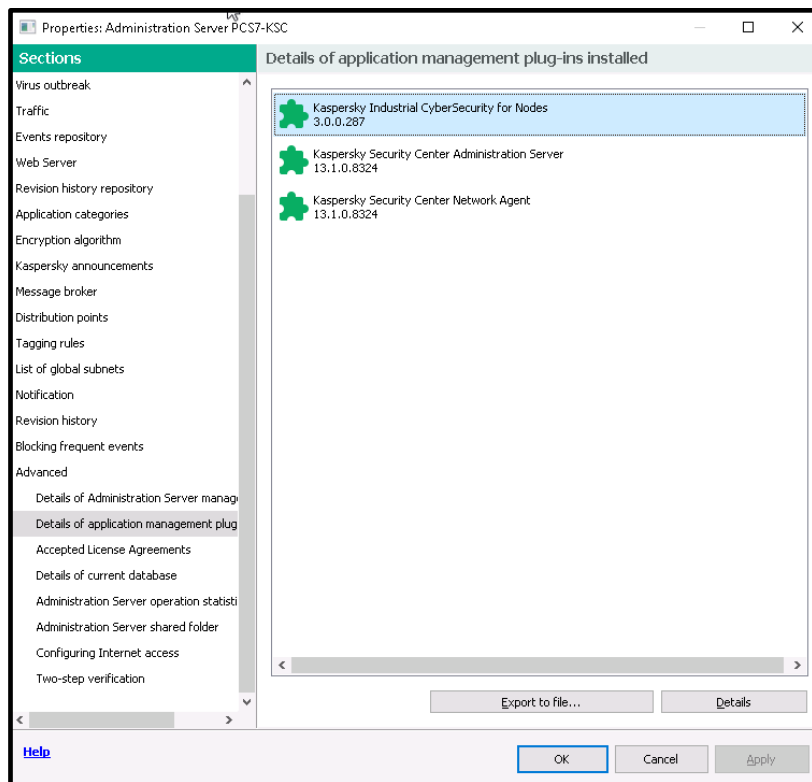
- Please wait patiently until the installation is completed. During the installation the user rights elevation may be requested, you should allow it. The installation process may run in the background for a while. Click **Finish** when the **Installation complete** window appears.



- 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.



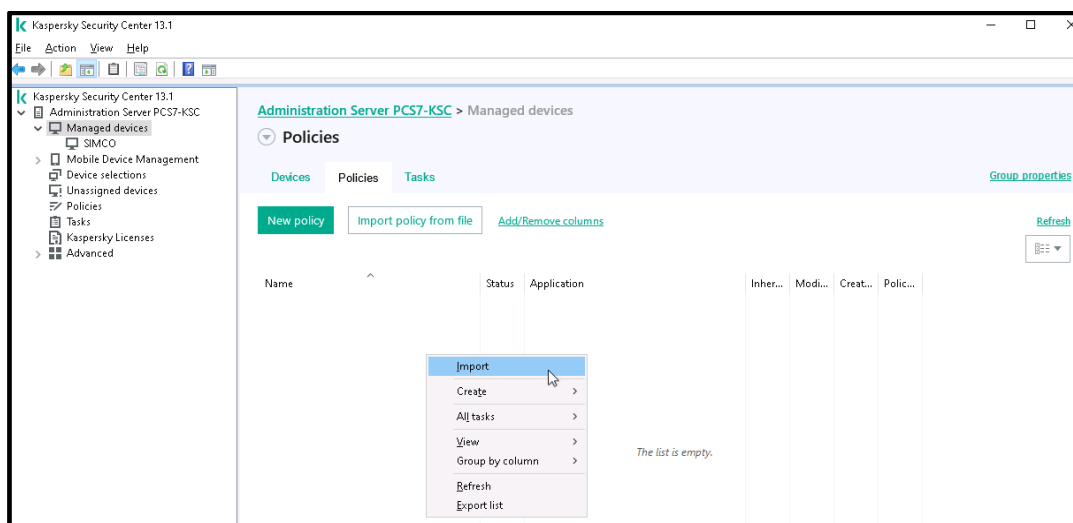
5. In the window that appears, go to **Advanced->Details of the application management plug-ins**. Make sure that the **Kaspersky Industrial CyberSecurity for Nodes 3.0.0.287** plugin is present.



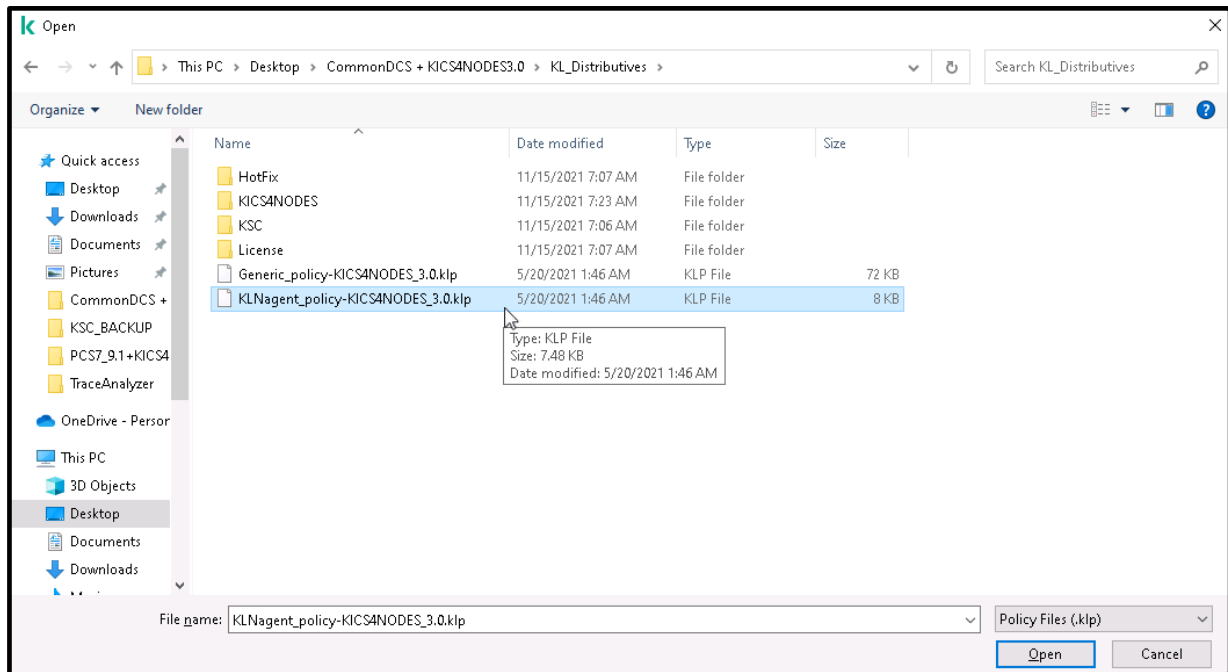
General configuration of the security policy for KLnagent

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

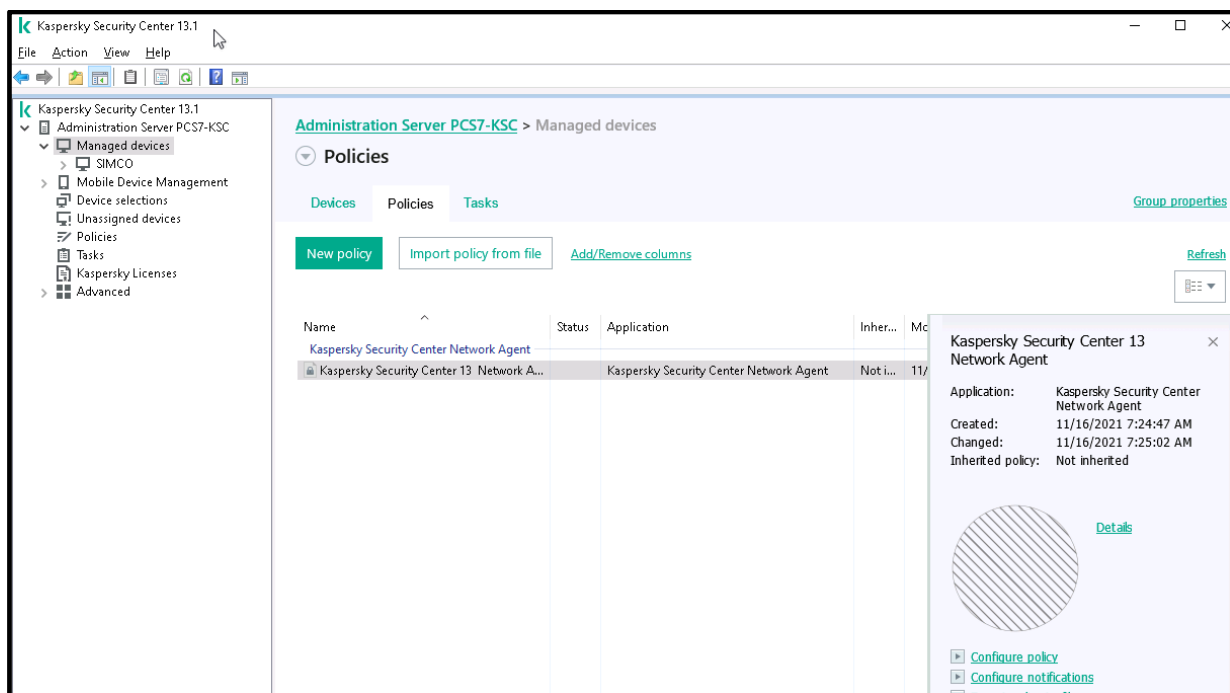
1. Go to **Administration Server->Managed Devices** and switch over to the **Policies** tab. Right-click on the **Policies** list and in the context menu select **Import**.



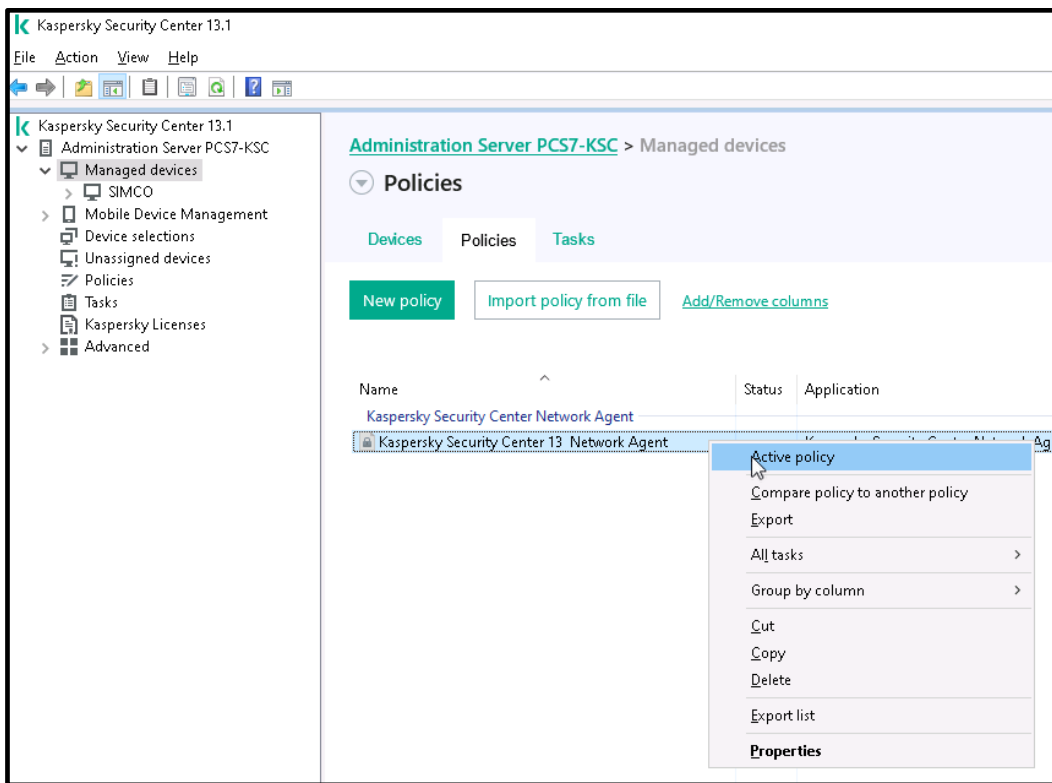
- Using the file browser, go to the distribution package and locate the **KLAgent_policy-KICS4NODES_3.0.klp** file as shown below. Click **Open**.



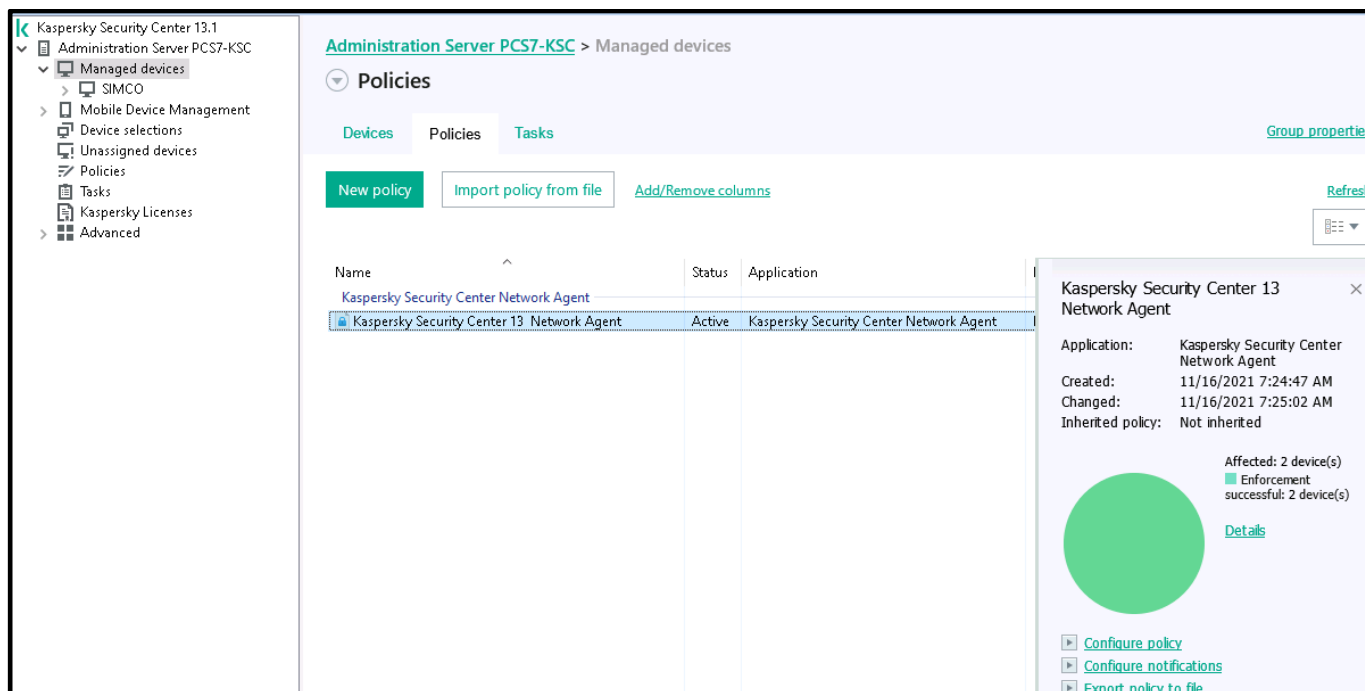
- The new **KLAgent** policy should immediately appear on the list. The policy applies to every host assigned to the top-level **Managed devices** group and to the derivative groups. By default, the newly created policy remains inactive until you put into force manually.



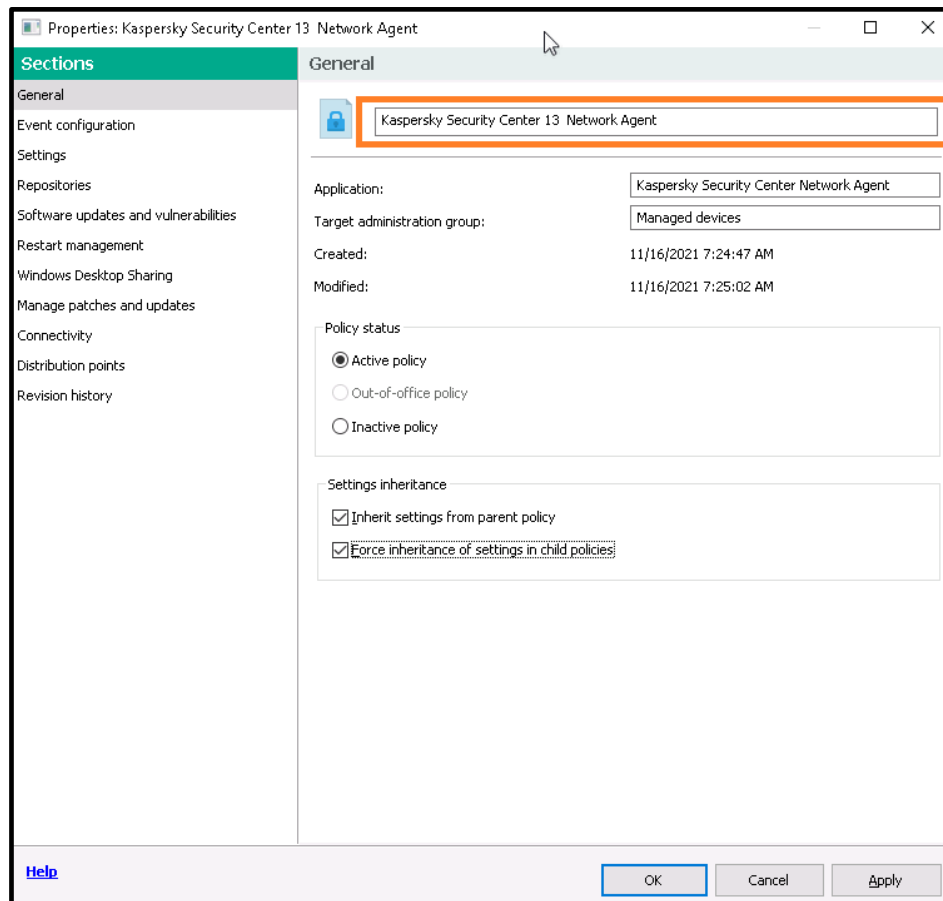
- Right-click on the just created policy and in the context menu choose **Active policy**.



- 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.



- If you are not OK with the default name of the policy, you can change it at any time. Right-click on the policy item and select **Properties** from the menu. Change the name in the highlighted field to any that suits you better and click **OK** to confirm the modification.



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 and also applies to every subsidiary group. It is reasonable because the **KLnagent** policy is likely to be the same for every existing or newly added device.

Configuring KICS for Nodes instances

As was mentioned earlier, the configuration of **KICS for Nodes** is carried out by means of security policies, which are applied to the target hosts. In case of a multi-node installation, the centralized deployment technique, enabled by **KSC**, helps to reduce deployment time and minimizes efforts because there is no need to switch from one computer to another.

As long as **KSC** is utilized, 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. For a while this generic (“backbone”) policy of **KICS for Nodes** remains the same for every control system host because it excludes any device-specific white lists. Later on, we

have to “personalize” our generic policy for each workstation (**SIMCO**, in our example) by supplementing specific white lists for **Application launch control** and **Device Control**.

When it comes to **Application launch control** and **Device Control**, some preparation should be made prior to switching on these features. This involves 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 3.0** configuration routine will comprise the following sequential steps:

- Import of the generic (optimized, “backbone”) policy for **KICS for Nodes** from the **Generic_policy-KICS4NODES_3.0.klp** file supplied as a part the distribution package.
- Remote installation of **KICS for Nodes 3.0** onto the target hosts.
- Remote installation of **Hotfix**⁵ onto the target hosts.
- Initial update of antivirus databases.
- Performing the **On-Demand** scan 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 **File Operations Monitor** and **Network Threat Protection**.
- Setting up **PLC Integrity Checker**, providing that there are supported **PLCs** installed on your production site.

Import of the generic policy for KICS for Nodes

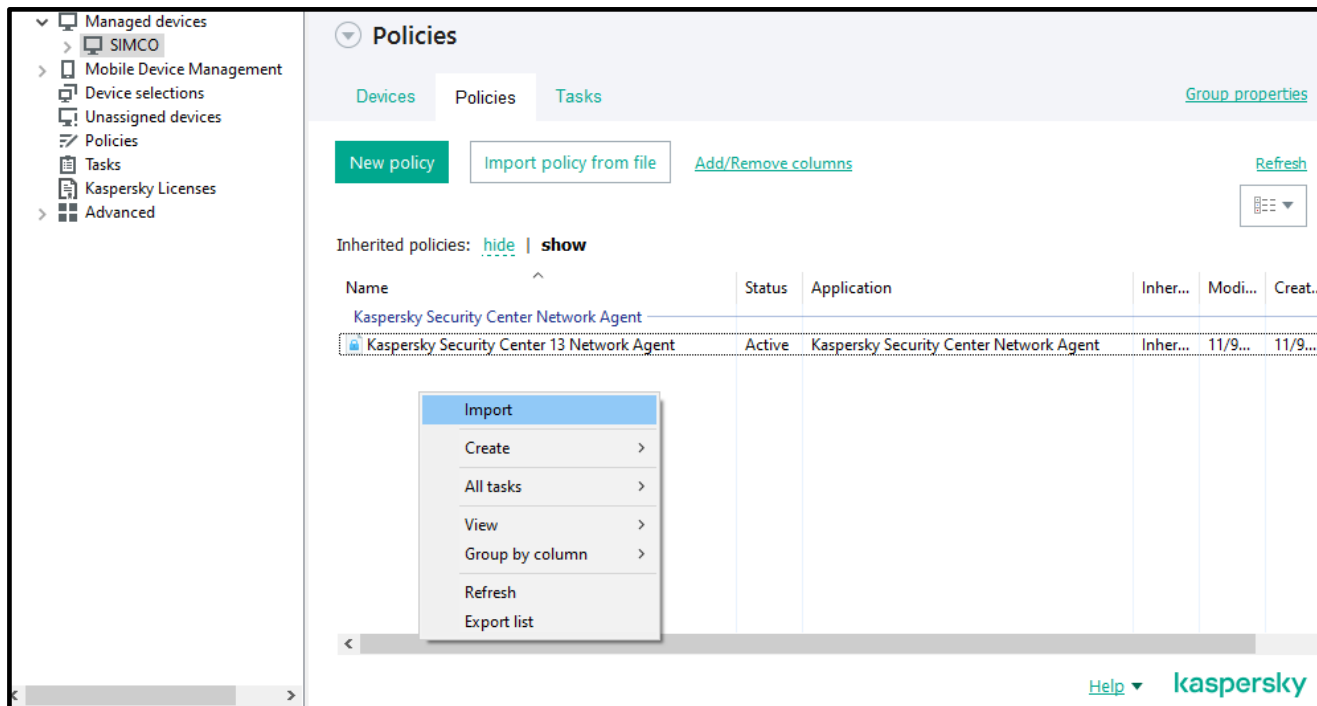
KICS for Nodes configuration should be carried out in strict accordance with operational and security requirements of your control system. It is crucial to consider the preservation of DCS operational characteristics to be the top priority!

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** settings optimized for this or that brand and version of the control system (so make sure to get a distribution package adequate for your control system!). Once the security policy is complete, we will activate the pending protection modules (**Application Launch Control**, **Device Control**).

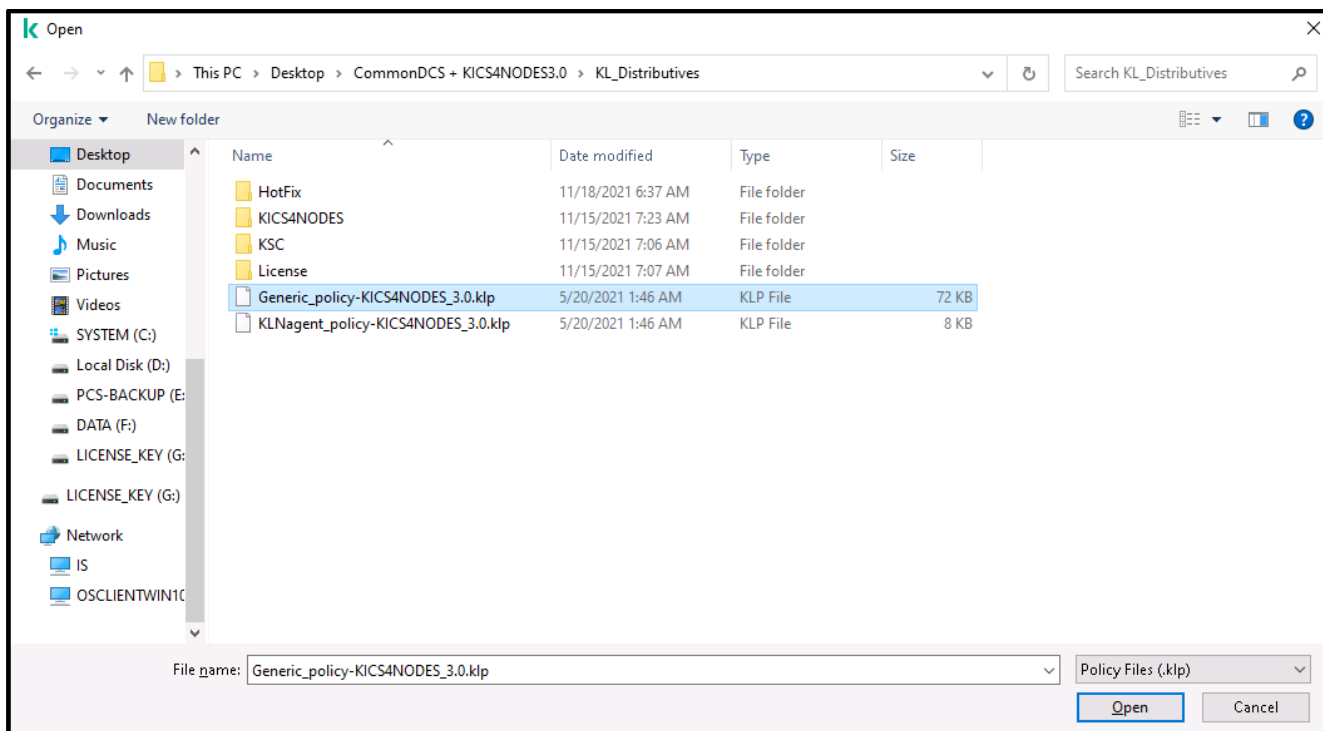
⁵ If **KICS for Nodes** is deployed onto critical infrastructure production sites located in Russia, the **Hotfix** installation may not be compulsory. Please refer to the “FSTEK certification for **KICS for Nodes** installations within the territory of Russia” section.

Please follow the following steps to create the generic policy for **KICS for Nodes**.

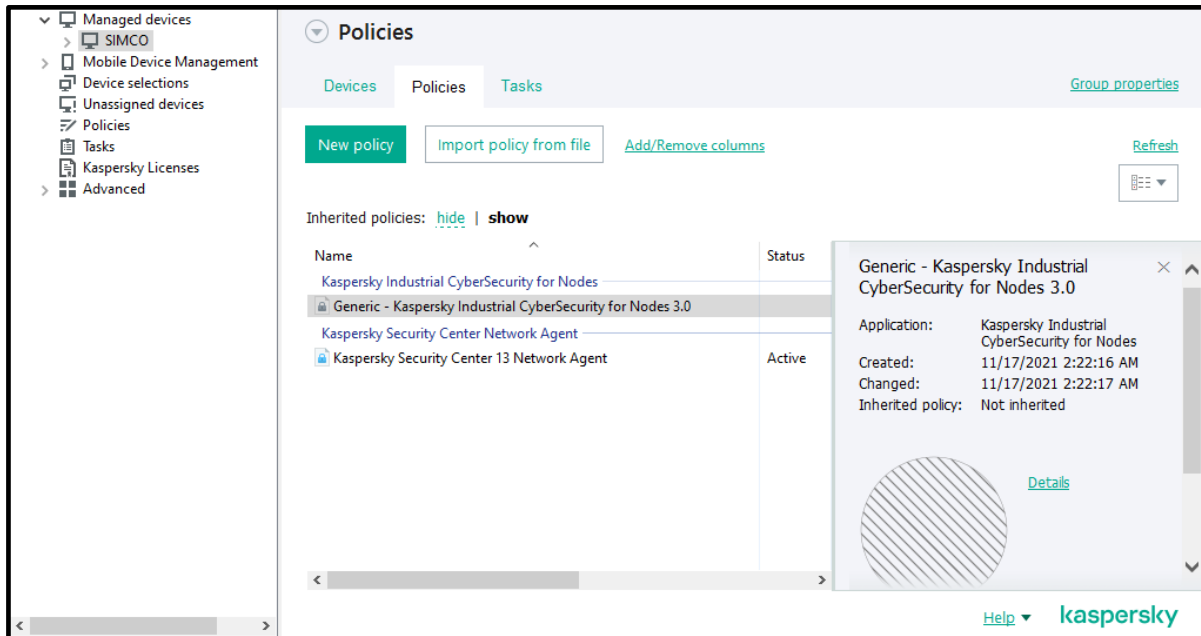
1. Dip into the subsidiary device group, which contains our target host (in our case, **SIMCO**). Switch over to the **Policies** tab. Start importing a new policy in exactly the same manner as we did before with **KLAgent**.



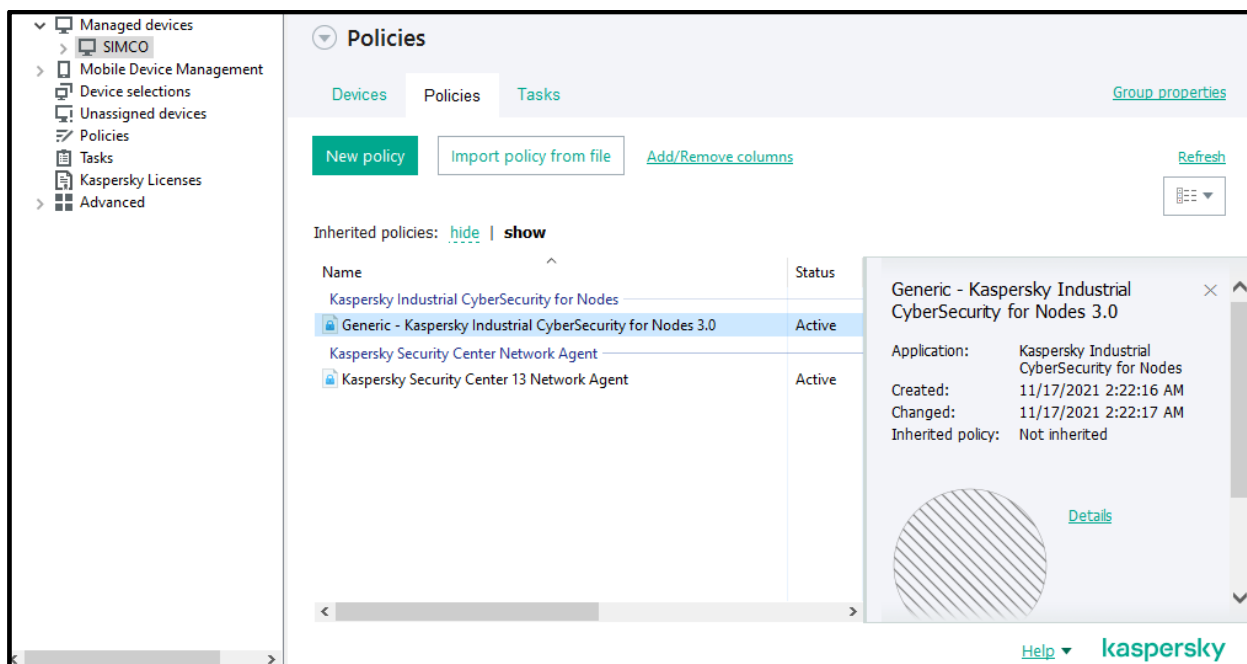
2. Using the file browser, go to the distribution package and locate the **Generic_policy-KICS4NODES_3.0.klp** file as shown below. Click **Open**.



- The new **KICS for Nodes** policy should appear on the list of the policies. Obviously, it solely applies to the hosts assigned to the **SIMCO** subgroup. By default, the newly created policy remains inactive until you put into effect manually.



- 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.
- This time the right-hand pane chart will not turn green, because **KICS for Nodes** application is not installed on the **SIMCO** host yet.



At this stage, the **KICS for Nodes** policy incorporates only general security settings, which are, nevertheless, optimized for your process control system. Later, we will revert to this policy in order to make it more specific to the **SIMCO** host in terms of whitelisting.

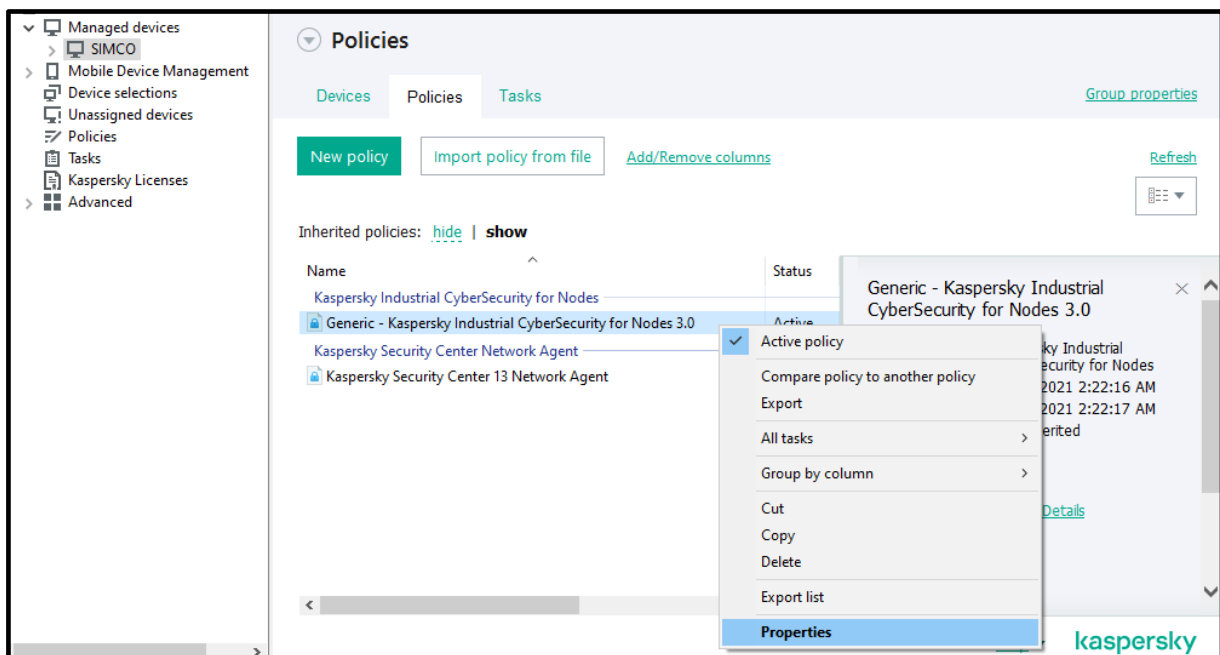
Settings of KICS for Nodes generic policy

Generally speaking, the policy settings may vary significantly depending on the model and even version of your control system stuff. Obviously, there can be no unified policy.

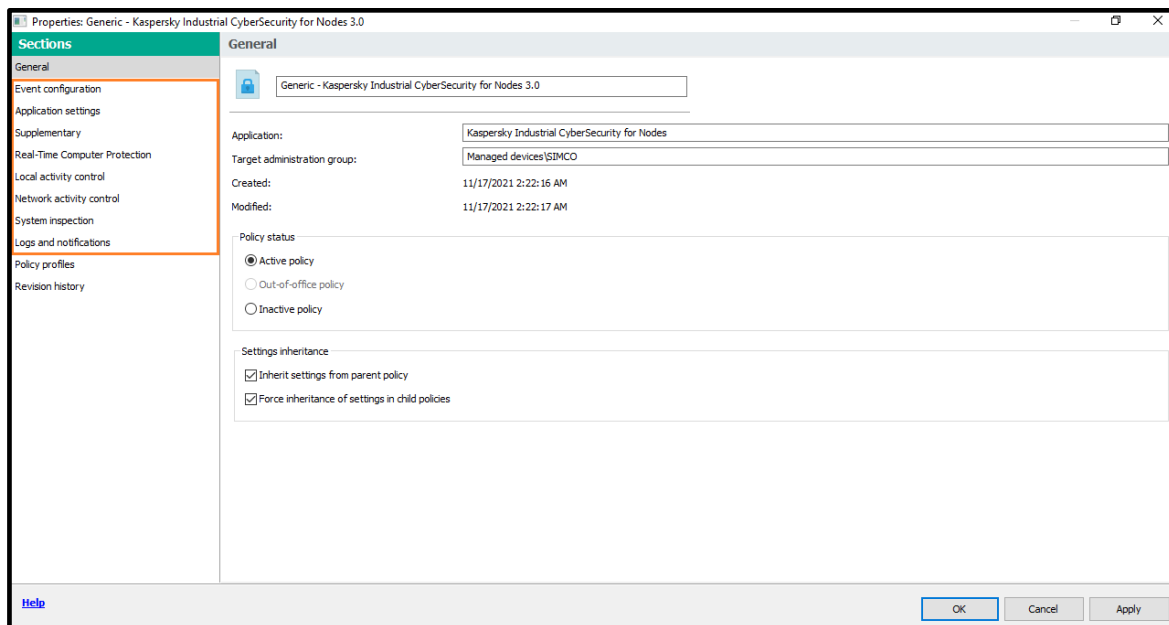
However, there is a minor subset of the policy settings which remains more or less invariant regardless of which automation system you use. These are so called “soft” settings that should not generally cause adverse effects on the control system characteristics. So, let us look through some of them without getting into details.

In order to inspect or modify the policy settings you should:

1. Right-click on the policy you are interested in and select **Properties** from the menu that has appeared.

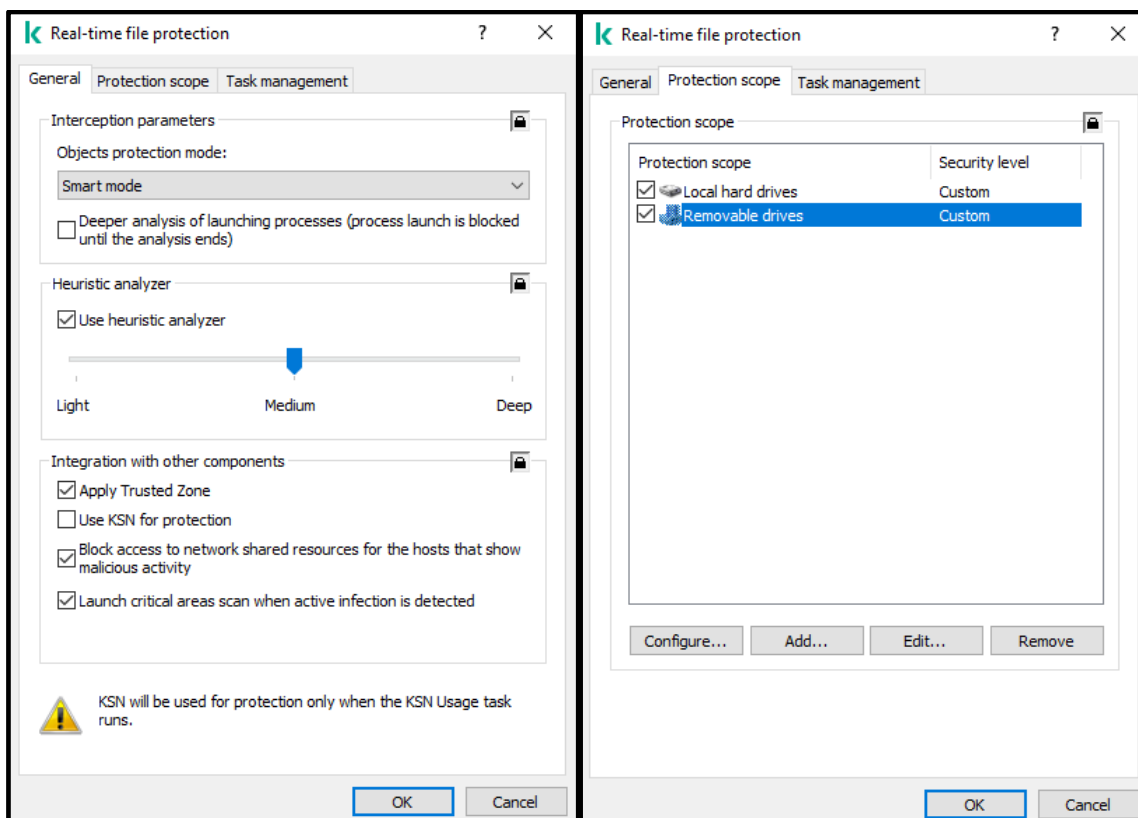


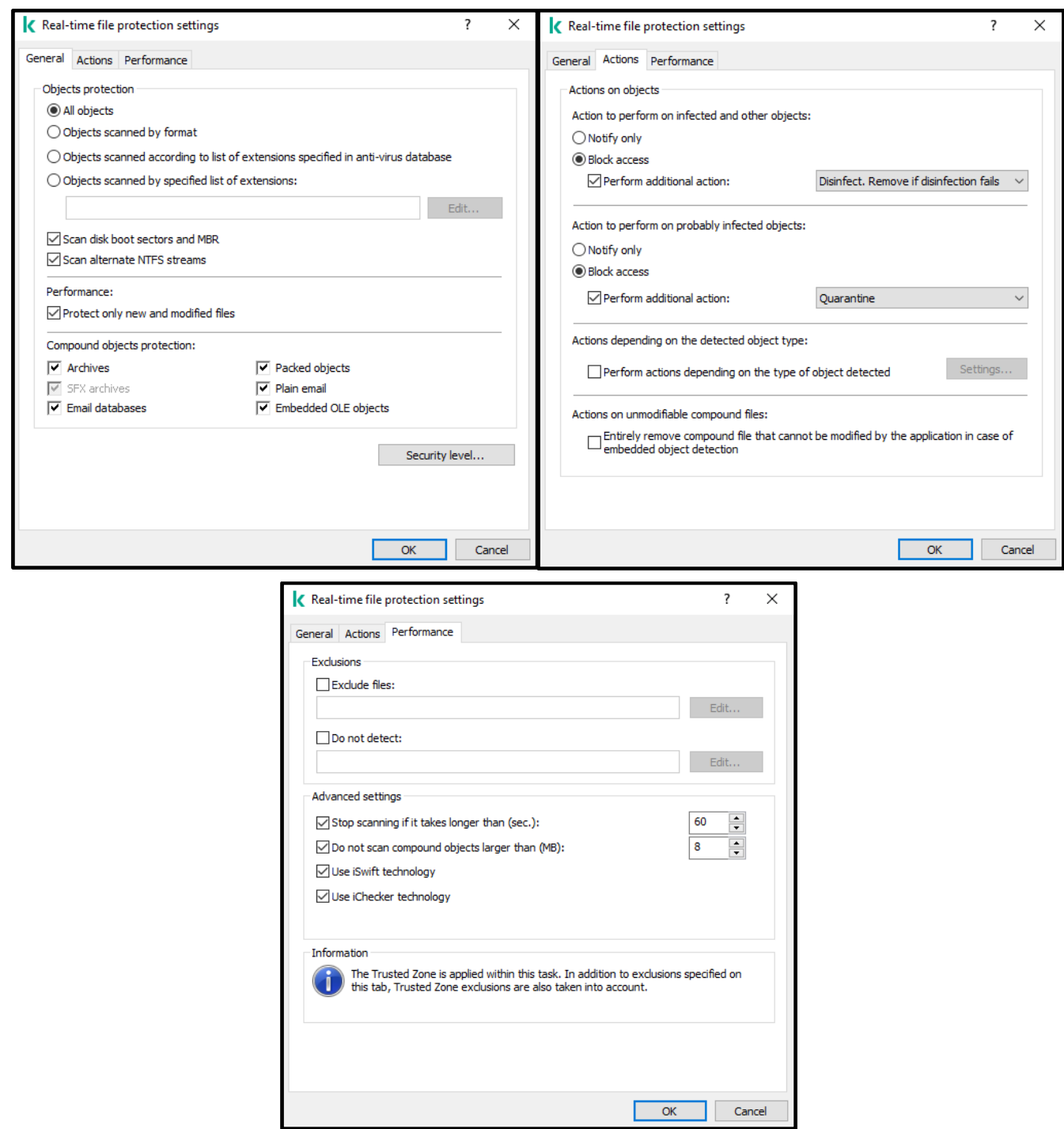
- The policy settings can be found in the left-hand sections highlighted in the screenshot below.



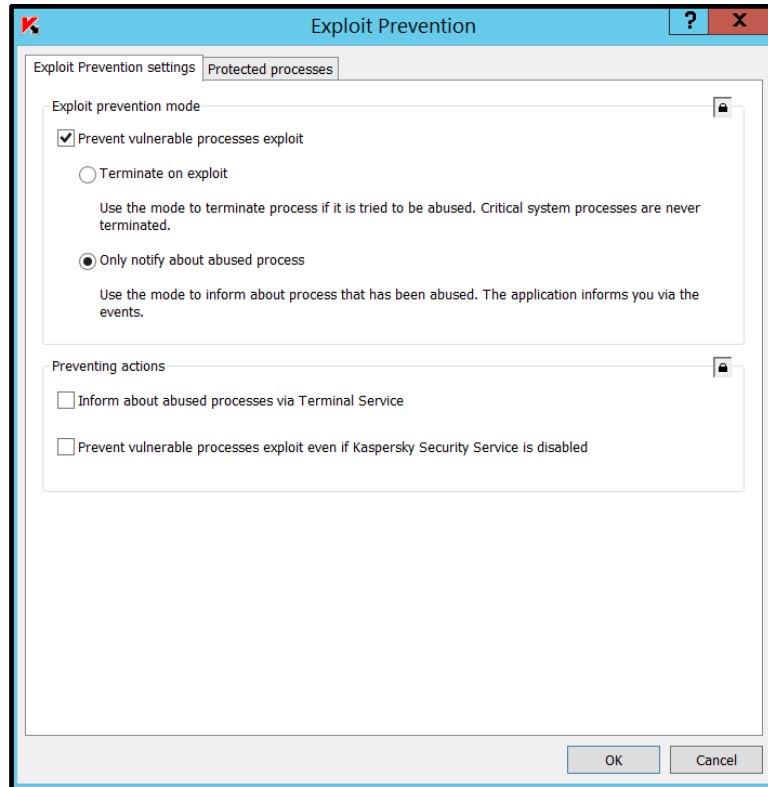
So now, let us have a glance at some of the most important settings contained in **Generic_policy-KICS4NODES_3.0.klp**:

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

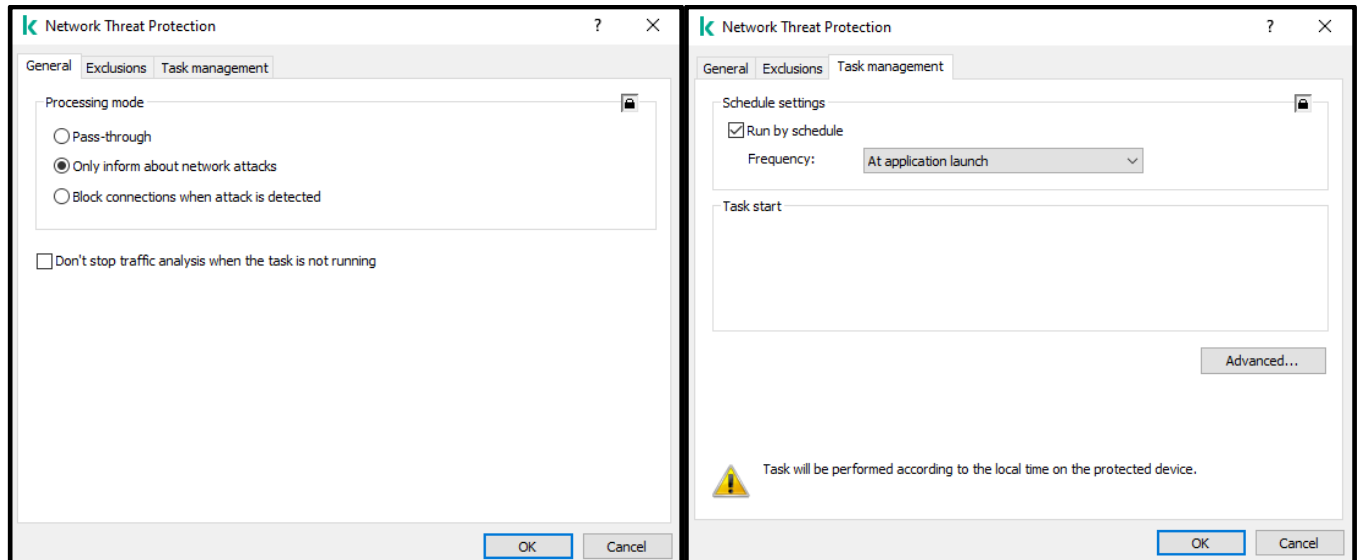




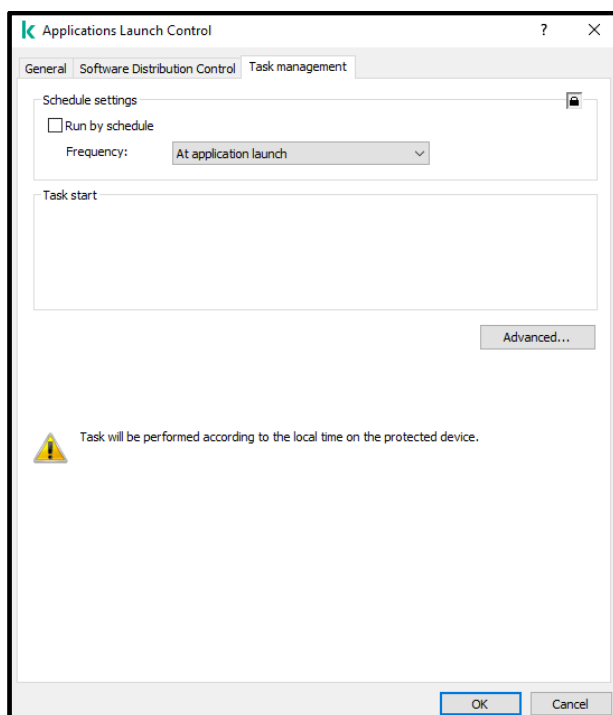
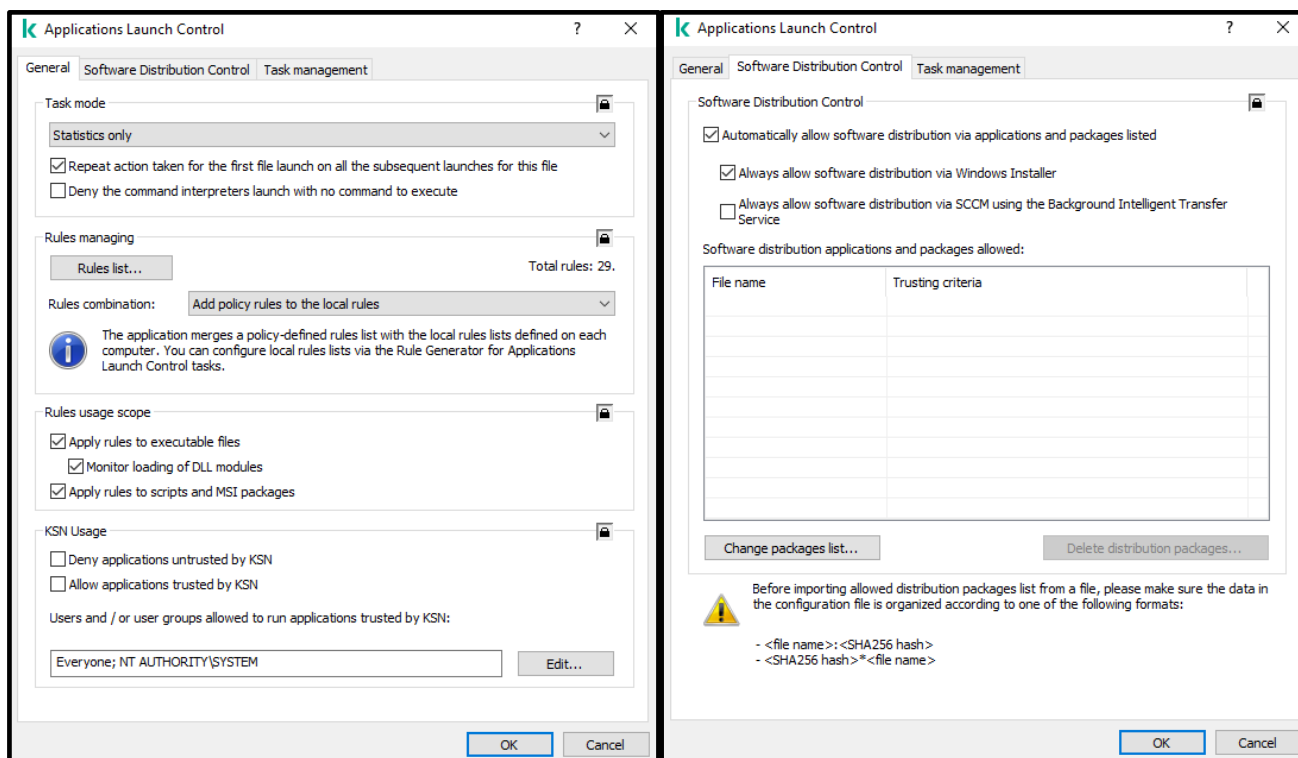
2. **Kaspersky Security Network (KSN)** is disabled.
3. **Exploit Prevention** settings are as shown in the screenshot below:



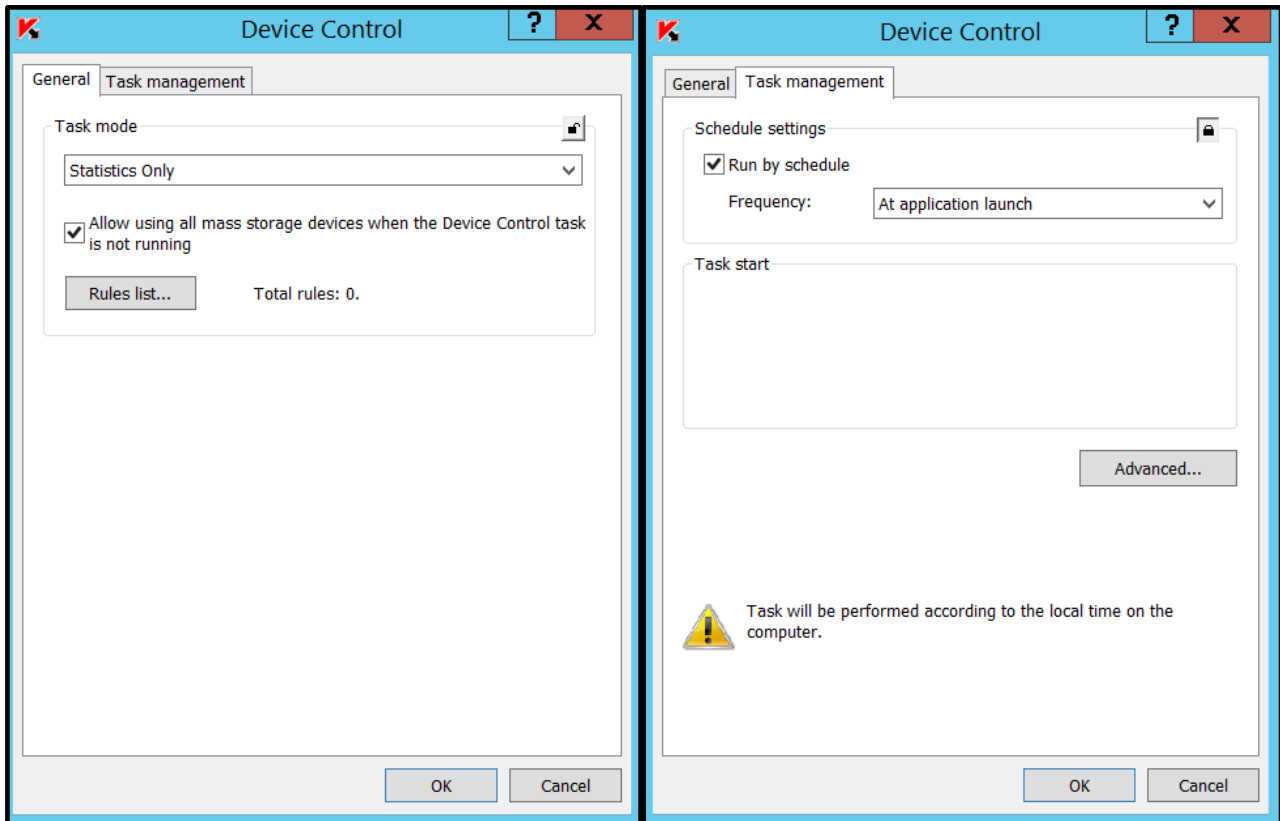
4. **Network Threat Protection** settings are as shown in the screenshot below:



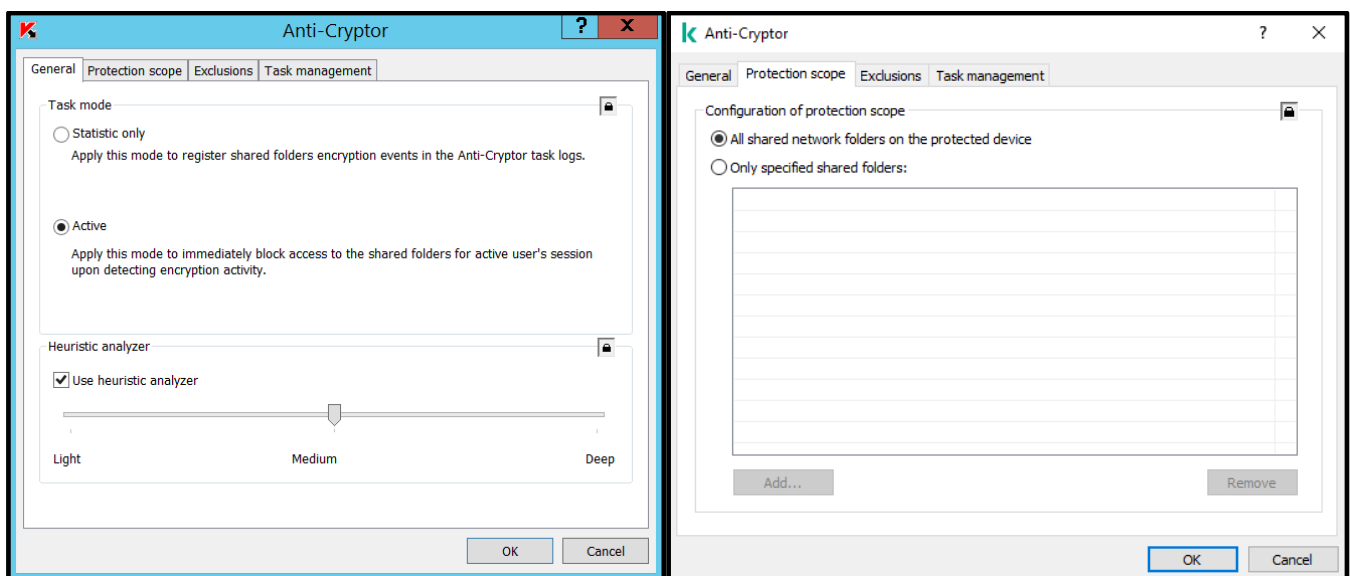
5. **Application Launch Control** settings are shown in the screenshots below. Please note that the rule list (commonly referred to as “white list”) is not always empty. According to Kaspersky experts’ research, some control systems tend to dynamically create scripts during runtime. So, it is better not to modify the default contents of the list. Also note that at this stage the task itself should be disabled but we will switch it on a bit later.

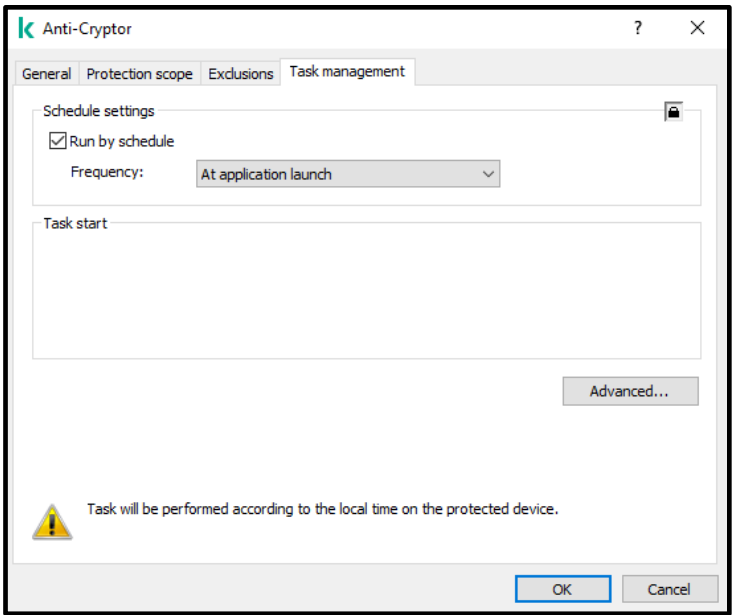


6. **Device Control** settings are as shown in the screenshots below. Please note that the task is already activated with a blank white list, which implies alerting any USB storage device plugged in. Similar to **Application Launch Control**, the white list for **Device Control** is to be filled up later.

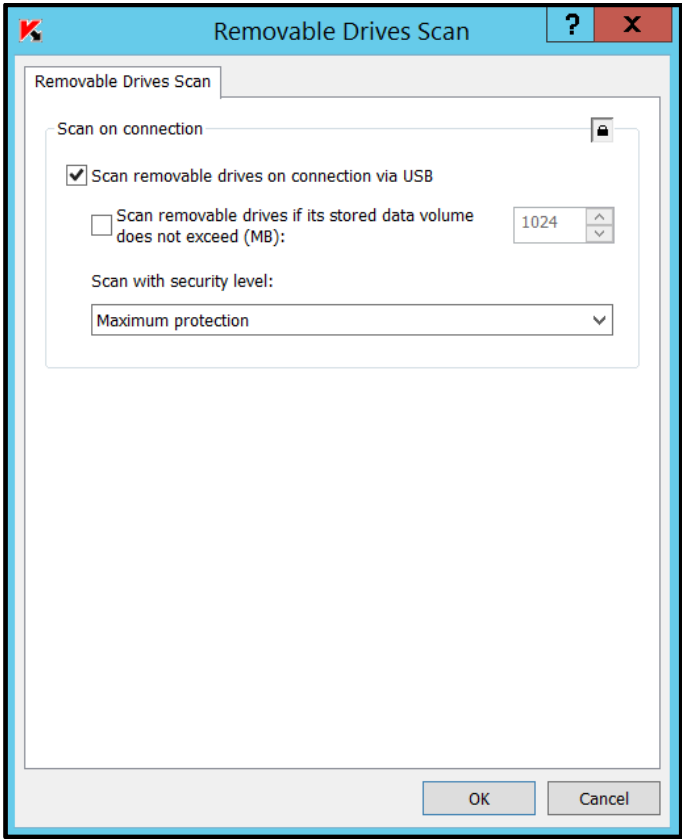


7. **Wi-Fi Control** is disabled.
8. **Firewall Management** is disabled.
9. **Anti-Cryptor** settings are as shown in the screenshot below:



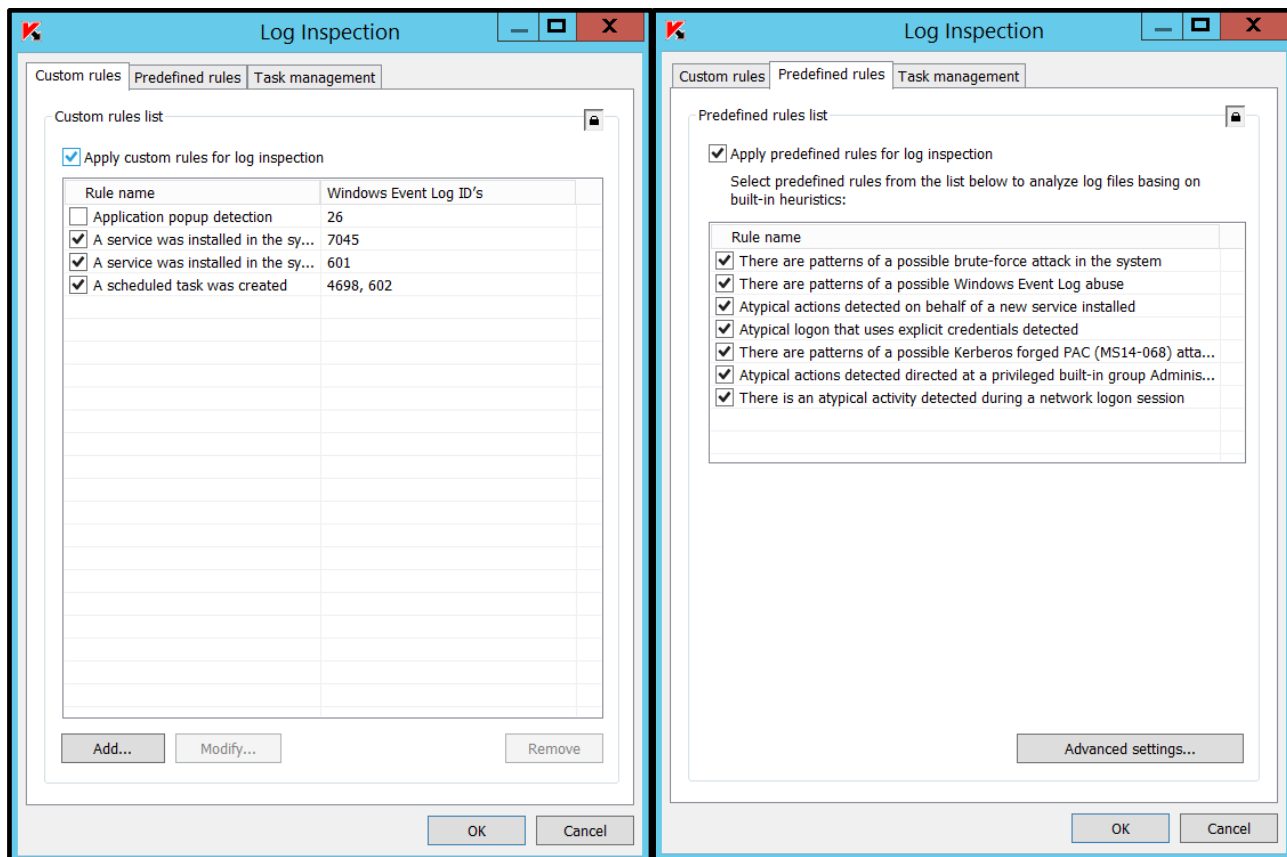


10. Removable Drives Scan settings are as shown in the screenshot below:

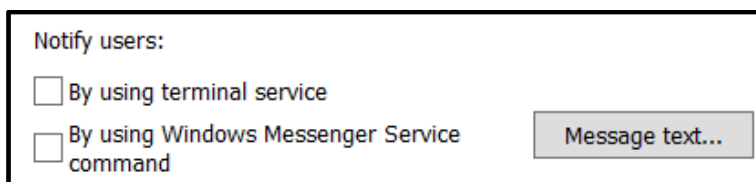


11. File Integrity Monitor is disabled.

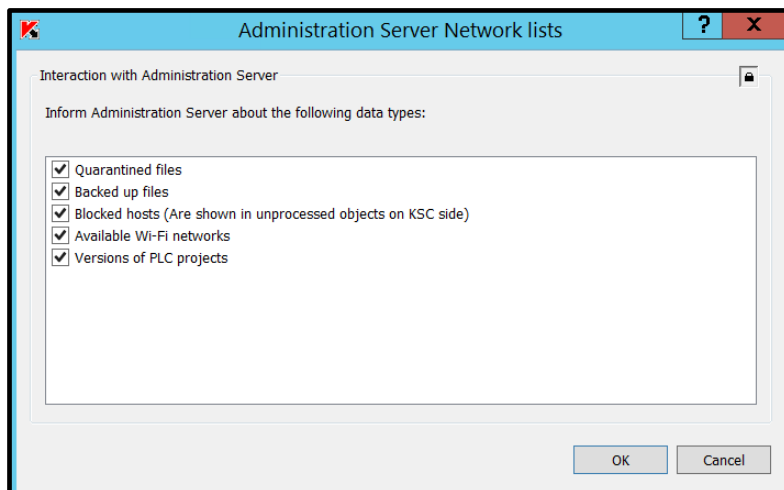
12. **Log Inspection** settings are as shown in the screenshot below:



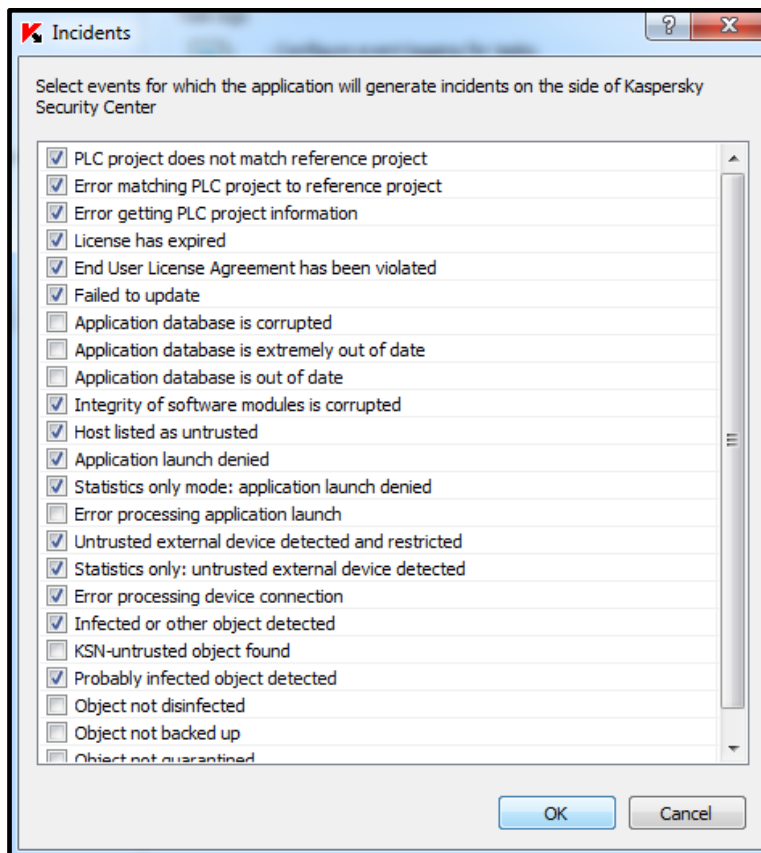
13. In **Logs and notifications->Event notifications** for each event type the following options are unchecked:



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



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



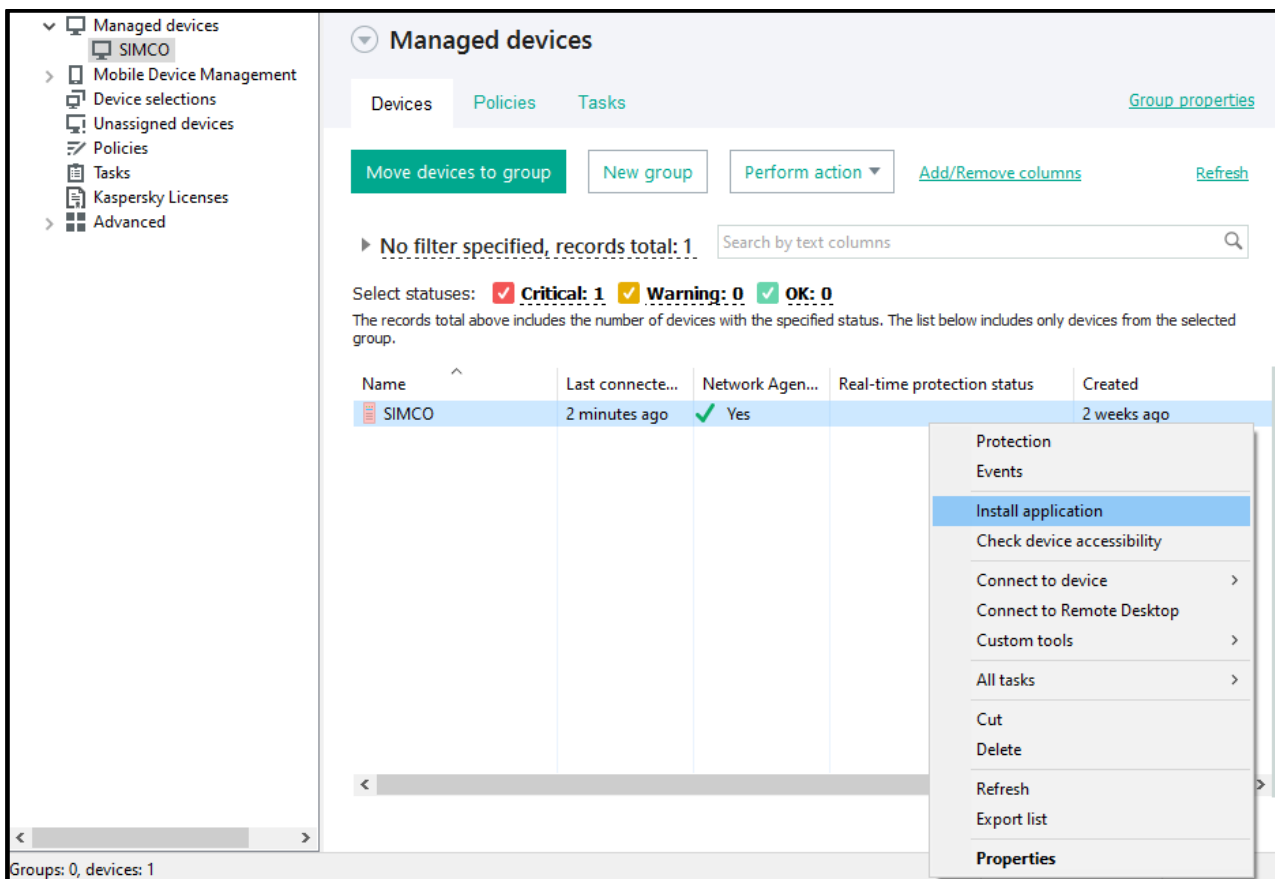
If specific antivirus exclusions have been provided by an automation vendor, they can be found in **Supplementary->Trusted Zone->Exclusions** and **Supplementary->Trusted Zone->Trusted Processes** accordingly. Normally such fine-tuning slightly improves overall performance.

Prior to proceeding to the next steps, please inspect all the policy settings 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. Remain in the newly created device group (**SIMCO**, in our case) and locate the managed device we have installed **KLnagent** on (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.



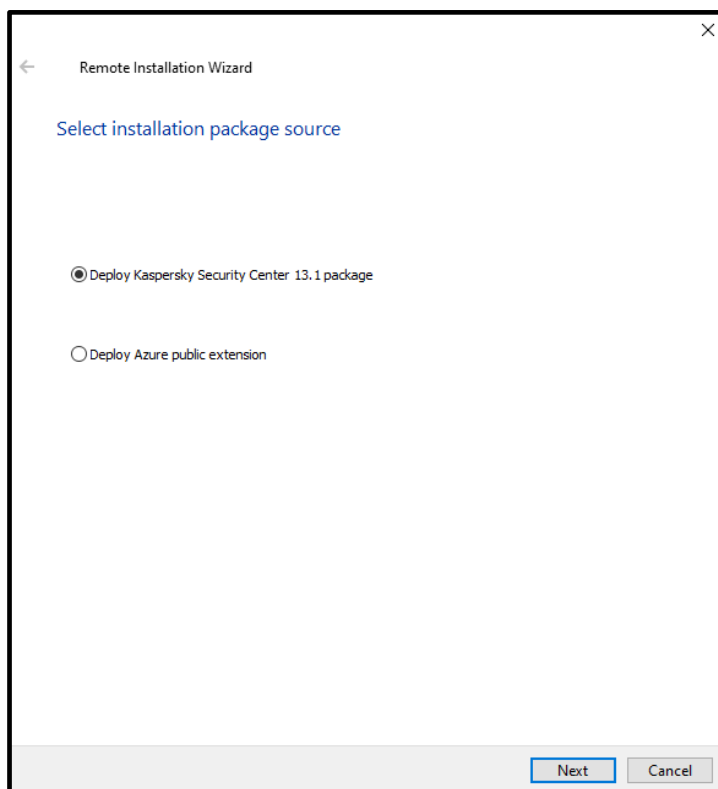
The screenshot shows the Kaspersky Mobile Device Management (MDM) console interface. On the left is a navigation pane with categories like 'Managed devices', 'Mobile Device Management', 'Device selections', 'Unassigned devices', 'Policies', 'Tasks', 'Kaspersky Licenses', and 'Advanced'. The main area is titled 'Managed devices' and has tabs for 'Devices', 'Policies', and 'Tasks'. Below the tabs are buttons for 'Move devices to group', 'New group', 'Perform action', 'Add/Remove columns', and 'Refresh'. A search bar is present with the text 'No filter specified, records total: 1'. Below this, status filters are shown: 'Select statuses: ☒ Critical: 1 ☒ Warning: 0 ☒ OK: 0'. A note states: 'The records total above includes the number of devices with the specified status. The list below includes only devices from the selected group.' A table lists the managed devices:

Name	Last connecte...	Network Agen...	Real-time protection status	Created
SIMCO	2 minutes ago	✓ Yes		2 weeks ago

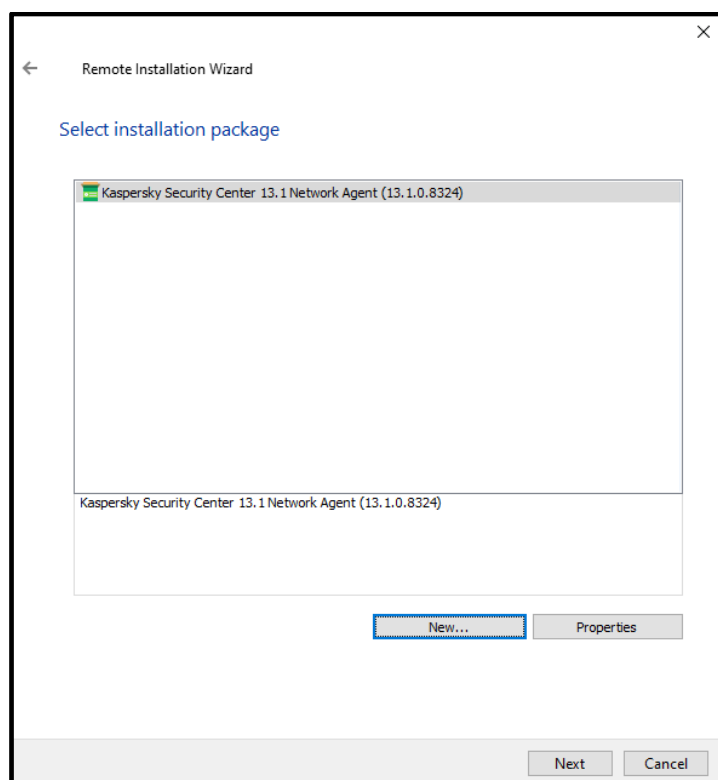
A right-click context menu is open over the 'SIMCO' device row. The menu items are: Protection, Events, **Install application** (highlighted), Check device accessibility, Connect to device, Connect to Remote Desktop, Custom tools, All tasks, Cut, Delete, Refresh, Export list, and Properties.

At the bottom left, it says 'Groups: 0, devices: 1'.

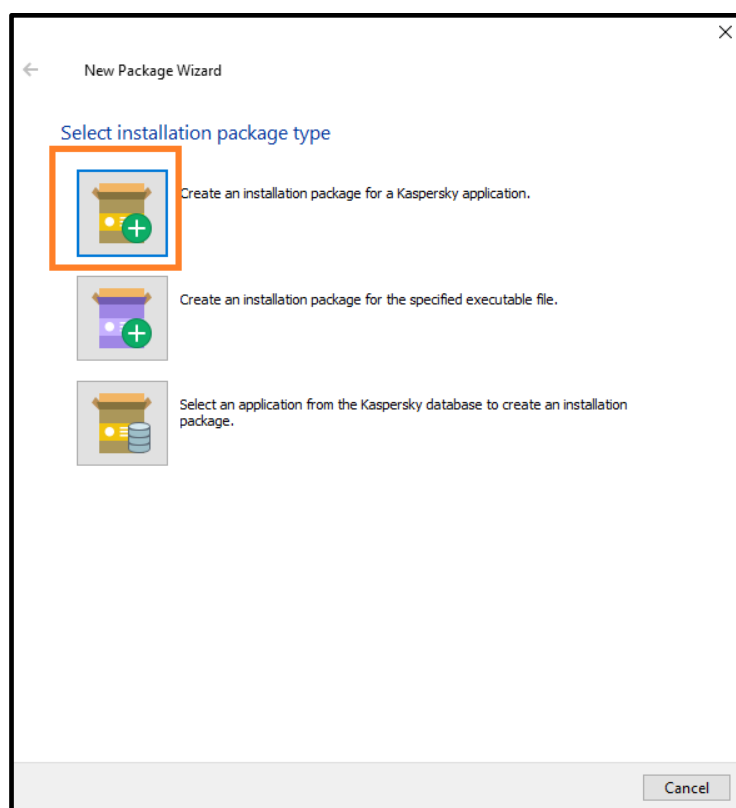
2. In the **Select installation package source** window select **Deploy Kaspersky Security Center 13.1** package and click **Next**.



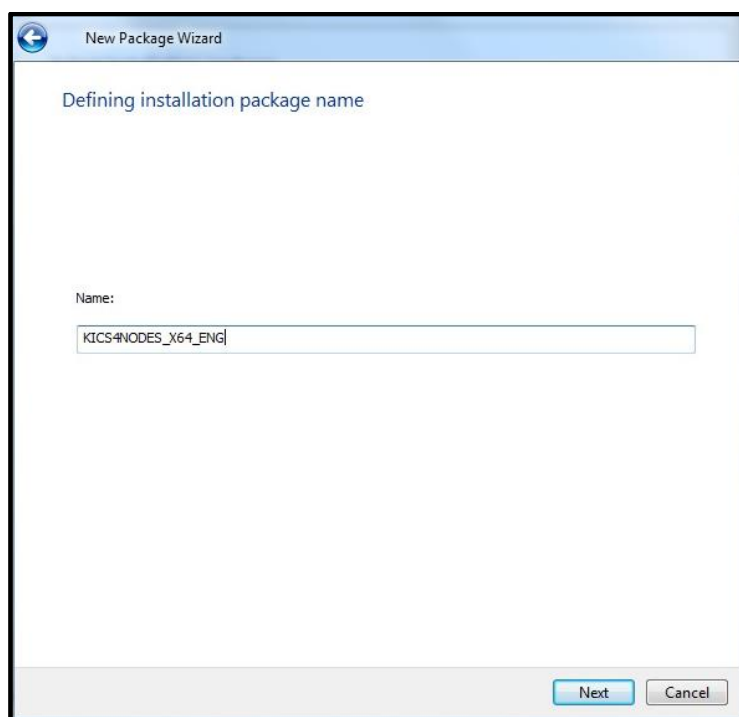
3. In the **Select installation package** window press the **New...** button.



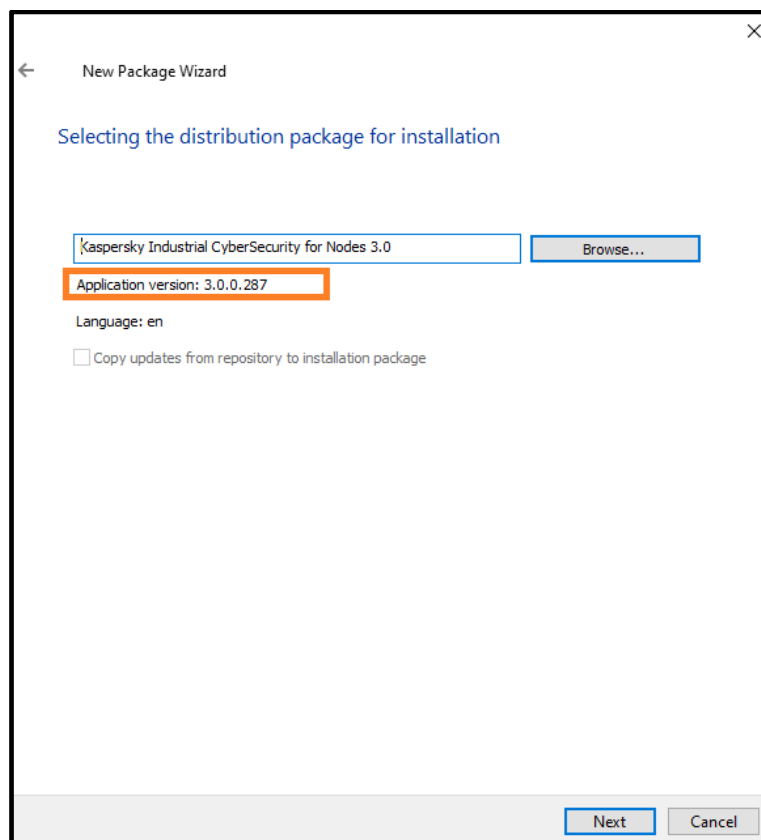
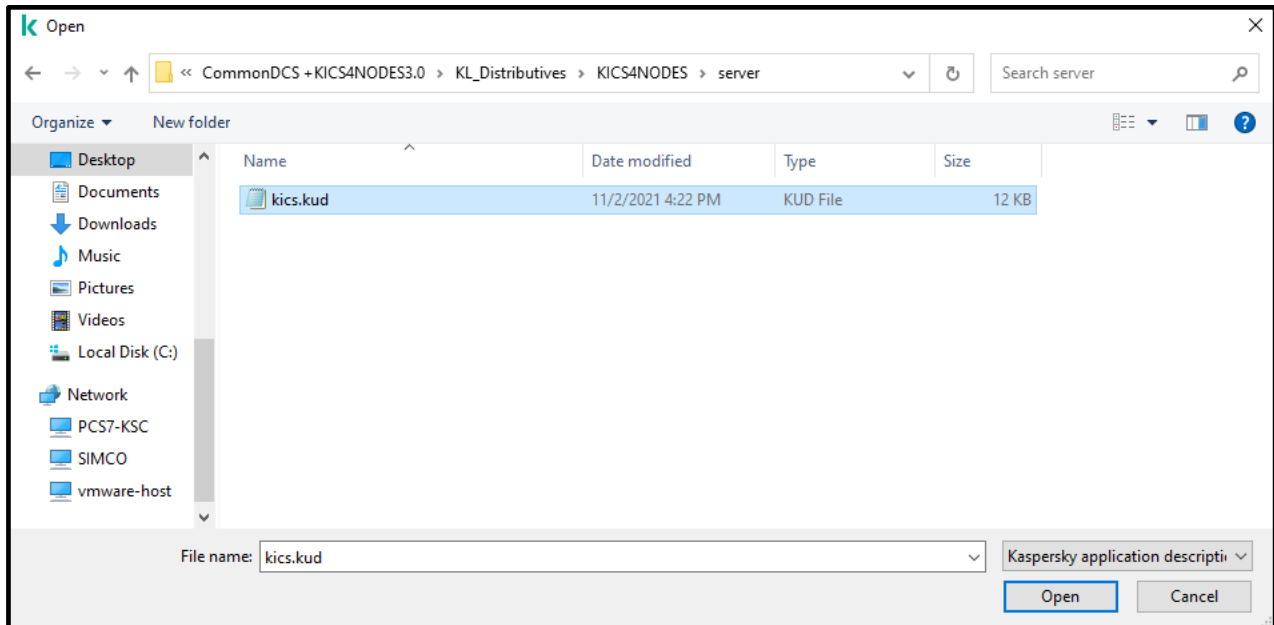
- Click the **Create Installation package for a Kaspersky Lab application** button.



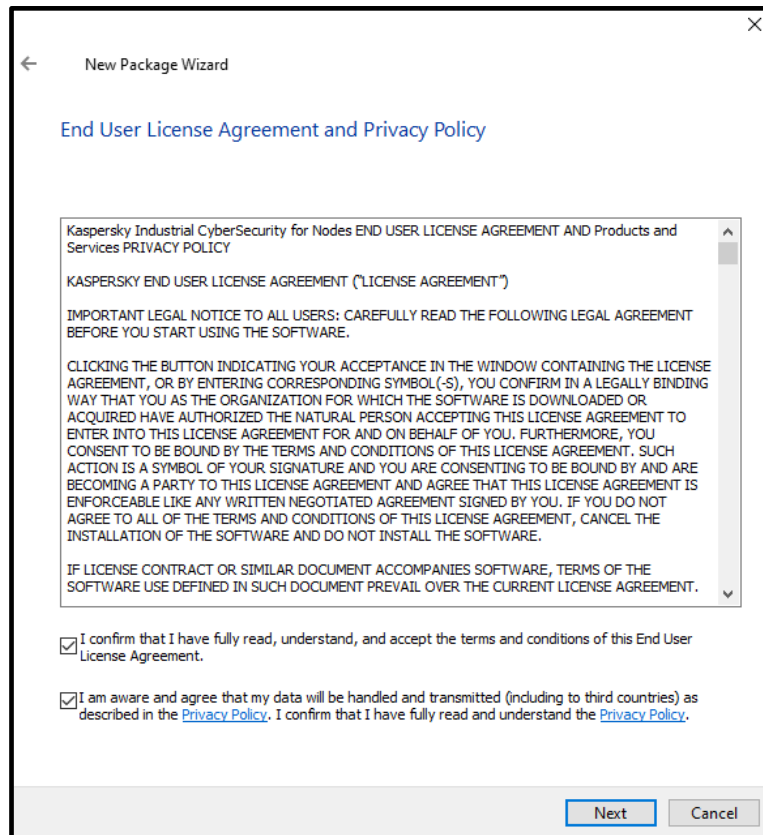
- Give a name to the newly created installation package (**KICS4NODES_X64_ENG**, in our case). Click **Next**.



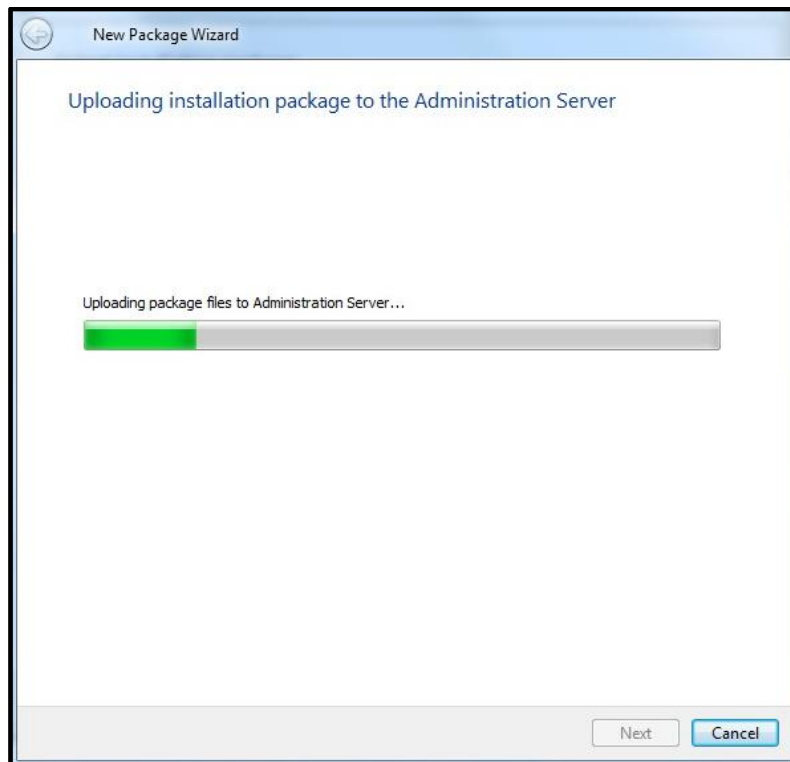
- In the **Selecting the distribution package for installation** window click **Browse** to locate the **kics.kud** file, which is located in **KL_Distributives\KICS4NODES\server** of the distribution package. After you open it make sure that the application version is displayed as **3.0.0.287**. Click **Next** to continue.



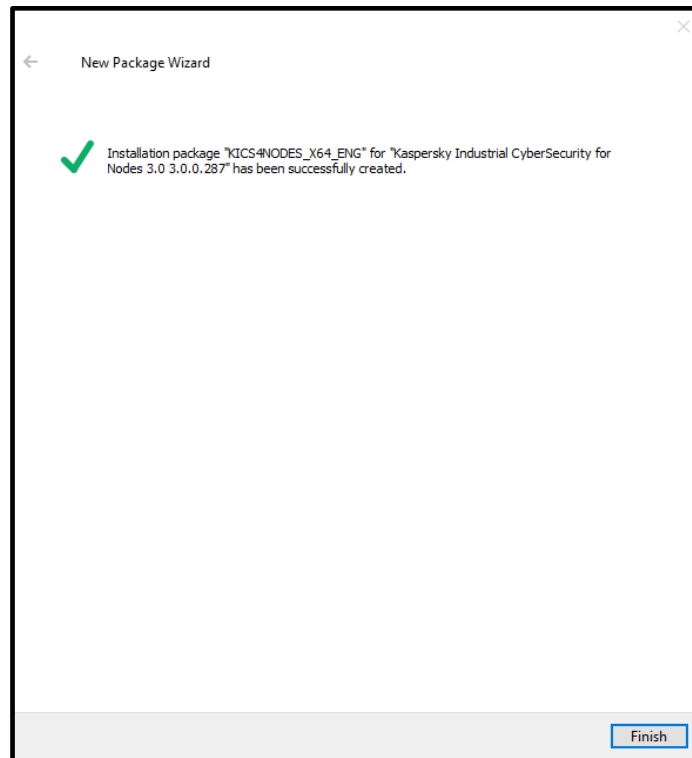
7. Read attentively the terms of use and accept the license agreement and privacy policy. Click **Next**.



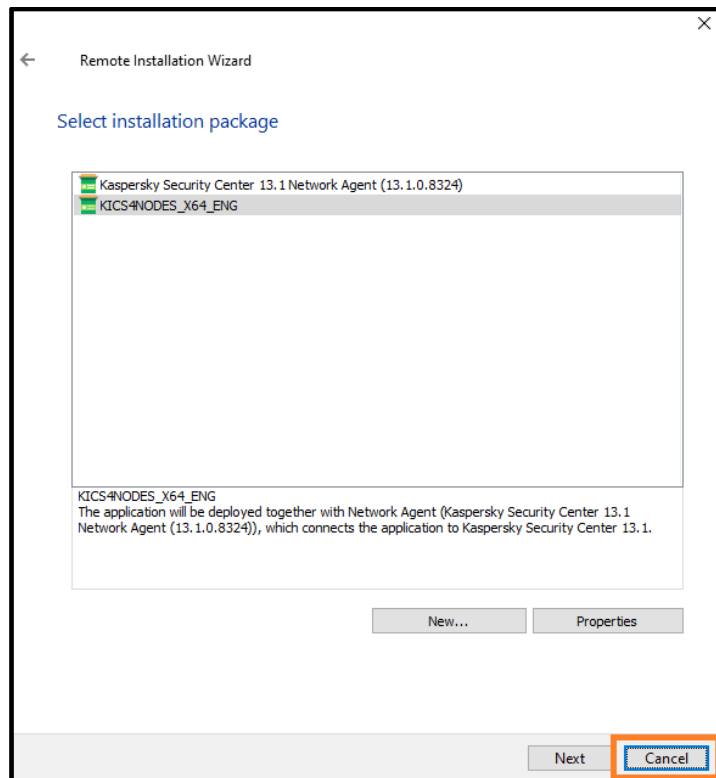
8. Wait while the installation package is being added to the **KSC** software repository.



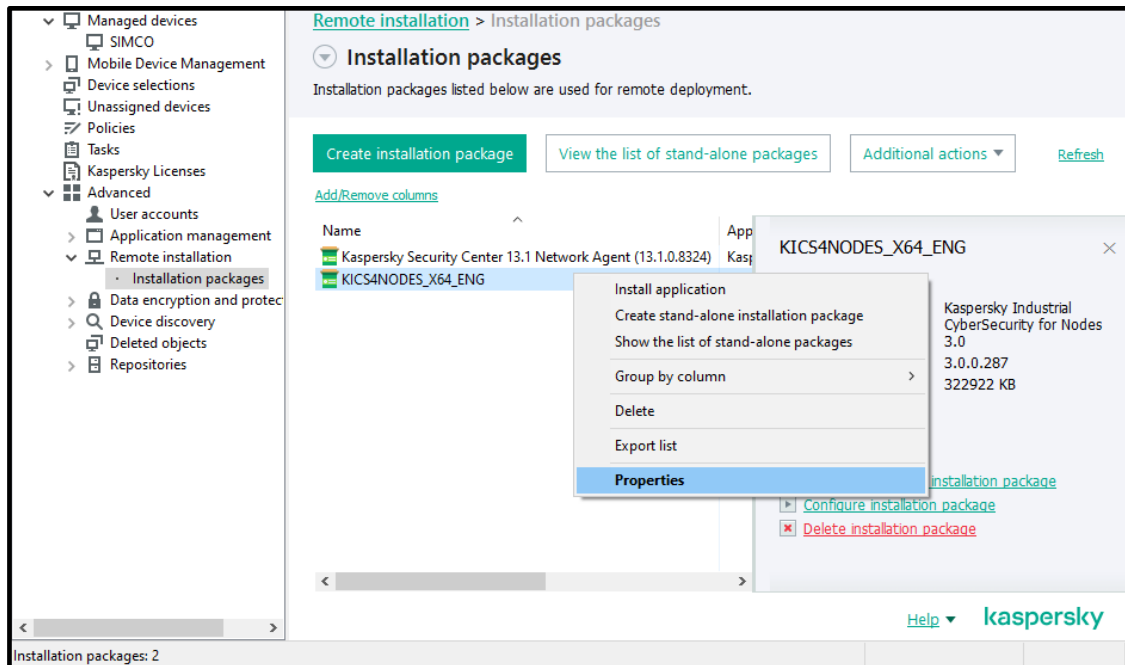
9. Press **Finish** upon installation completion to exit **New Package Wizard**.



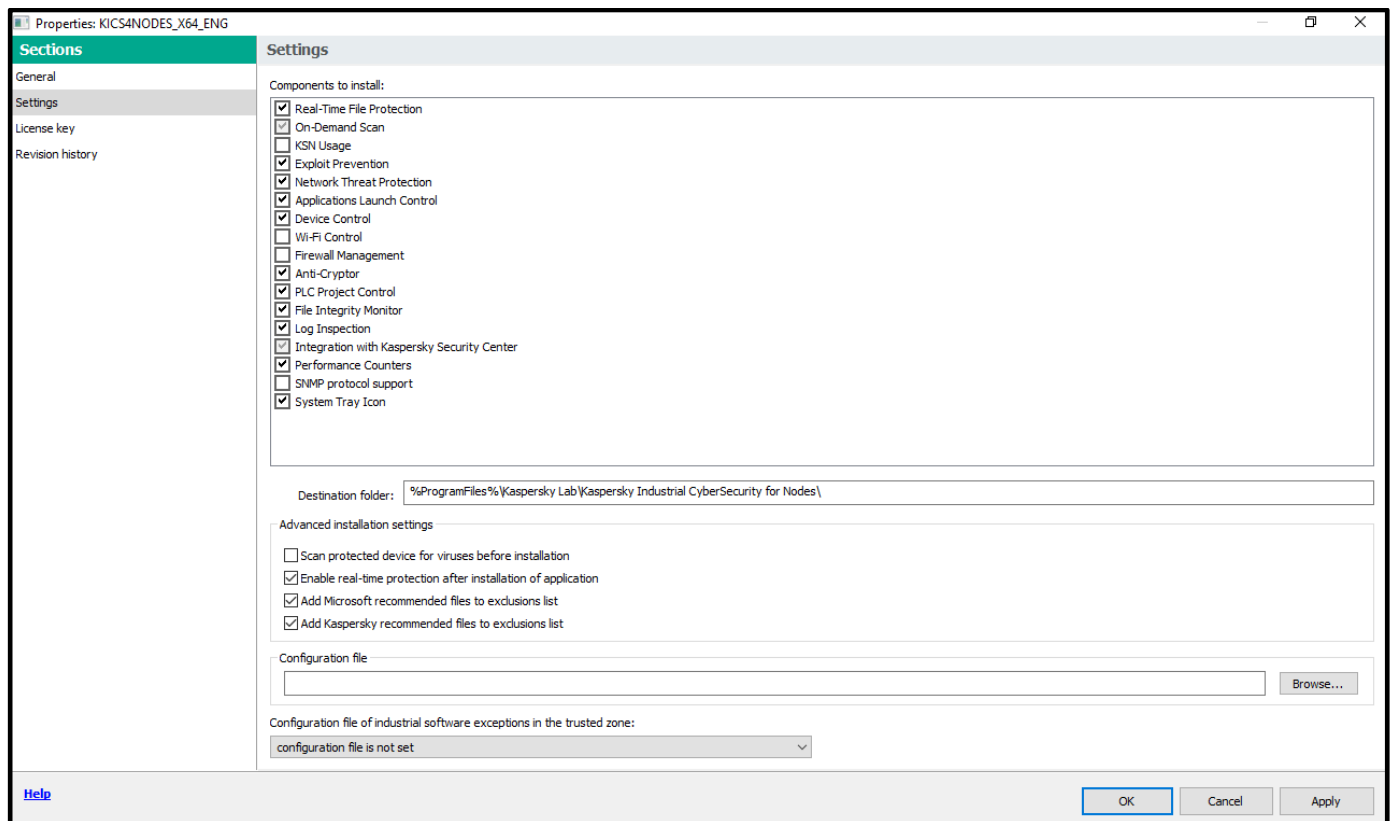
10. Click **Cancel** in the parent window to close **Remote Installation Wizard**. We need to abort the installation since we still have some more configuration to do.



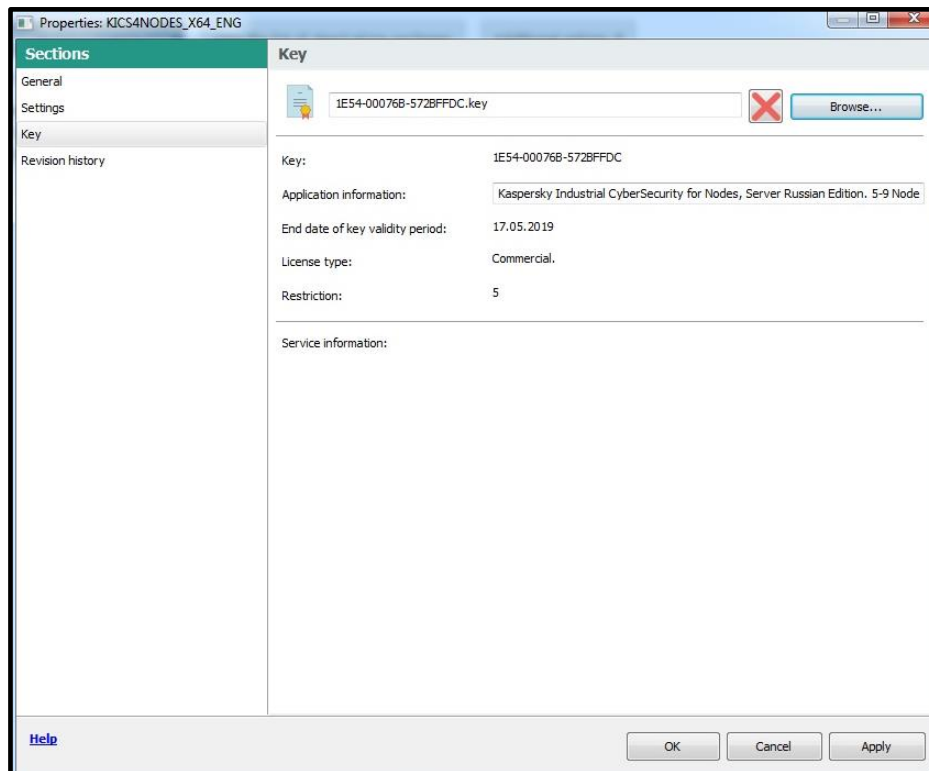
11. Revert to **Administration Server->Advanced->Remote installation->Installation packages**. Now select the just created installation package, right-click on it and choose **Properties** in the context menu.



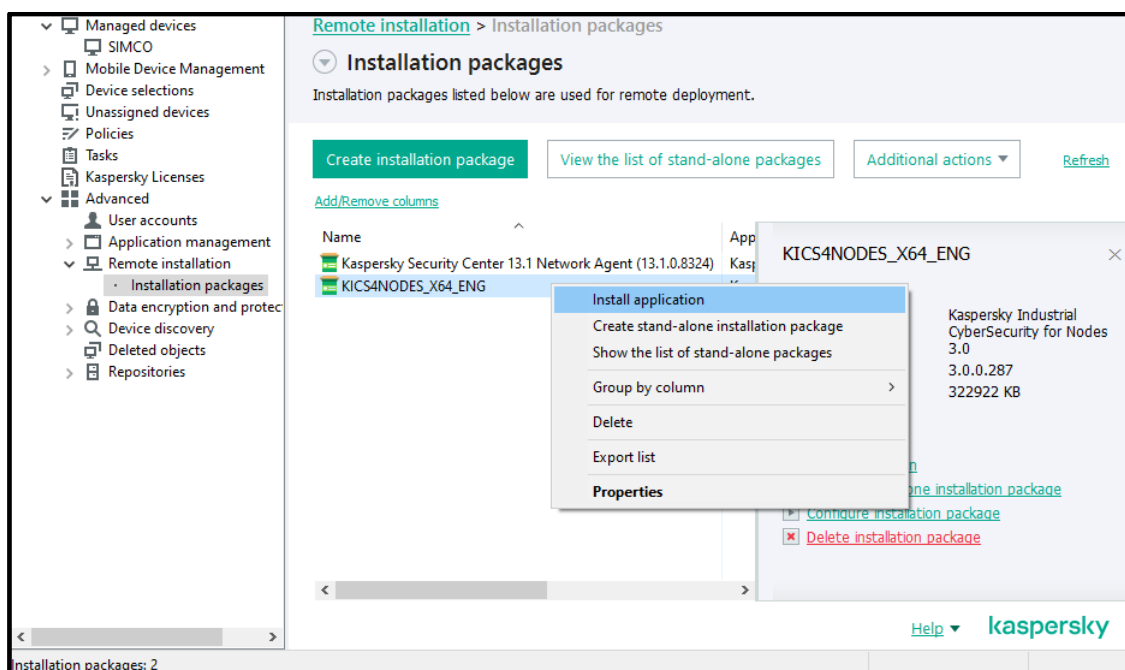
12. In the window that pops up go to **Settings**. In the **Settings** pane specify the set of **Components to install** strictly as shown below. Then specify **Advanced installation settings** as shown below.



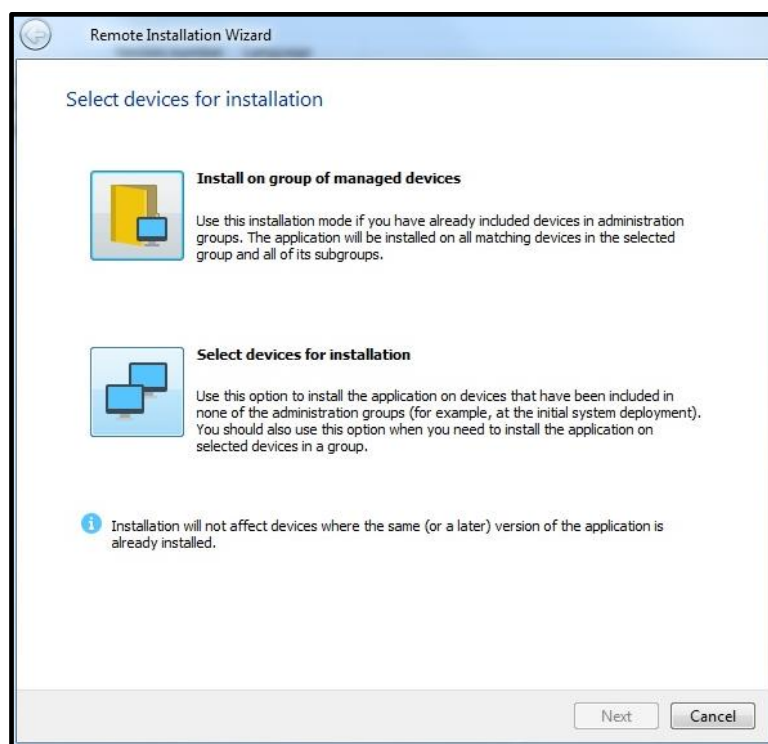
- Proceed to the **Key section** and, using the **Browse** button, locate the very same key-file (*.key) as was shown in “Initial configuration of **KSC**”. Follow the instructions of the familiar **Add key** wizard. Make sure that the license term is valid. Click **OK** to finalize the fine-tuning of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



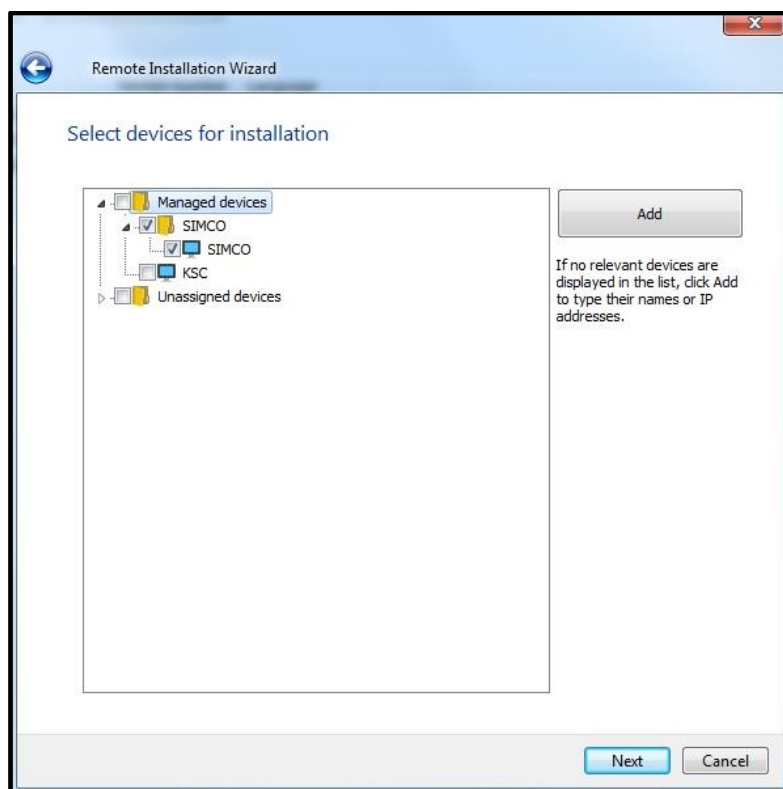
- After you have created and tuned up the **KICS for Nodes** installation package, select it again, right-click on it and in the context menu choose **Install application**.



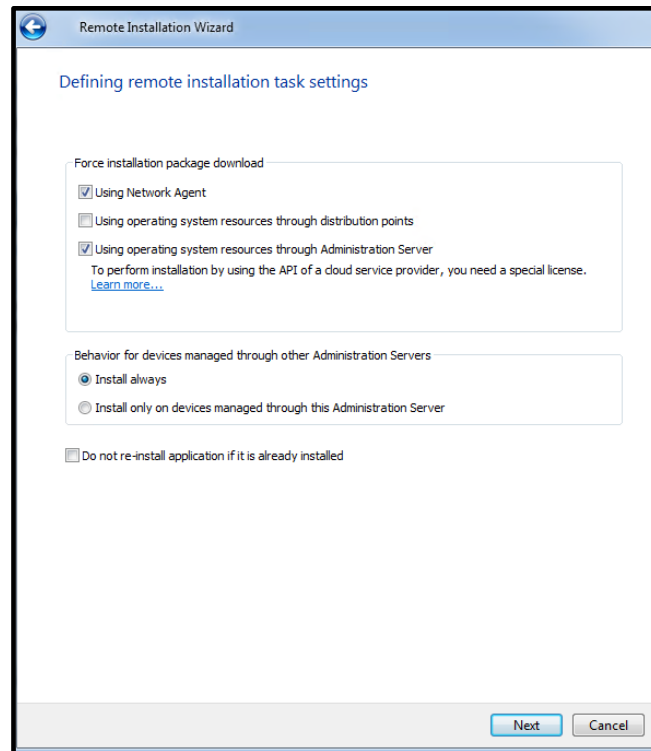
15. In the **Remote Installation Wizard** click **Select devices for installation**.



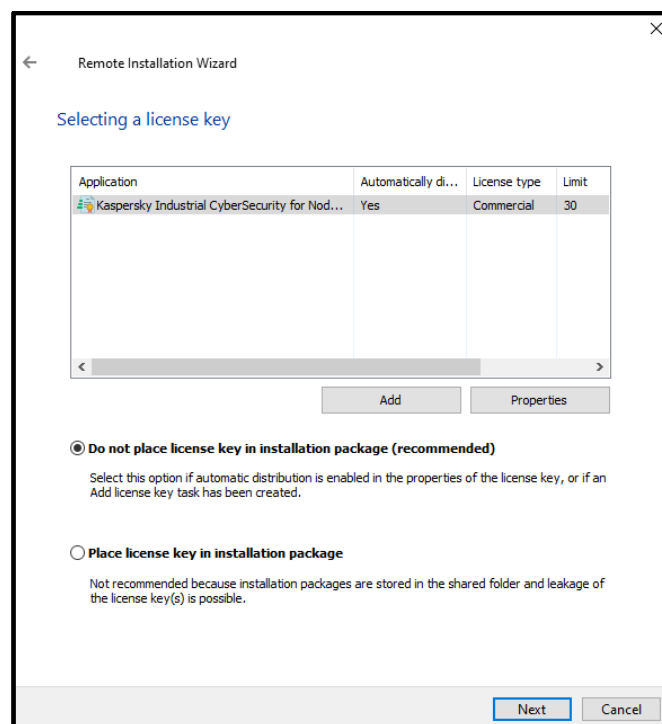
16. In the **Select devices for installation** tree view, select the recently added device running **KLnagent** (in our case, **SIMCO**). Select it and press **Next**.



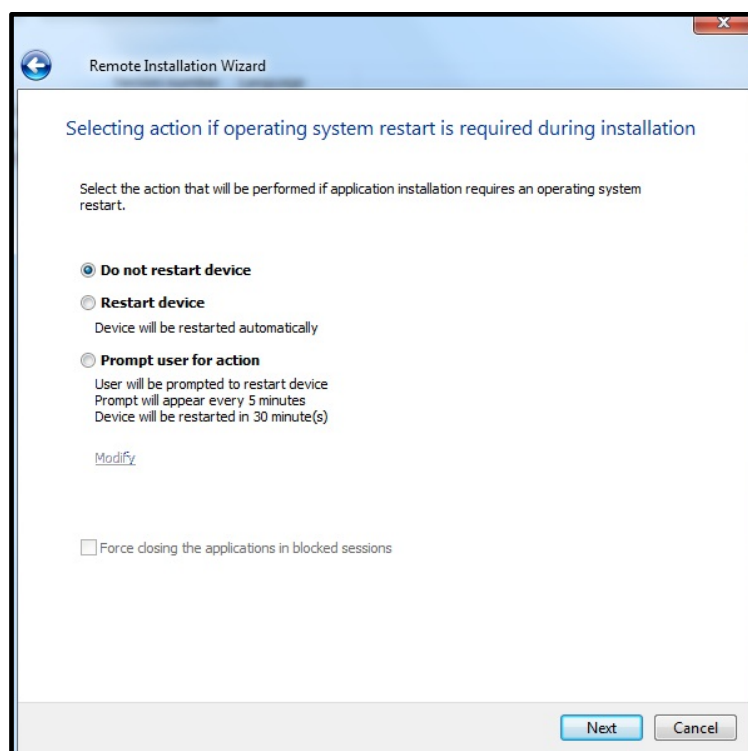
17. In the **Defining remote installation task settings** window, apply the settings as shown below. Click **Next**.



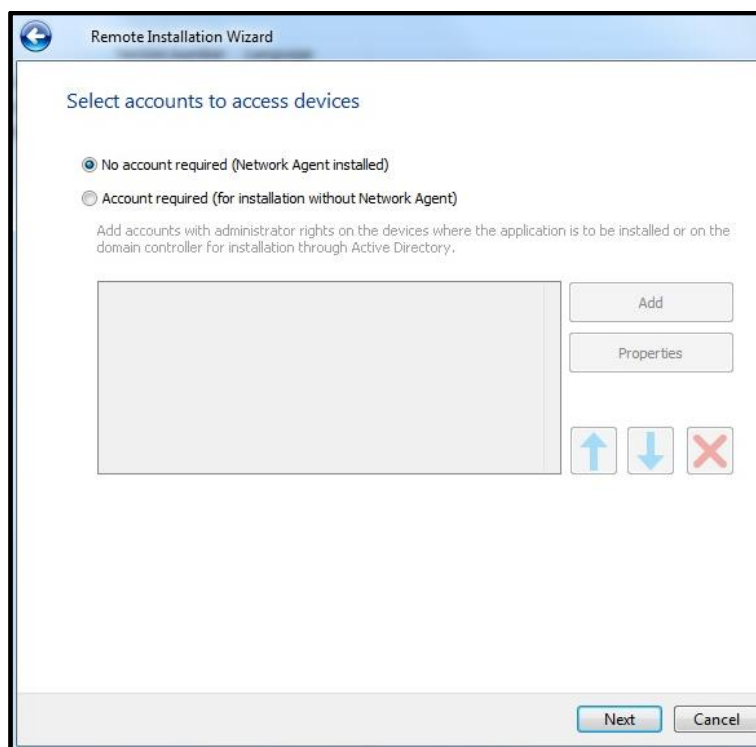
18. In the **Selecting a license key** window select the license you would want to apply to **KICS for Nodes** hosts (in our case we have just one option, but in general it may not be like this). We also recommend not integrating the license into the installation package. Click **Next** to continue.



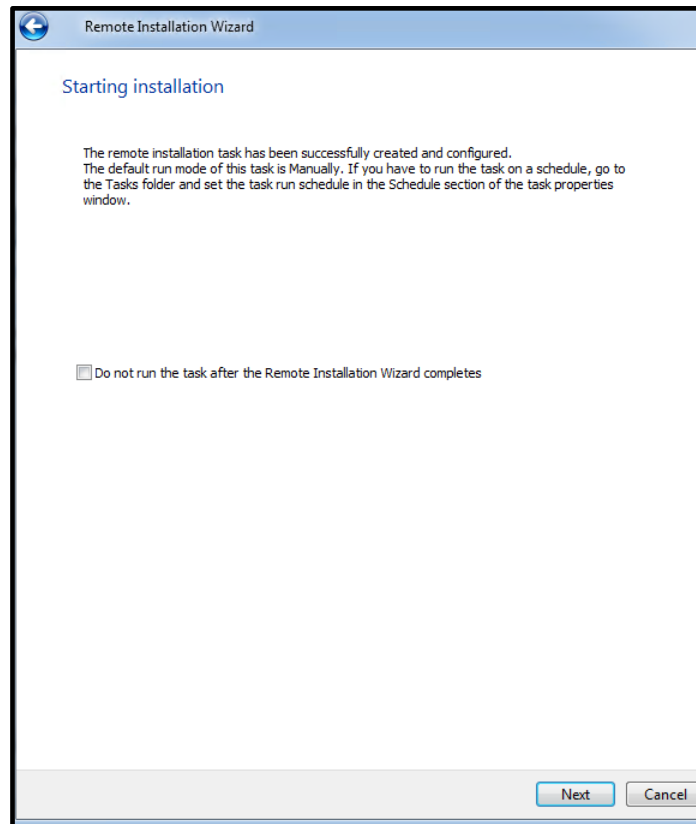
19. In the windows that appears apply the settings as shown below. Click **Next**.



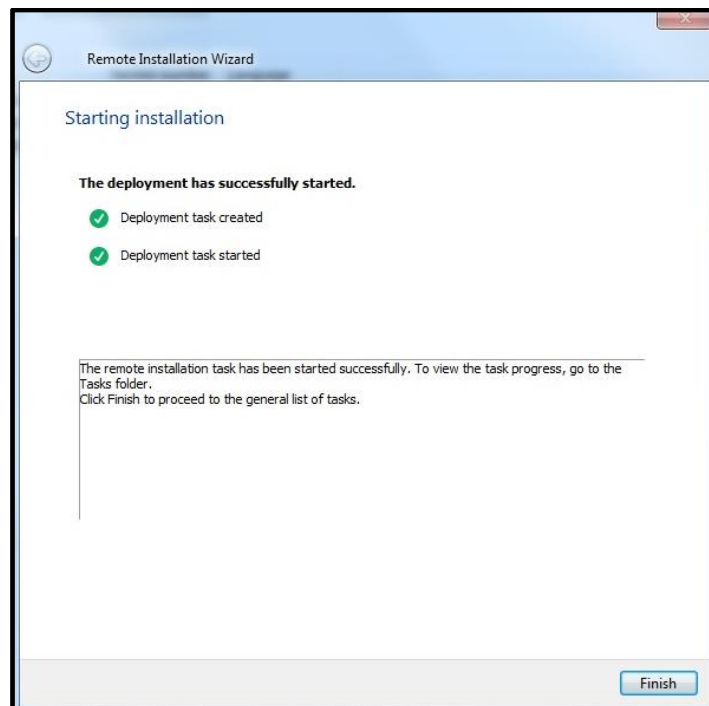
20. In the window that comes next, leave the default account settings as shown below. Click **Next**.



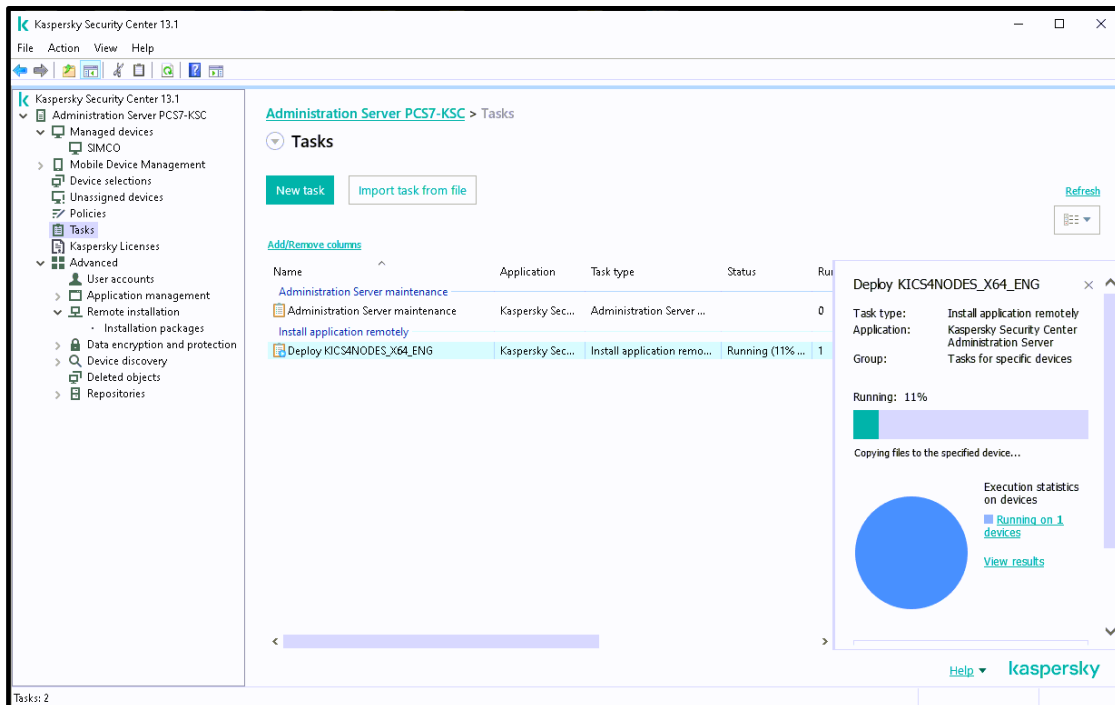
21. In the **Starting installation** window just click **Next**.



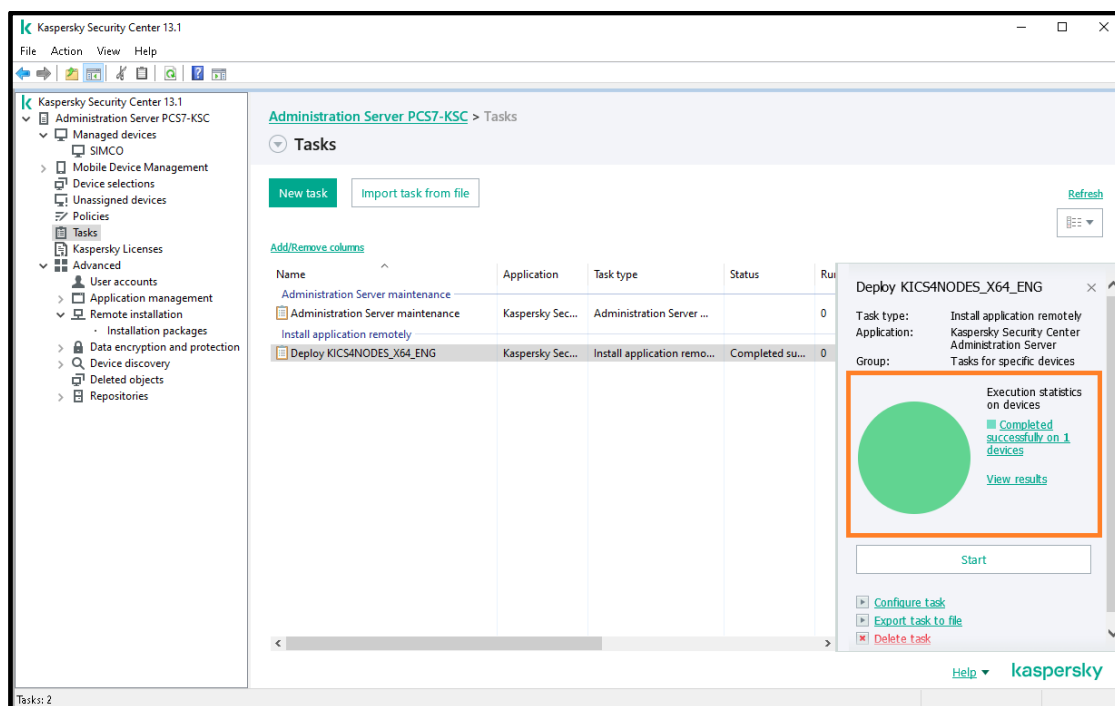
22. In the window that appears just click **Finish**. Now we have created and launched the **KICS for Nodes** remote installation task. You will automatically be transferred to **Administration Server->Tasks**.



23. Once you have entered **Administration Server->Tasks**, you can select the ongoing installation task in order to track its execution progress as shown below.

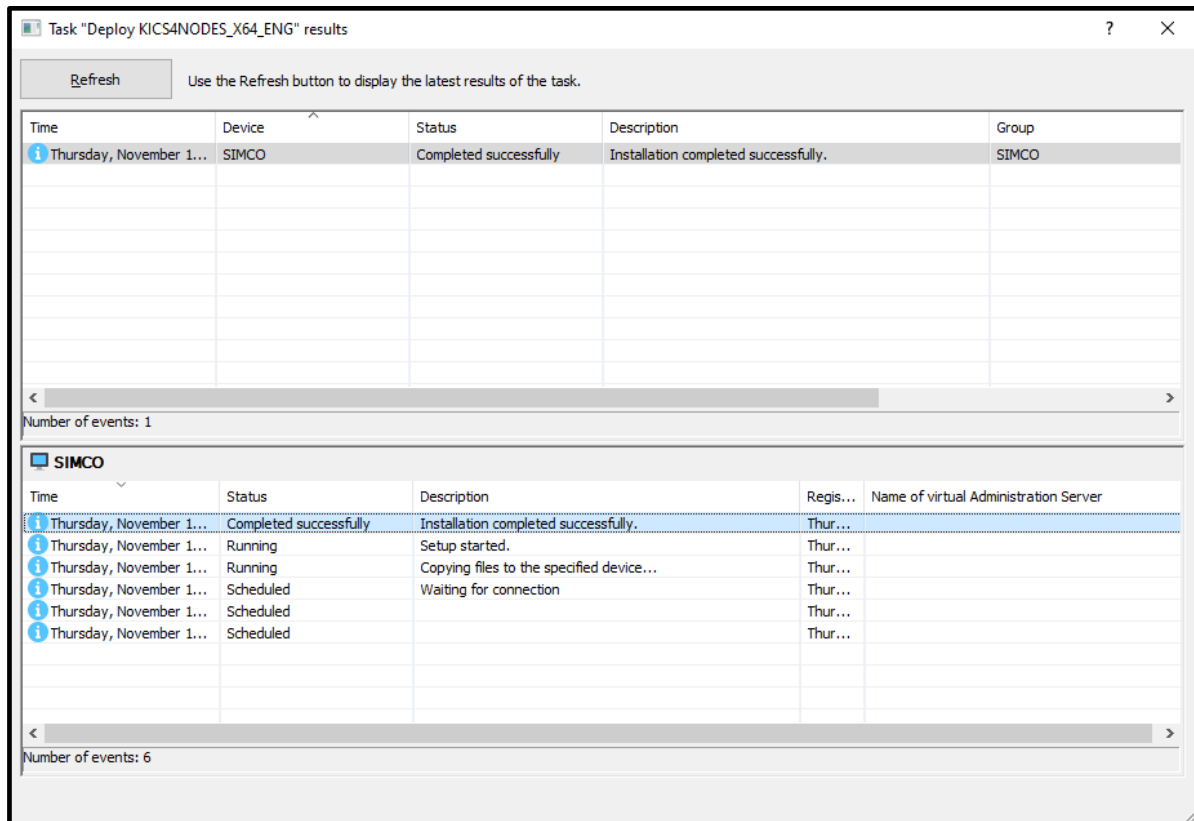


24. Wait until the installation task is completed⁶. Make sure that the task **execution statistics** are displayed as **Completed on ... devices** and the chart has turned green.



⁶A remote installation task may take up to 15 minutes depending on the performance of the target PC as well as the network throughput.

25. 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.



Remote installation of Hotfix onto target computers via KLnagent

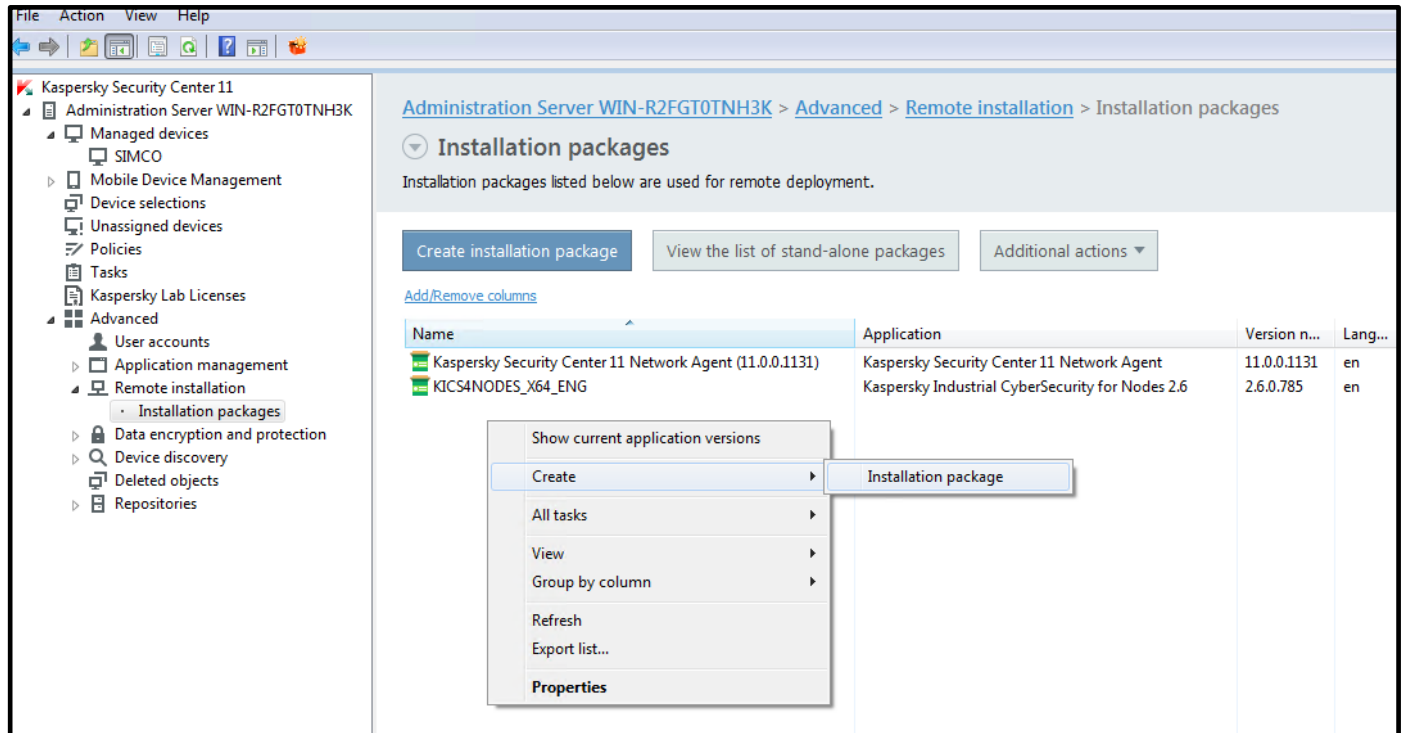
At the time, we are preparing this installation and deployment guide; the actual **Hotfix** version is **critical_fix_core_3**. However, you are likely to receive the installation package with a different **Hotfix** version: the one that has successfully been tested for compatibility with the particular model/version of your control system.

Every **Hotfix** is cumulative as it incorporates all the previous patches and improvements. Conversely, there is no need to uninstall any of the previous hotfixes (if already installed) before installing a newer one. Since the installation procedure remains the same regardless of the hotfix version, we recommend that you always follow the steps described below.

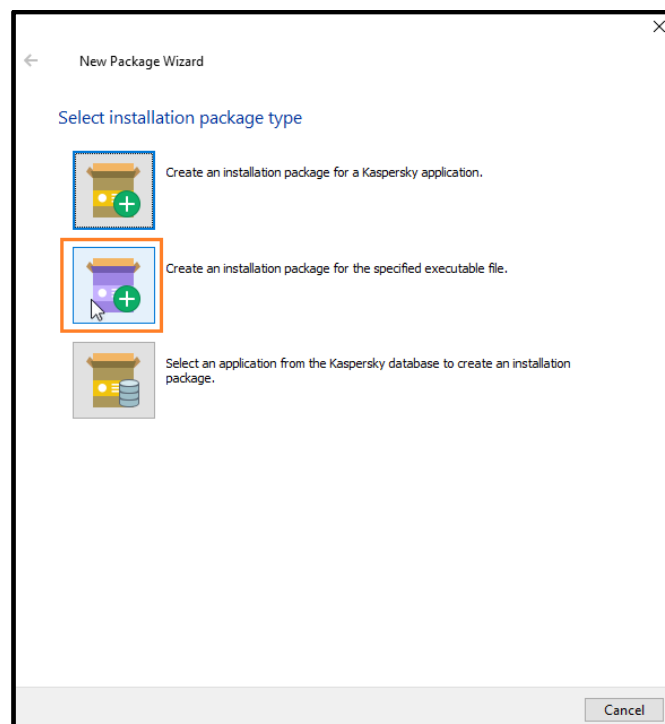
The following note applies only to Russia: due to the industry-specific regulations of Russia, the installation of patches and Hotfixes relative to KICS for Nodes may be restricted so that this deployment step is sometimes skipped. Please refer to the section “FSTEK certification for KICS for Nodes installations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

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

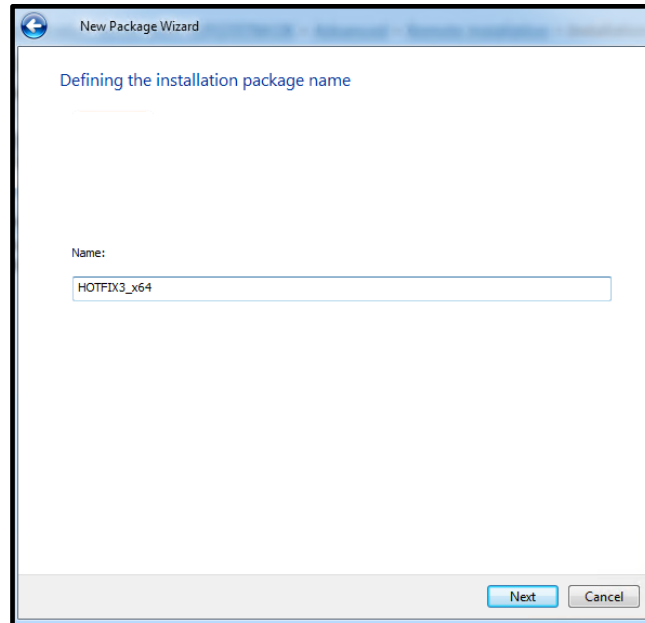
1. Go to **Administration Server->Advanced->Remote Installation**. Right-click on any spare area of the installation packages list. In the context menu choose **Create->Installation package**.



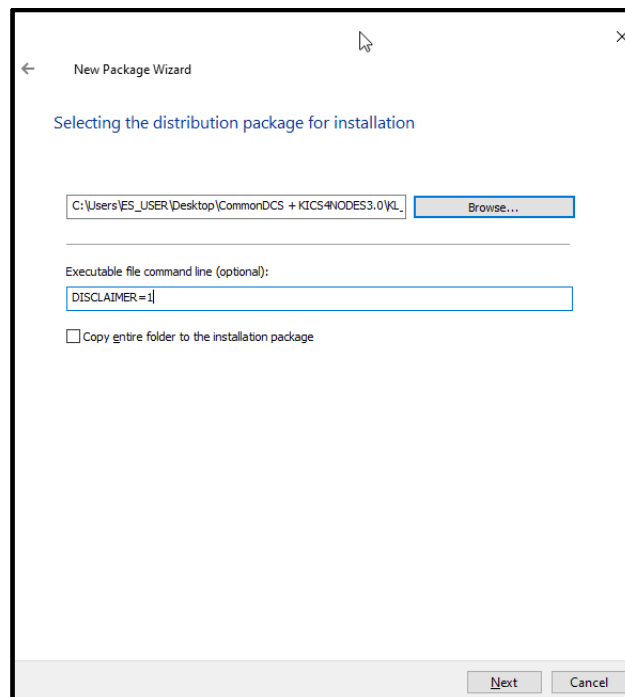
2. In the **Select installation package type** window, click **Create installation package for specified executable file**.



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

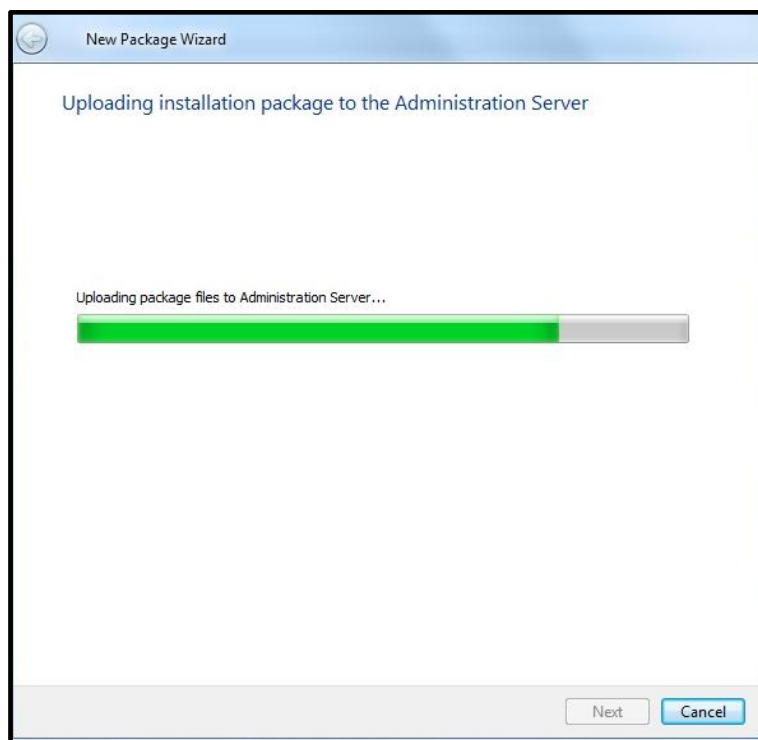


4. In the **Selecting the distribution package for installation** window browse to the **Hotfix⁷** file supplied as a part of the distribution package (the **Hotfix** file has the *.msp extension). Specify the **DISCLAIMER=1** attribute in the **Executable file command line** field and uncheck **Copy entire folder to the installation package**. Click **Next**.

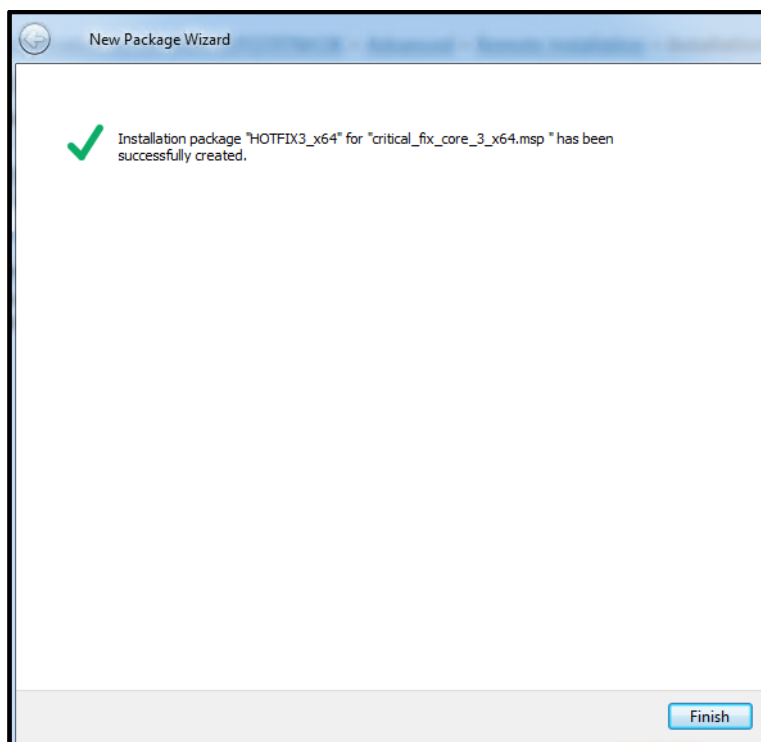


⁷ You should mind suffixes **X64** and **X86** in the names of **Hotfix** installation files. The installation file must match the target operating system bit depth you are planning to install hotfix on.

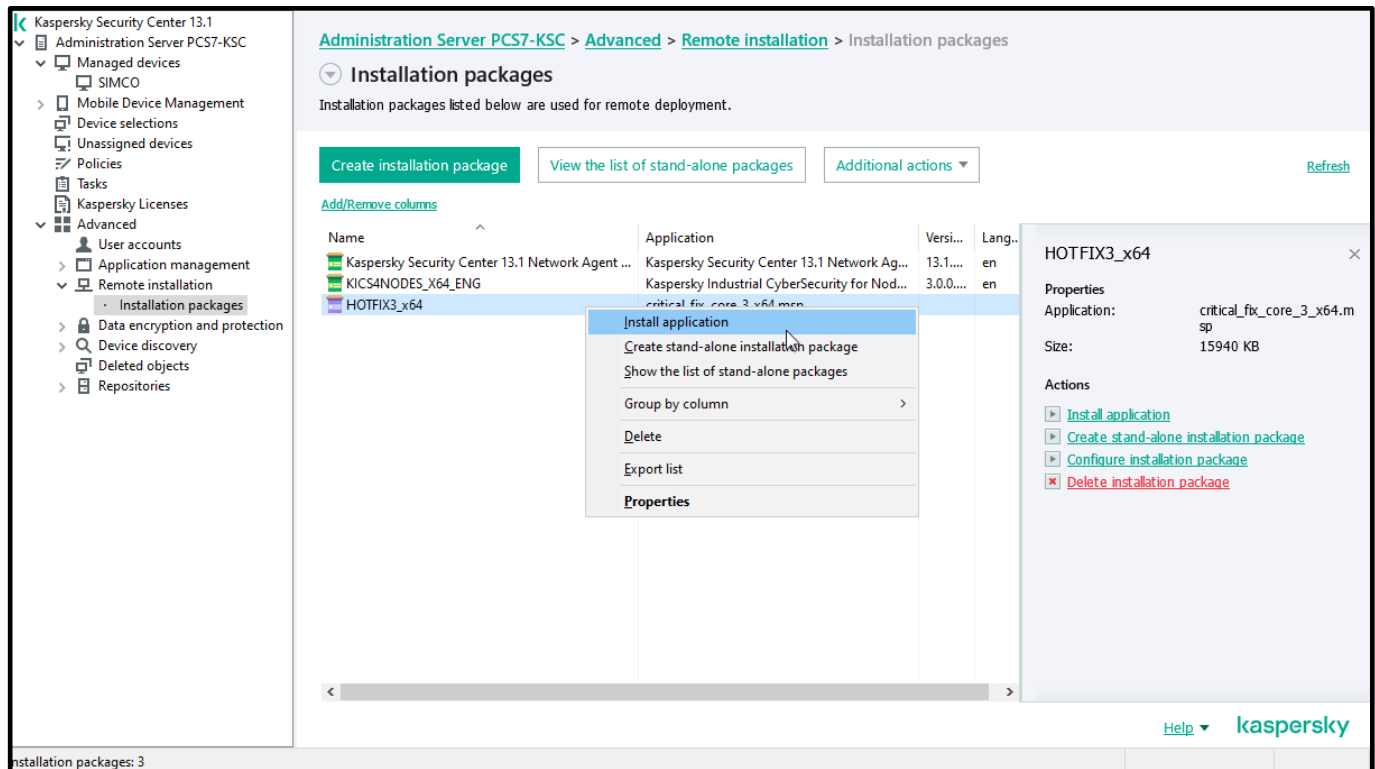
5. Wait while the **Hotfix** is being uploaded to the **Administration Server** repository.



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

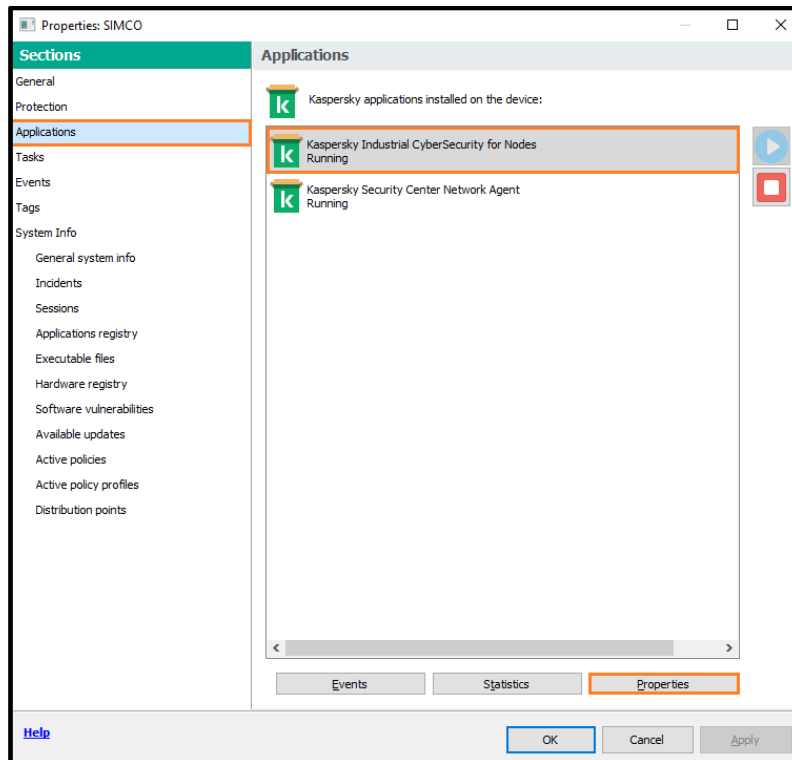
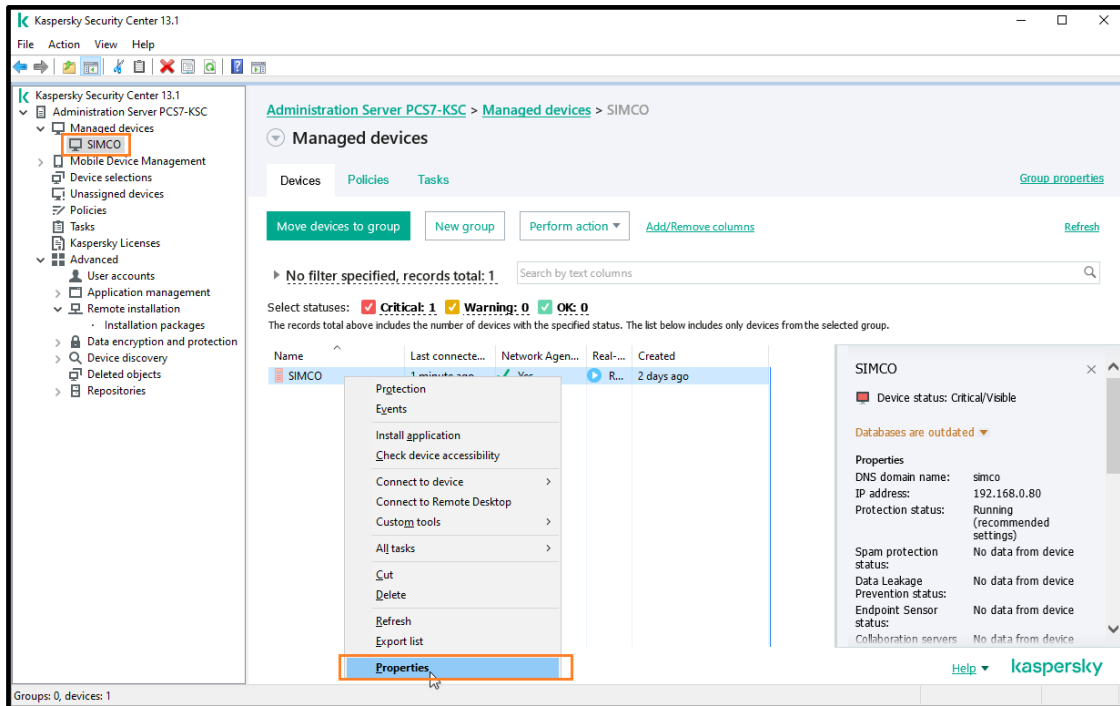


7. Remain in **Administration Server->Advanced->Remote Installation->Installation packages**. Right-click on the recently created **Hotfix** installation package and in the context menu choose **Install application**.

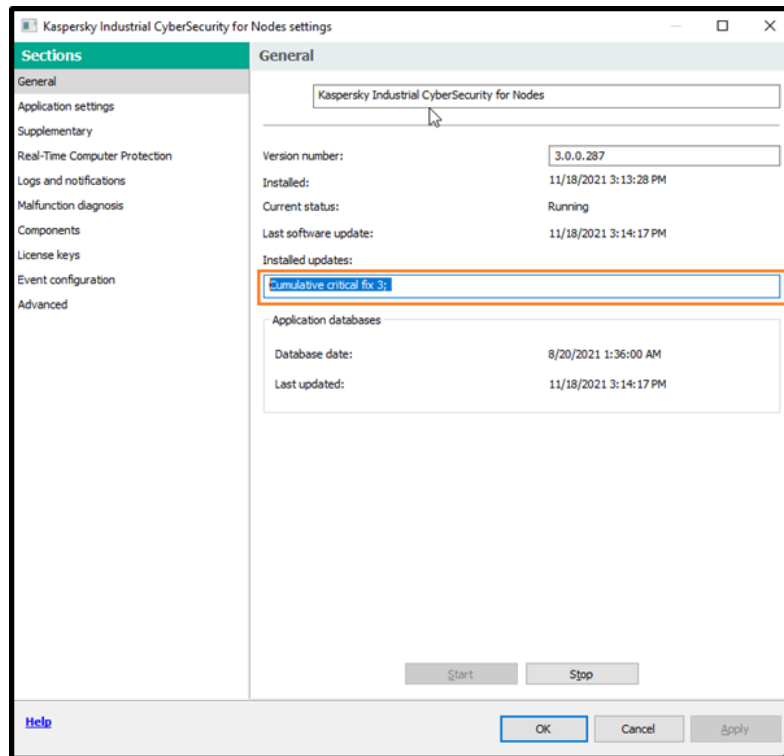


8. Perform exactly the same steps as were described in "Remote installation of KICS for Nodes onto target computers via KLnagent". At every subsequent prompt of the wizard specify the same settings as we did during the **KICS for Nodes** remote installation. The remote installation may last up to 10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

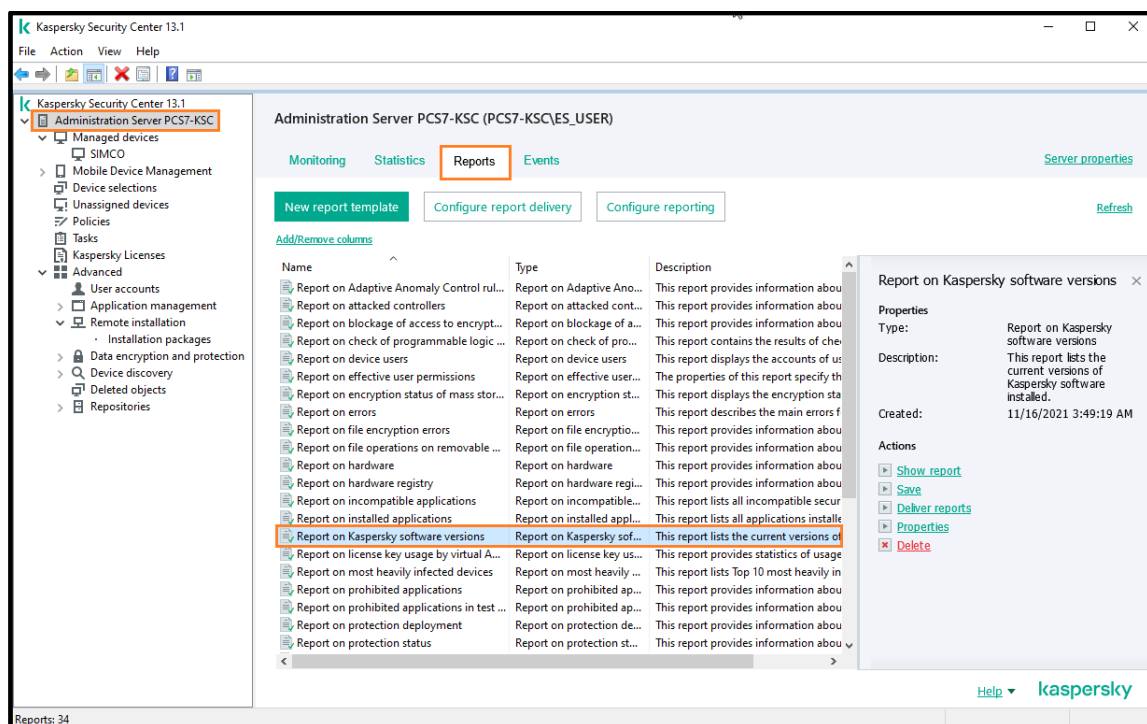
- In order to make sure that the **Hotfix** installation has been successful, go to your device located in the managed devices group (in our case, **SIMCO**). Then right-click on the device and select **Properties** in the context menu. Using the **Properties** window, proceed to **Application**, select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



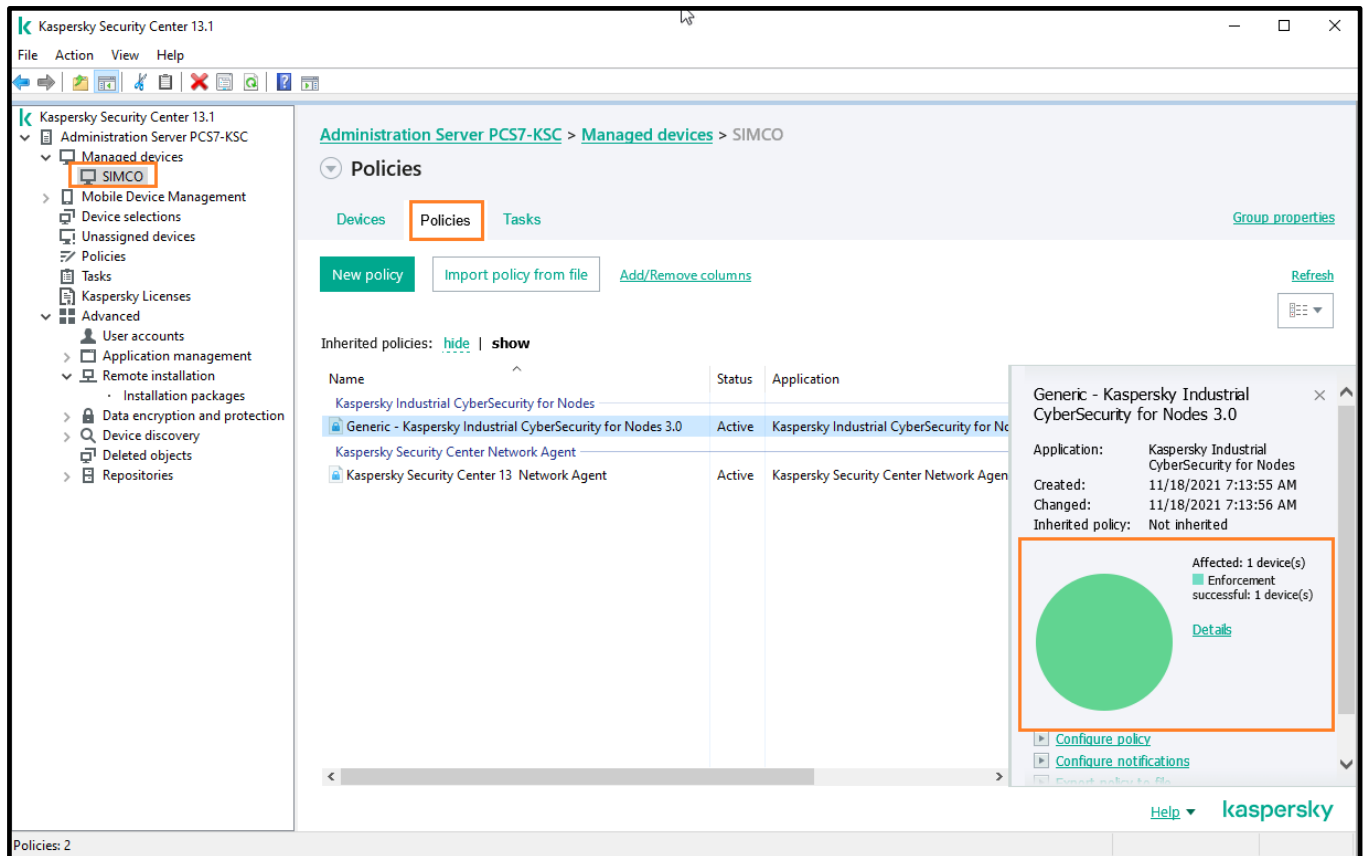
10. If the **hotfix** installation has been successful, you should see that the **Installed updates** field contains the name of the recently deployed **Hotfix**.



11. Alternatively, if there are multiple target hosts, you can check up the **Hotfix** installation at once by going up to **Administration Server** and switching over to the **Reports** tab. Double-click on **Report on Kaspersky software versions** and inspect the automatically generated report.



- Finally, it makes sense to verify that the recently created generic policy has reached the target host. Similar to checking up on your tasks, you can track policy enforcement by viewing the right-hand pane of the **Policies** tab as shown below. Wait until the round diagram turns green, indicating that the selected policy has been propagated to the target host and is applied.



Initial update of antivirus databases

No doubt, it is vitally important to keep **KICS for Nodes** AV definitions up to date. Although **KICS for Nodes** is designed to tolerate extremely rare actualization of AV definitions (at least, it is not going to molest a user with popup balloons and annoying notifications), it still requires occasional updates, which ensure secure operation of the protected host. There are at least 4 ways you can maintain antivirus databases actualized:

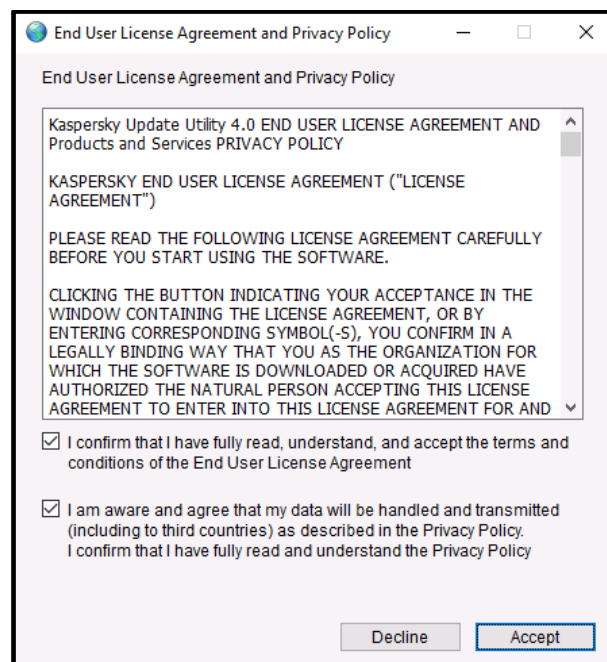
- You let the **KSC** server retrieve updates from the Kaspersky Lab update sources available on the Internet, so after that you perform databases propagation to **KICS for Nodes** devices directly from the **KSC** repository. This requires that your **KSC** server should be connected to the Internet.
- You let **KICS for Nodes** devices retrieve updates directly from the Kaspersky Lab update sources available on the Internet. This scheme does not utilize **KSC** at all but it requires that every **KICS for Nodes** device be able to access the Internet.
- You manually retrieve 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 storage.

4. You utilize **Kaspersky Update Utility** to retrieve updates from the Internet using whatever PC connected to the Internet (this PC may be even out of bounds of the control system). Then you transfer the downloaded updates to the **KSC** repository and initiate their propagation to the **DCS** nodes using the **KSC** mechanism.

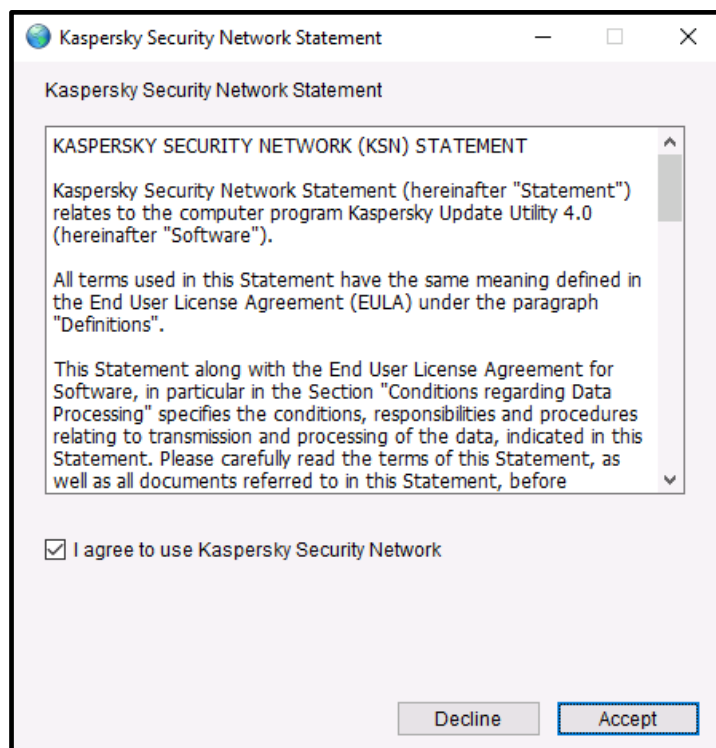
The latter scheme seems to be the most realistic for industrial sites. Therefore, we will solely focus on it; with one exception though. To make this guide simpler, we are going to launch **Kaspersky Update Utility** right on the **KSC**, which may seem ridiculous, of course. However, we do so only for illustration purposes: in practice you would rather use option 1, if you had your **KSC** connected to the Internet.

Follow the instructions given below:

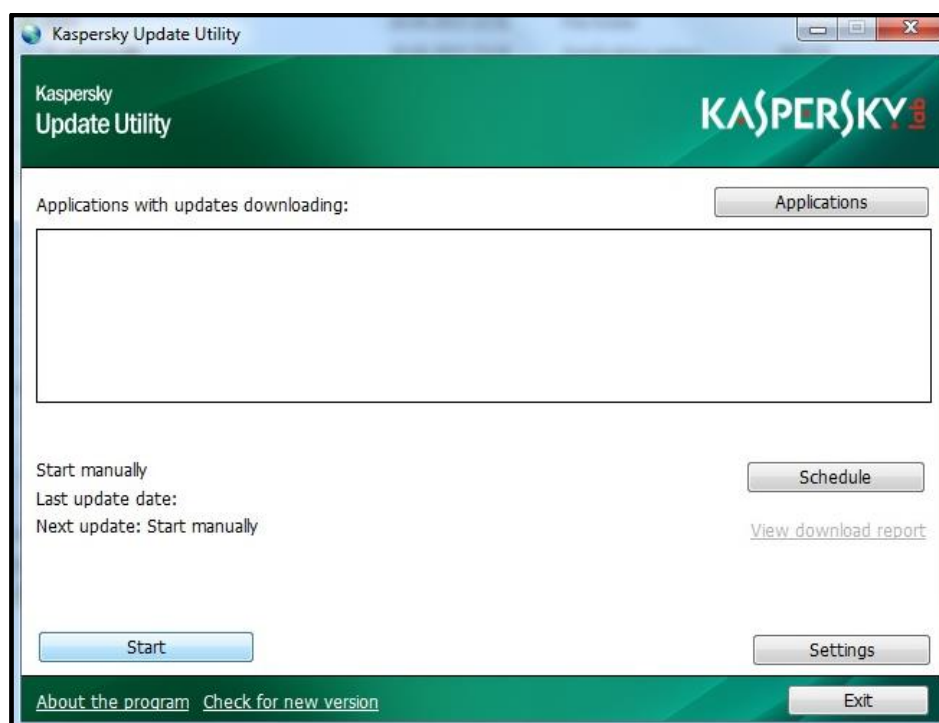
1. Let us create a new folder **KLUpdate** on the **C:** drive of our **KSC** server. This folder will be used as an intermediate storage of antivirus updates.
2. Follow <https://support.kaspersky.com/updater4> and download **Kaspersky Update Utility**.
3. Decompress the downloaded zip-archive to the recently created folder **C:\KLUpdate**.
4. Launch **UpdateUtility-Gui.exe** from **C:\KLUpdates**.
5. Accept the terms of use and privacy policy.



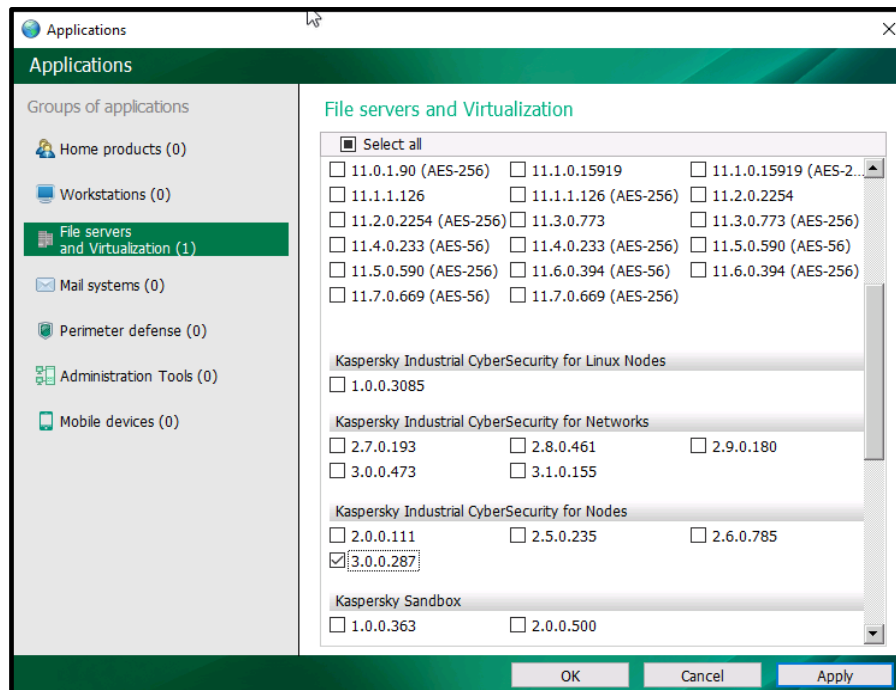
- Accept **KSN** use terms and conditions.



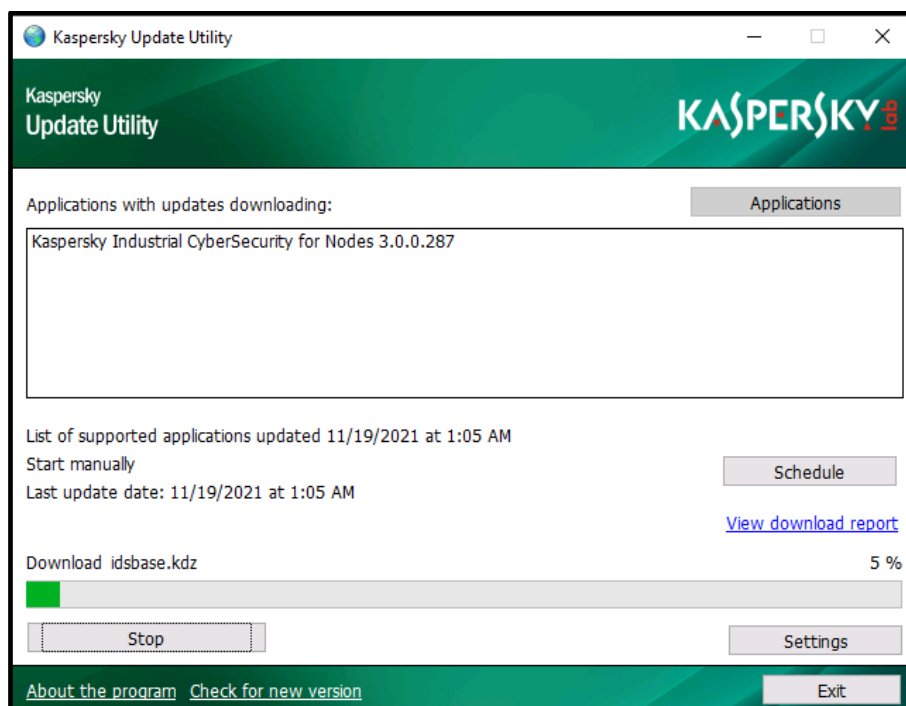
- The following window should appear.



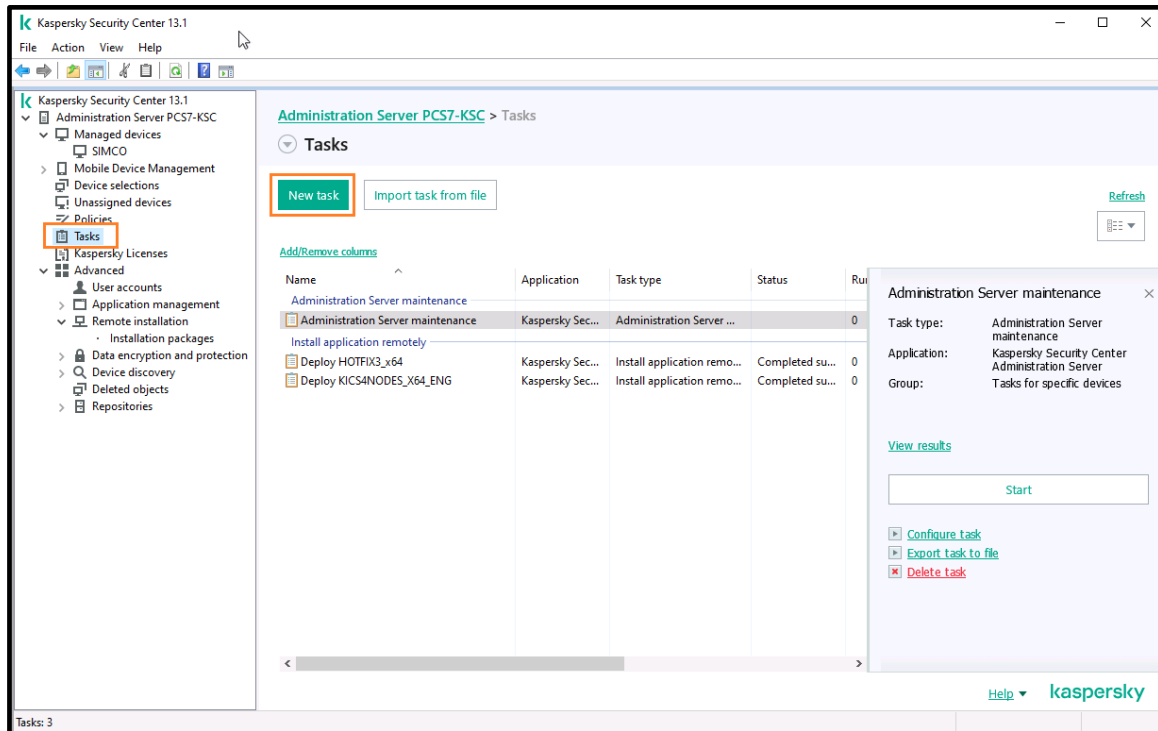
8. Click the **Start** button to update **Kaspersky Update Utility** itself in case its newer version has come out.
9. Press the **Applications** button and select the section **File servers and Virtualization**. Check **Kaspersky Industrial CyberSecurity for Nodes 3.0.0.287** as shown below. Click **OK**.



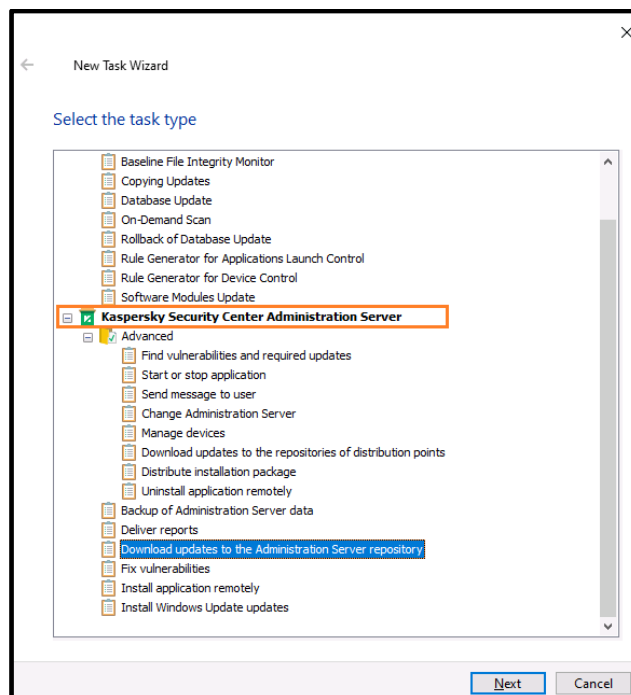
10. In the main window, press the **Start** button again and wait until necessary updates are downloaded. It may take up 10-15 minutes. The size of a regular update package may vary from 20 MB to 600 MB.



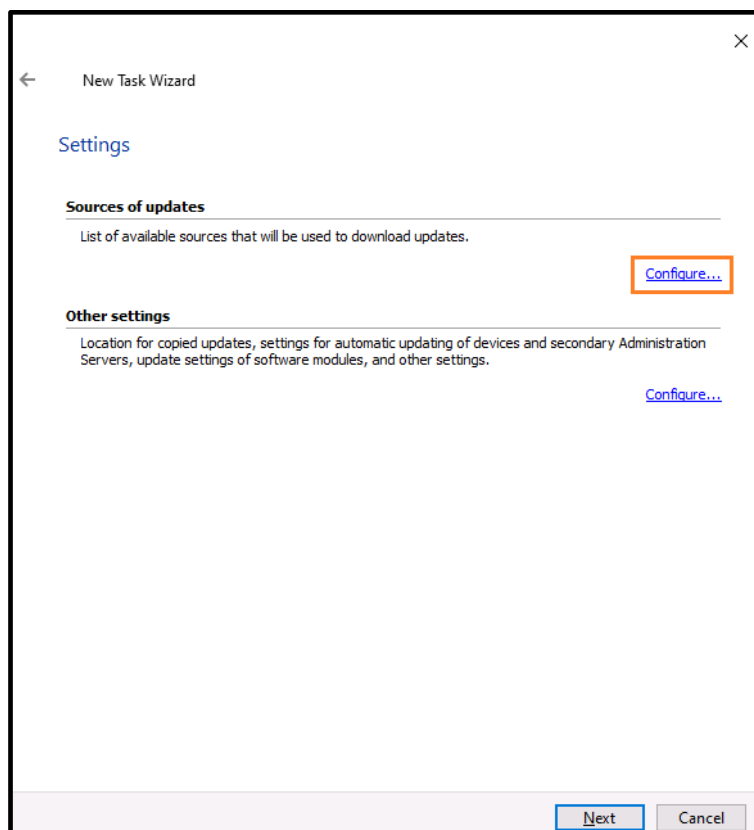
11. When all the updates are downloaded, click **Exit**.
12. Now return to the **KSC Administration Console**. Proceed to **Administration Server->Tasks** and click the **New task** button highlighted below.



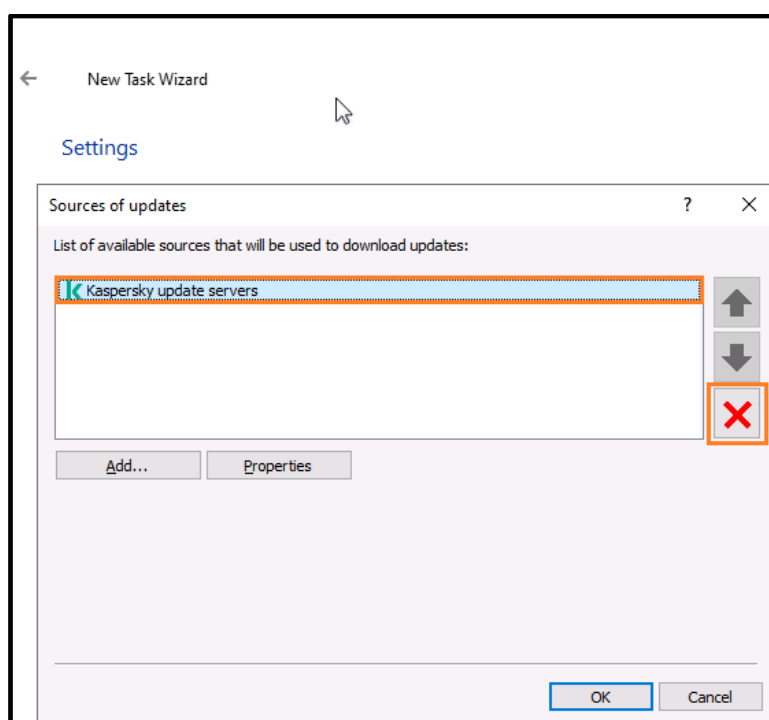
13. In the **New Task Wizard** window scroll down to the list item **Kaspersky Security Center Administration Server** and expand it. Select the task **Download updates to the Administration Server repository** and click **Next**.



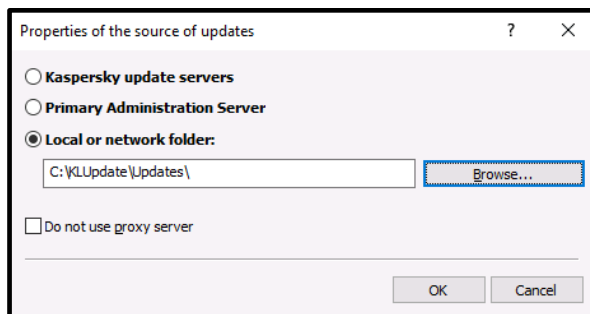
14. Click **Configure...** to set up an adequate source of updates.



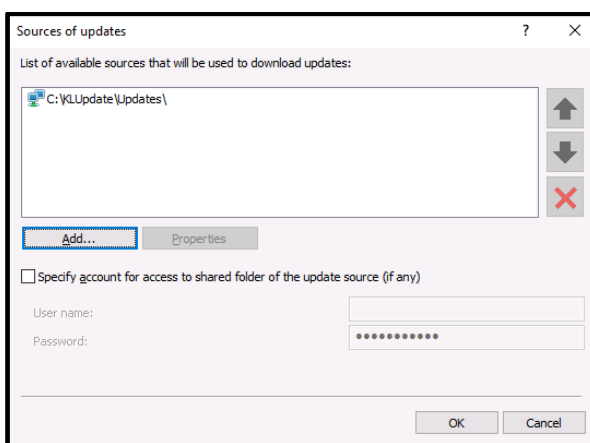
15. Select the default source of updates (highlighted below) and click the **red cross** button to clear the list. Then click **Add...** to supply a different source.



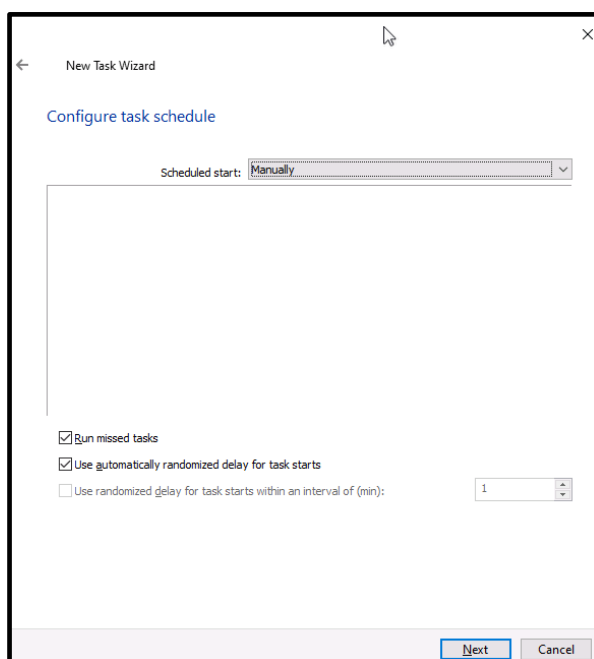
16. Select **Local or network folder** and specify the source of updates on the local computer. In our case, it is, as we remember, **C:\KLUpdates (+subfolder Updates)**. Click **OK** when done.



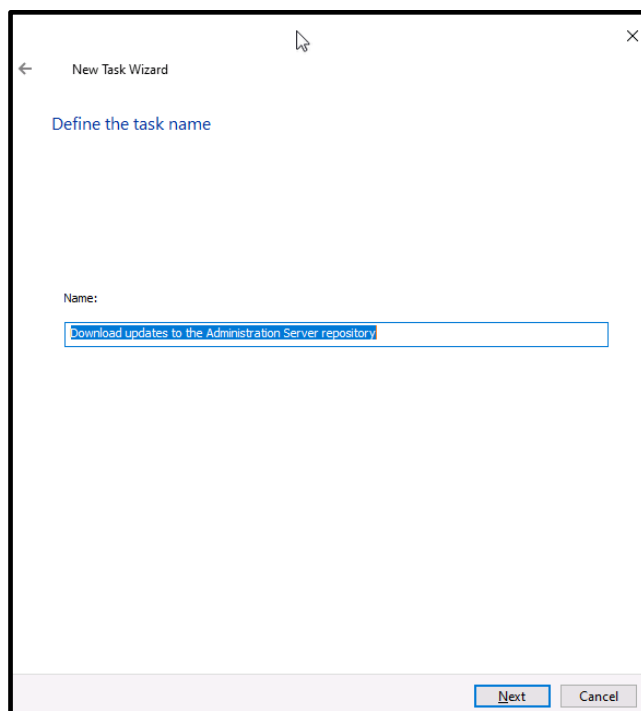
17. Now, the list of update sources should look as follows. Click **OK** in the **Sources of updates** window. Click **Next** in the parent window of the **Wizard**.



18. Manual installation of updates seems adequate for most of the control systems. So, we leave the default settings and click **Next** again.

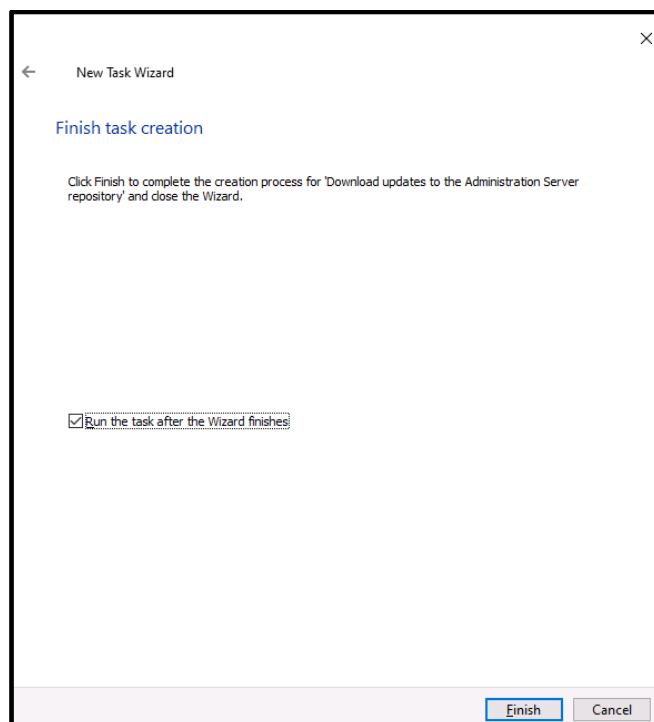


19. We suggest the you leave the default name intact and simply click **Next**.



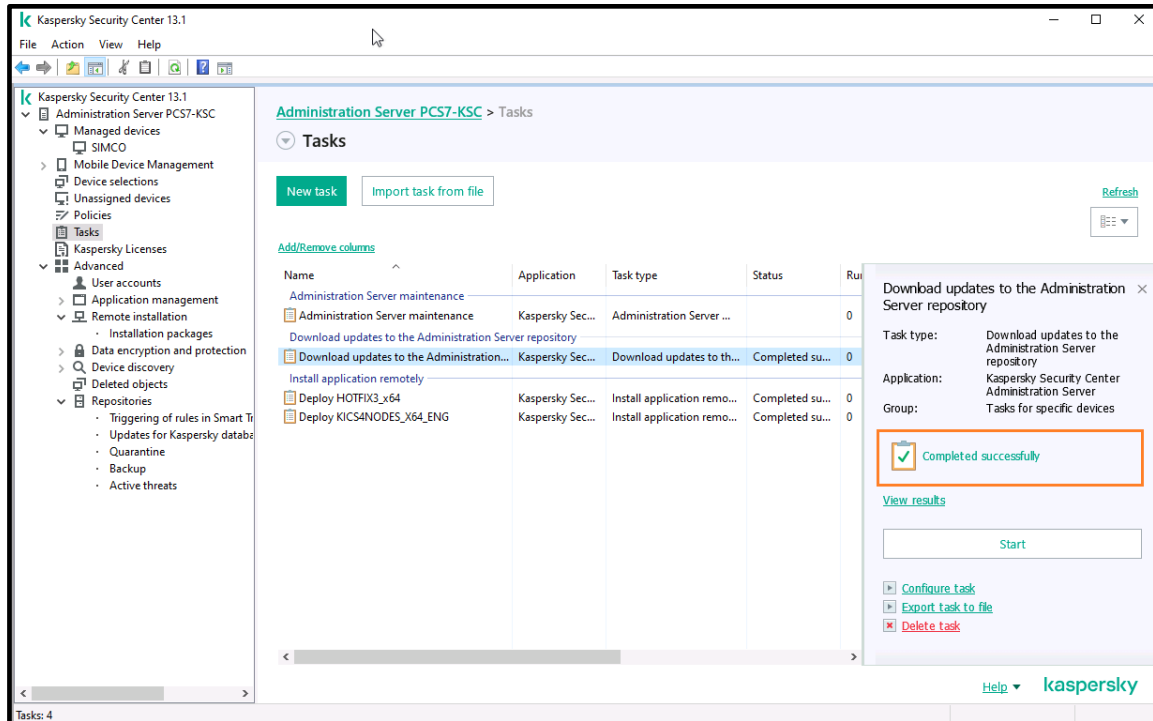
The screenshot shows the 'New Task Wizard' dialog box with the title bar 'New Task Wizard' and a close button (X). The main heading is 'Define the task name'. Below this, there is a label 'Name:' followed by a text input field containing the default name 'Download updates to the Administration Server repository'. At the bottom right, there are two buttons: 'Next' (highlighted with a blue border) and 'Cancel'.

20. Check **Run the task after the Wizard finishes** and click **Finish**.

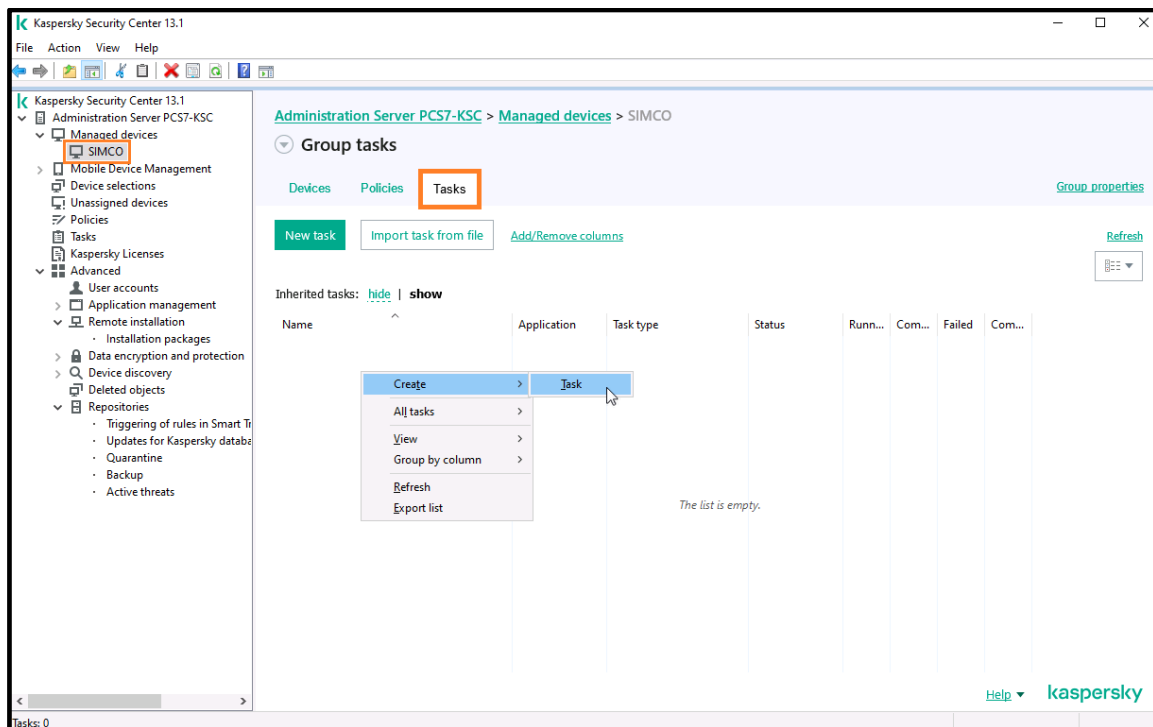


The screenshot shows the 'New Task Wizard' dialog box with the title bar 'New Task Wizard' and a close button (X). The main heading is 'Finish task creation'. Below this, there is a paragraph of text: 'Click Finish to complete the creation process for 'Download updates to the Administration Server repository' and close the Wizard.' Below the text, there is a checkbox labeled 'Run the task after the Wizard finishes' which is checked. At the bottom right, there are two buttons: 'Finish' (highlighted with a blue border) and 'Cancel'.

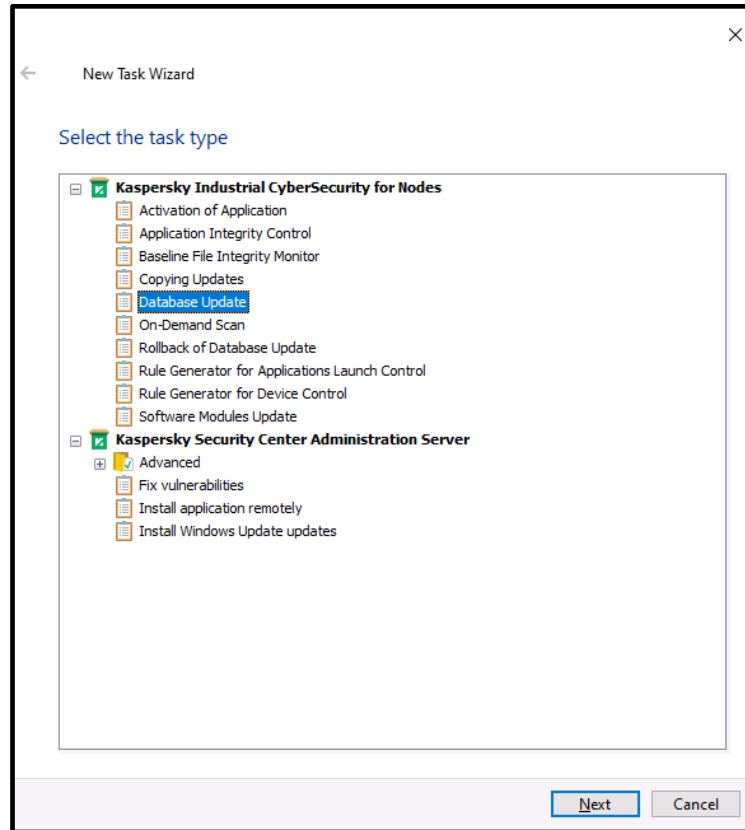
21. Wait until the task **Download updates to the Administration Server repository** gets marked as **Completed successfully** in the right-hand status pane as shown below.



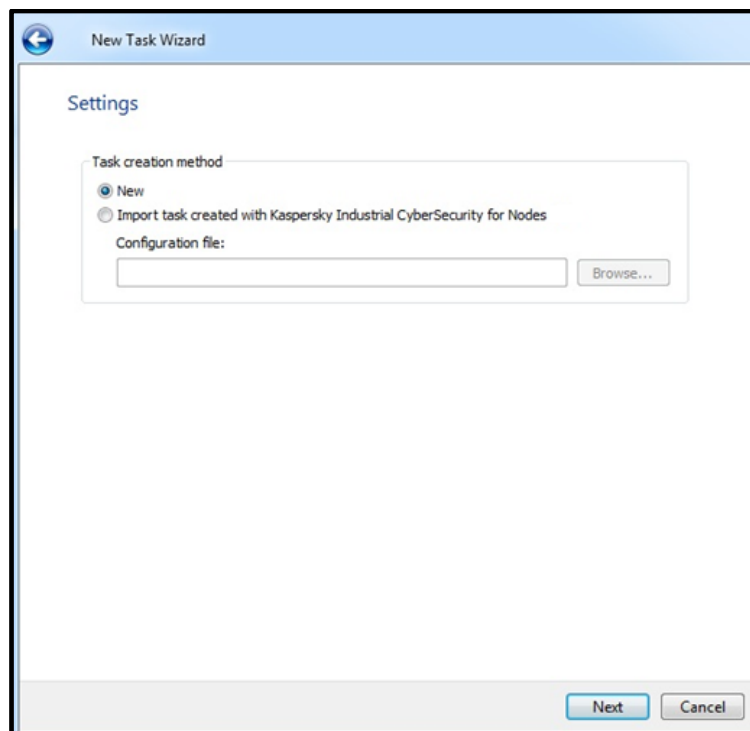
22. Now, go to our managed device (in our case, **SIMCO**); switch to the **Task** tab; right-click on any spare area of the **Tasks** list; in the context menu choose **Create->Task**.



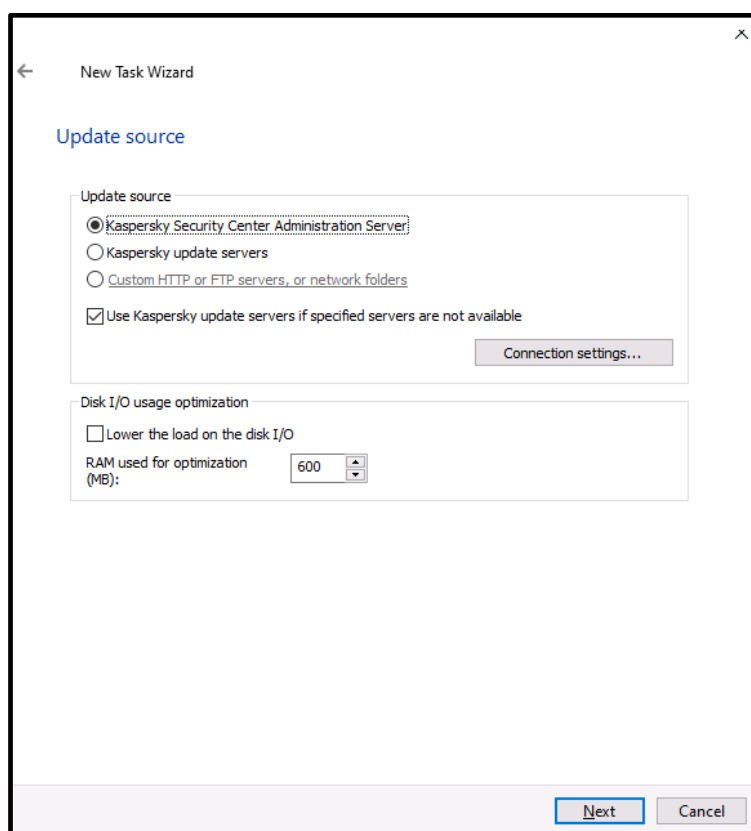
23. In the **Select the task type** window, select **Kaspersky Industrial CyberSecurity for Nodes->Database Update** and press **Next**.



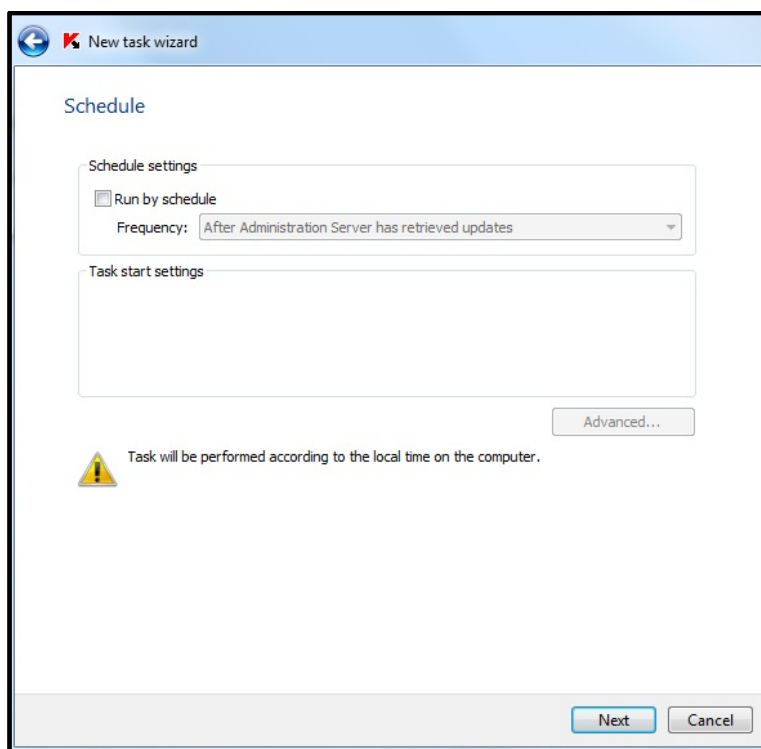
24. Leave the **Task creation method** as **New** and click **Next**.



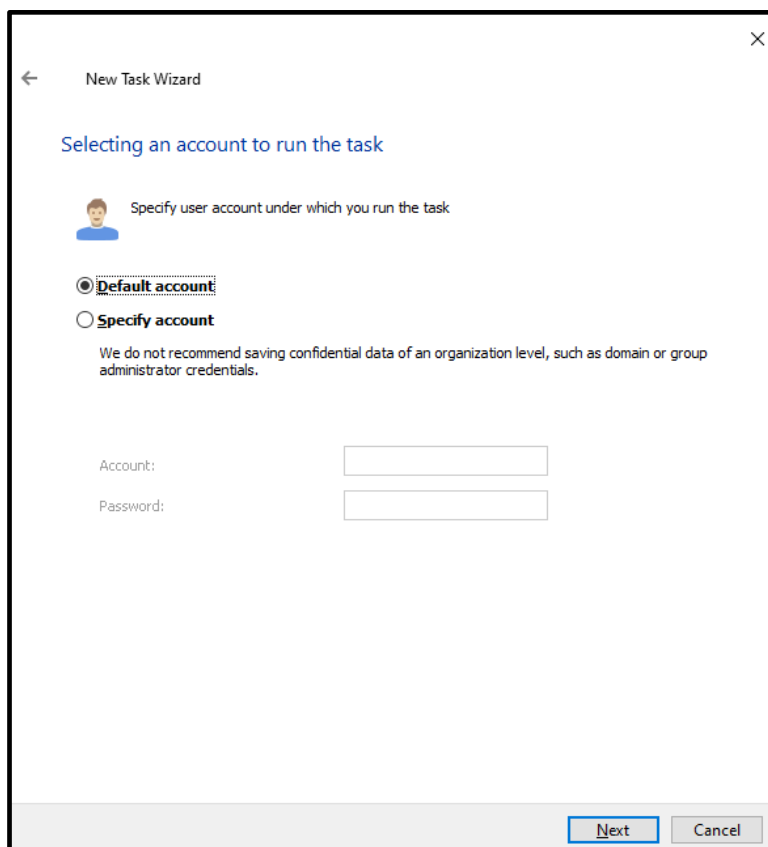
25. In the **Update source** window check **Kaspersky Security Center Administration Server**. and click **Next**.



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

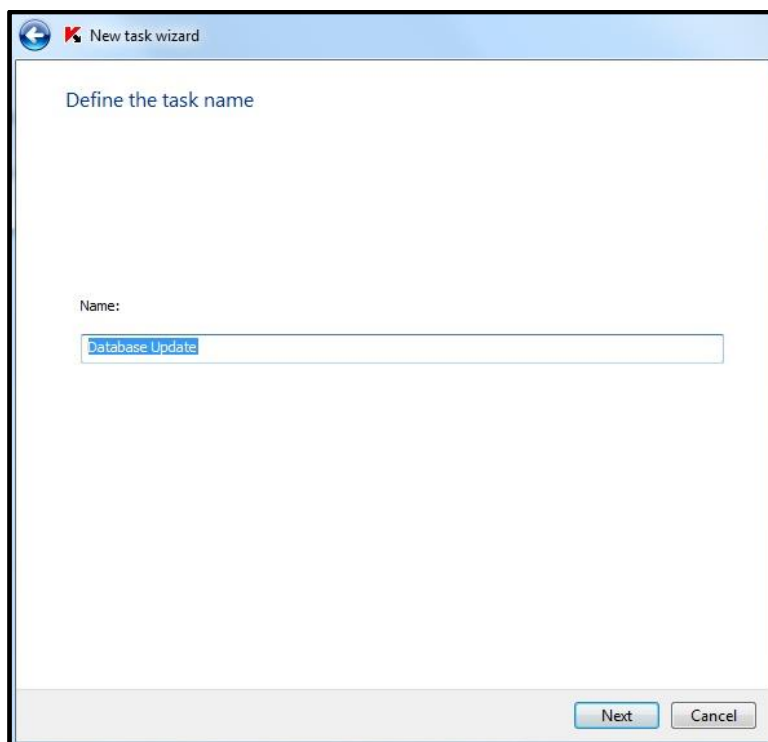


27. In the **Selecting an account to run the task** window specify the **Default account**. Click **Next**.



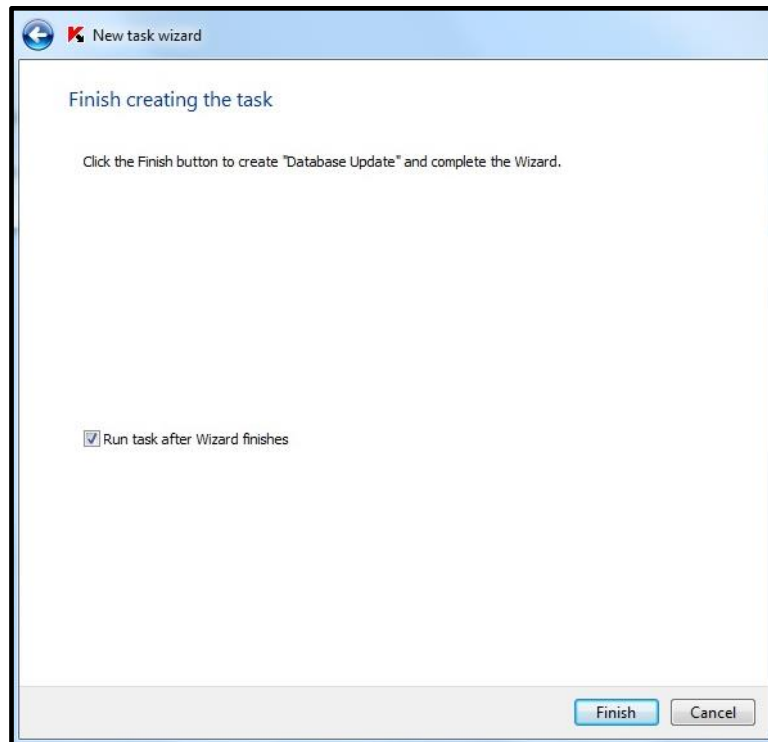
The screenshot shows the 'New Task Wizard' window with the title bar 'New Task Wizard'. The main heading is 'Selecting an account to run the task'. Below this, there is a user icon and the text 'Specify user account under which you run the task'. There are two radio button options: 'Default account' (which is selected) and 'Specify account'. Below the 'Specify account' option, there is a warning message: 'We do not recommend saving confidential data of an organization level, such as domain or group administrator credentials.' At the bottom, there are two input fields labeled 'Account:' and 'Password:'. At the very bottom right, there are 'Next' and 'Cancel' buttons.

28. Give a new name to the task or keep the default one. Click **Next**.

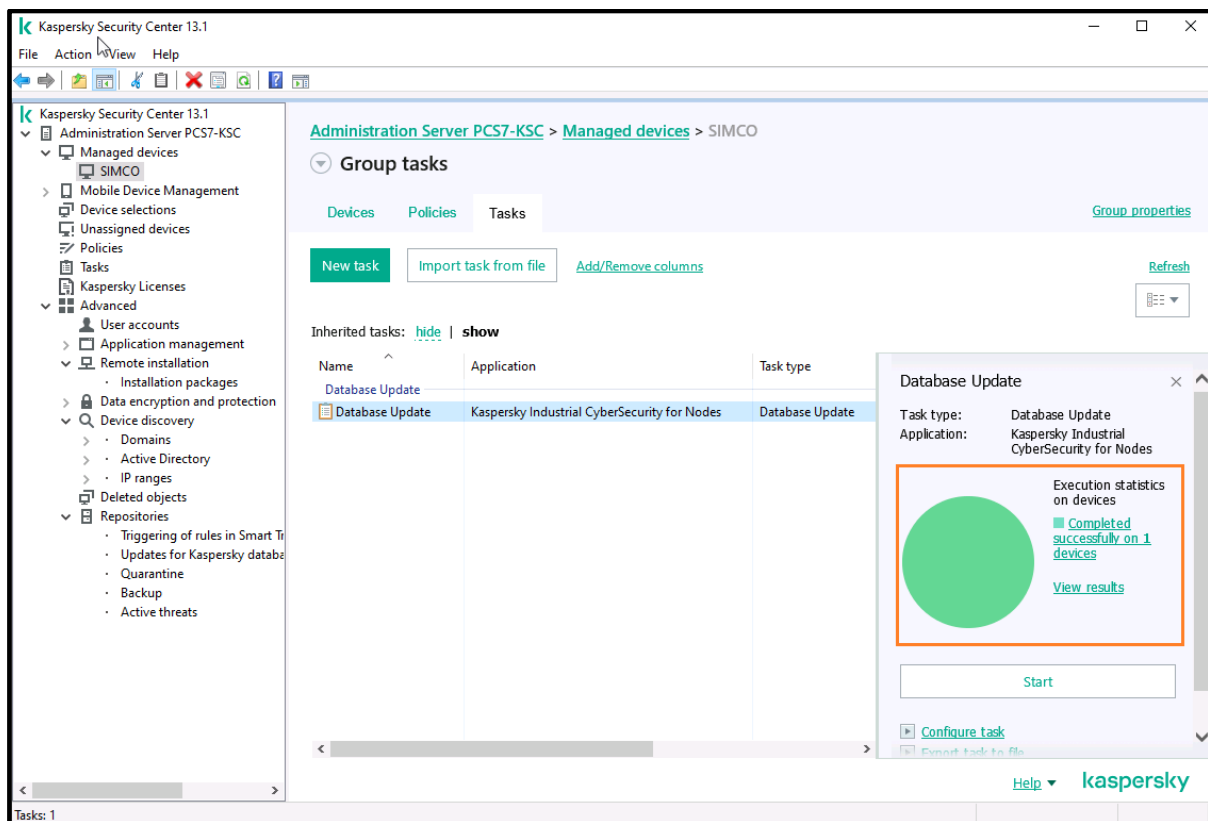


The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Define the task name'. Below this, there is a label 'Name:' followed by a text input field. The input field contains the text 'Database Update'. At the bottom right, there are 'Next' and 'Cancel' buttons.

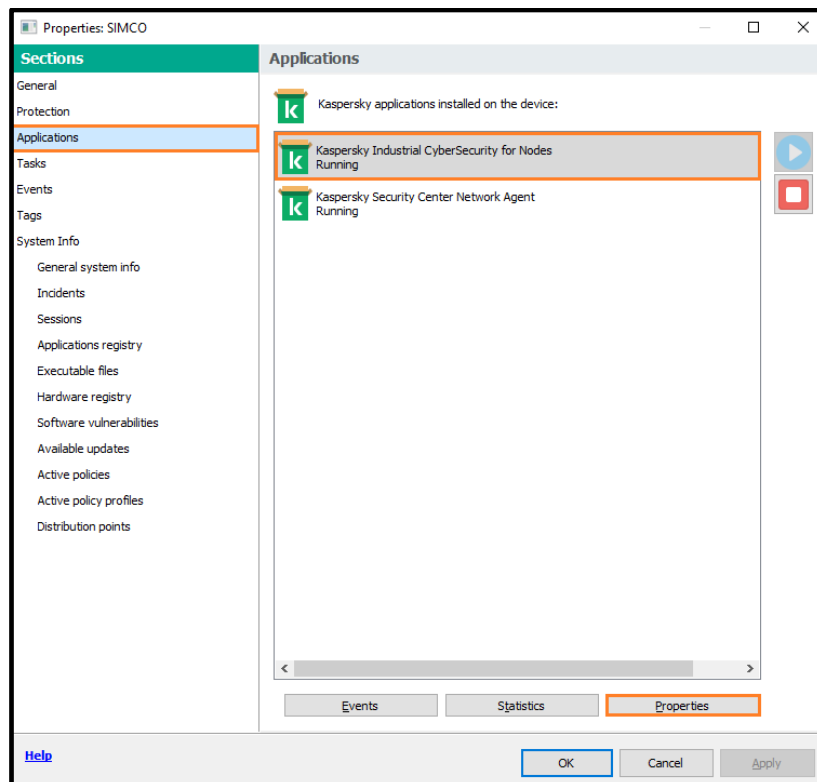
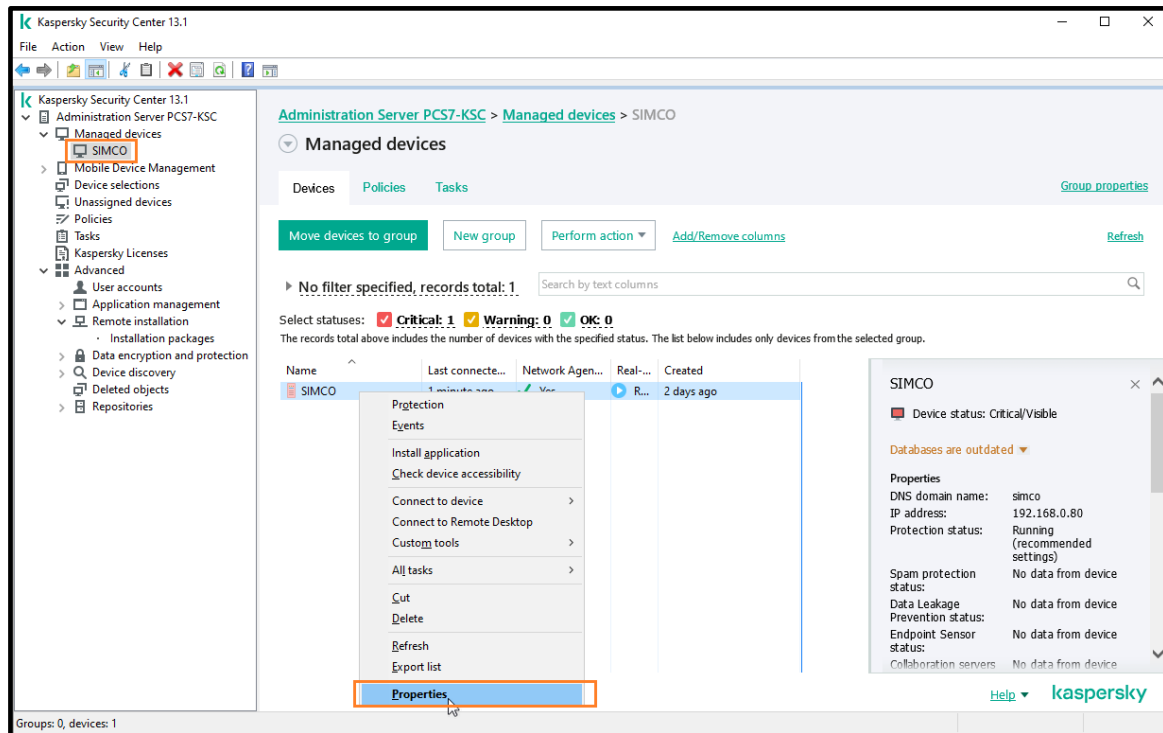
29. In the **Finish creating the task** window, check **Run task after Wizard finishes** and click **Finish**.

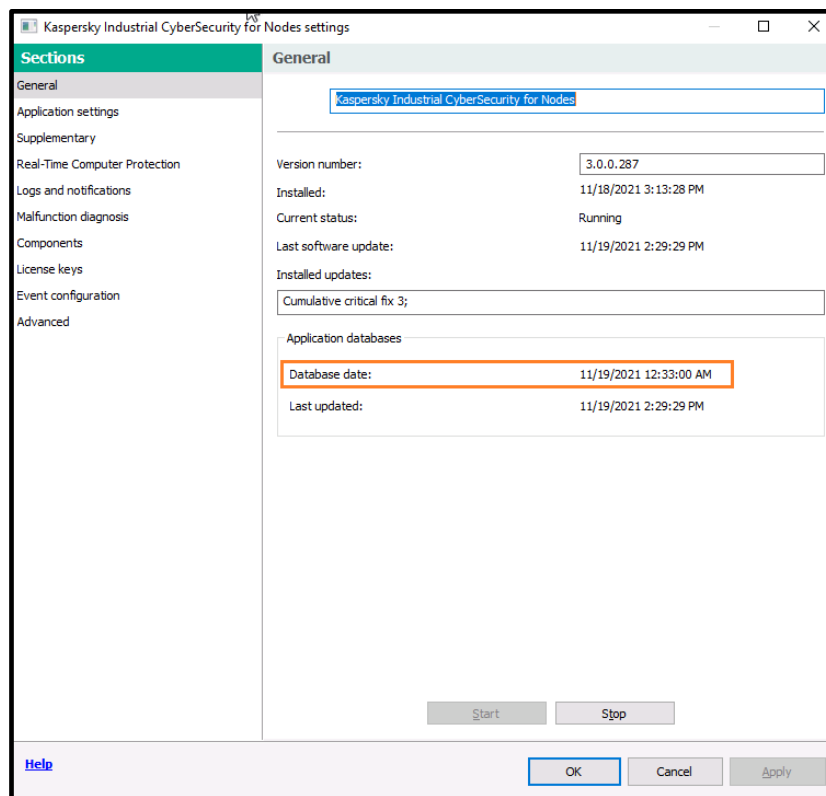


30. If you go to the group task list and select the just created task, you will see its execution progress displayed in the right-hand pane. Wait until the **Database Update** task gets marked as **Completed successfully**.

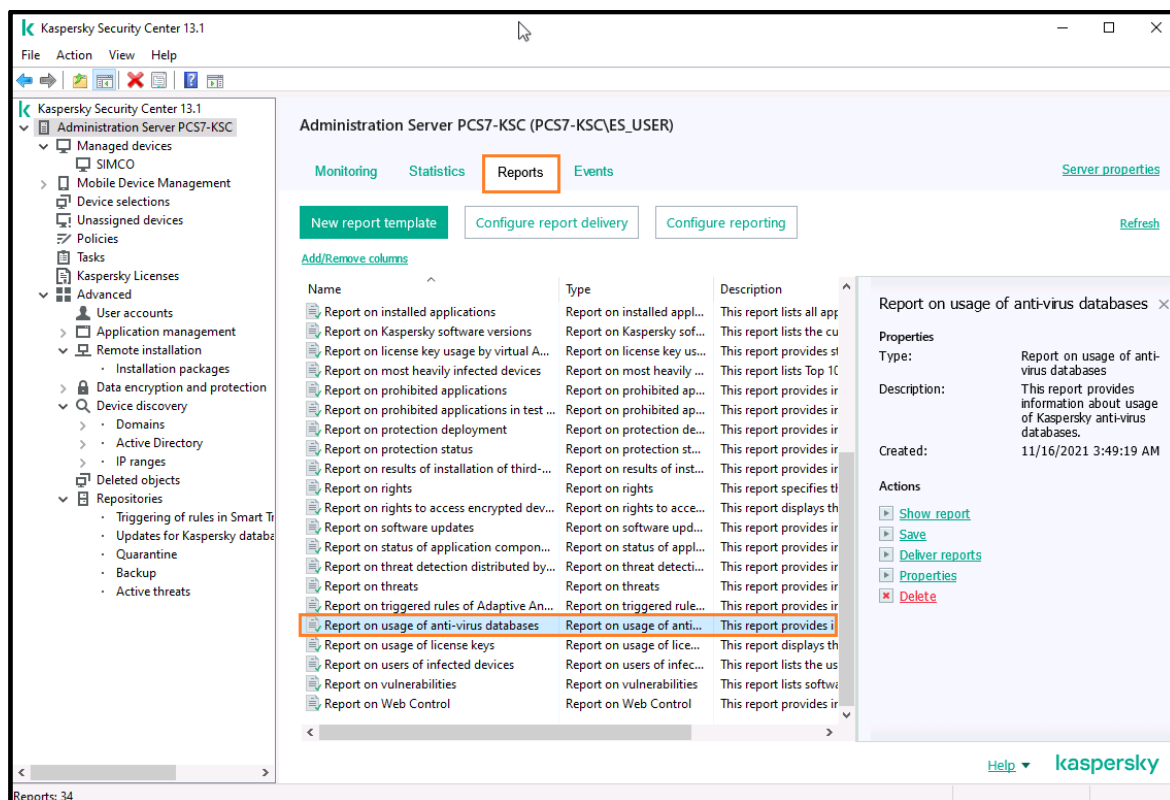


31. In order to make sure that our **KICS for Nodes** host (in our case, **SIMCO**) has received updated AV databases, switch to the **Devices** tab. Then right-click on the device and in the context menu select **Properties**. In the **Properties** window go to **Applications**; select **Kaspersky Industrial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





32. Alternatively, you can obtain detailed information on the actual databases from the **Report on usage of anti-virus databases**, available in **Administration Server->Reports** as shown below.



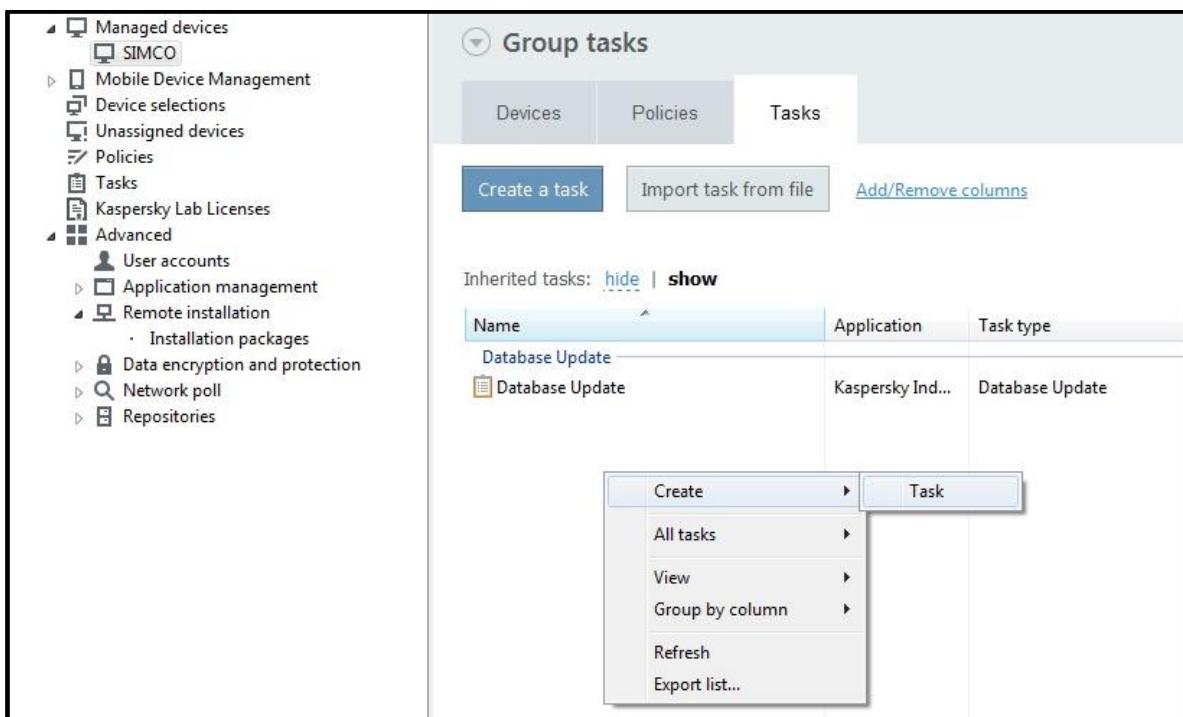
Performing On-Demand Scanning on target hosts

Once we the antivirus databases are actualized, 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 that could later appear on the **Application Launch Control** white list.

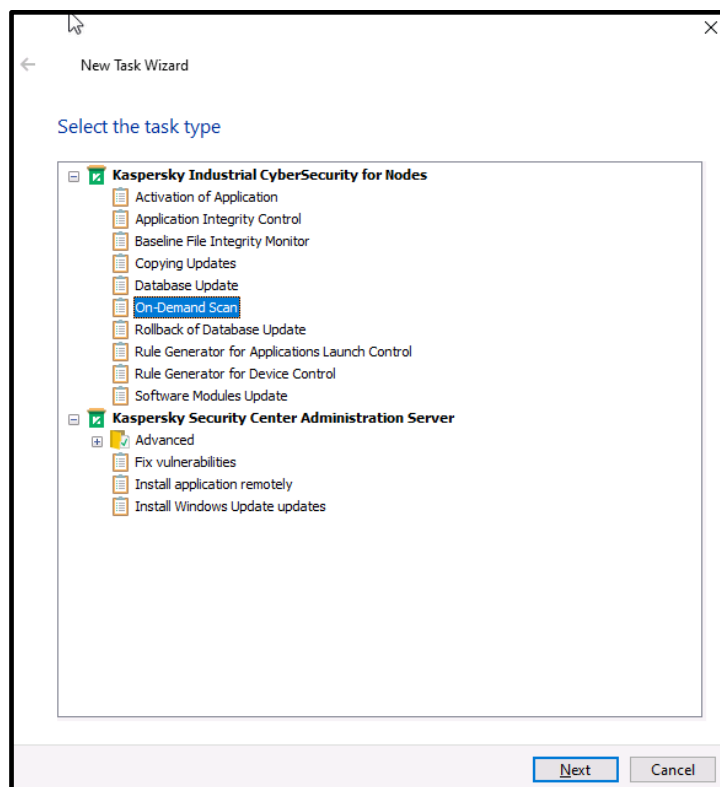
Obviously, the **On-Demand scan** requires some additional processing resources and may slightly deteriorate computer performance. That is why we recommend that you start this task only in the manual mode in order to be able to supervise its execution. The ideal case would be running this task during a control system standstill.

Please perform the following steps to configure the scanner:

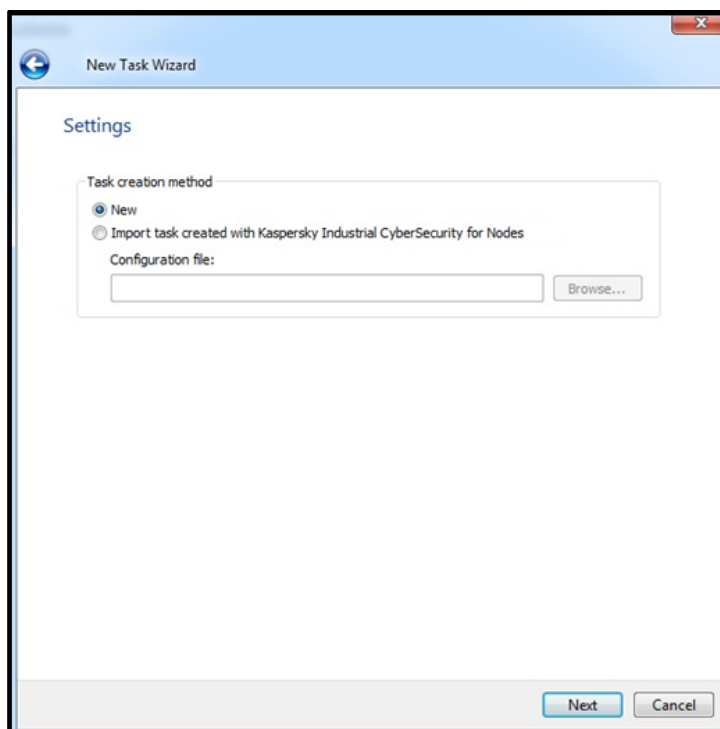
1. Go to the **SIMCO** group and switch to the **Tasks** tab. Using the context menu, start creating a new task as was shown earlier.



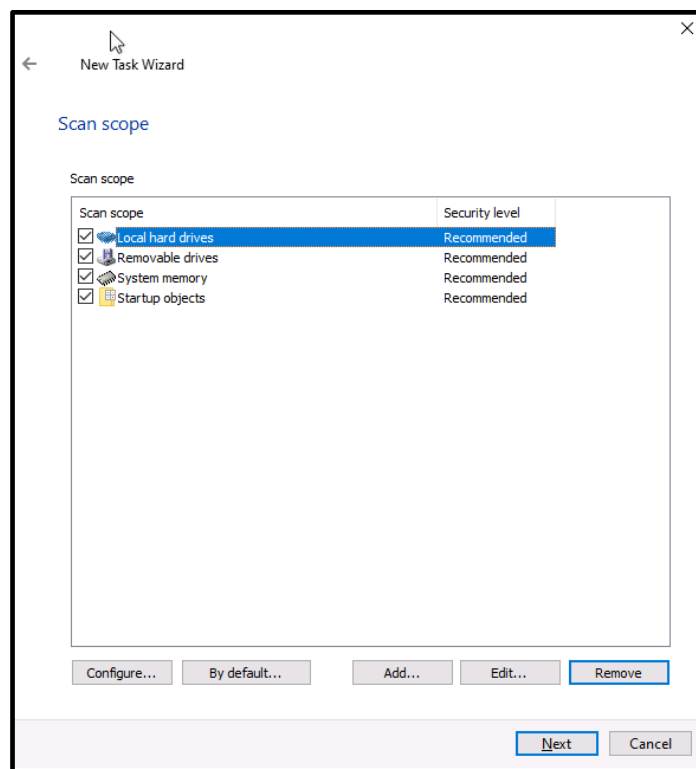
2. In the **New task wizard** window select **Kaspersky Industrial CyberSecurity for Nodes -> On-Demand Scan**. Click **Next**.



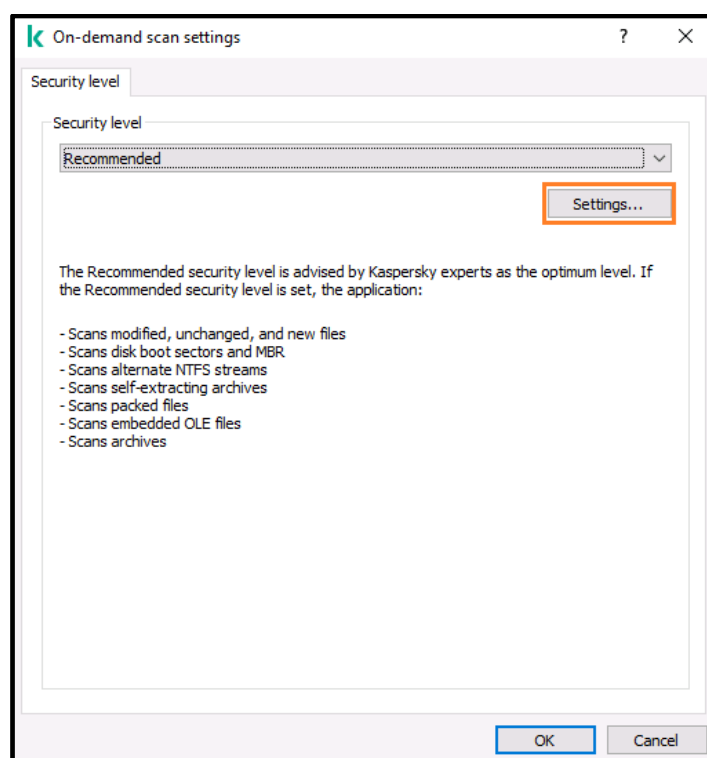
3. Keep the **Task creation method** selected as **New** and click **Next**.



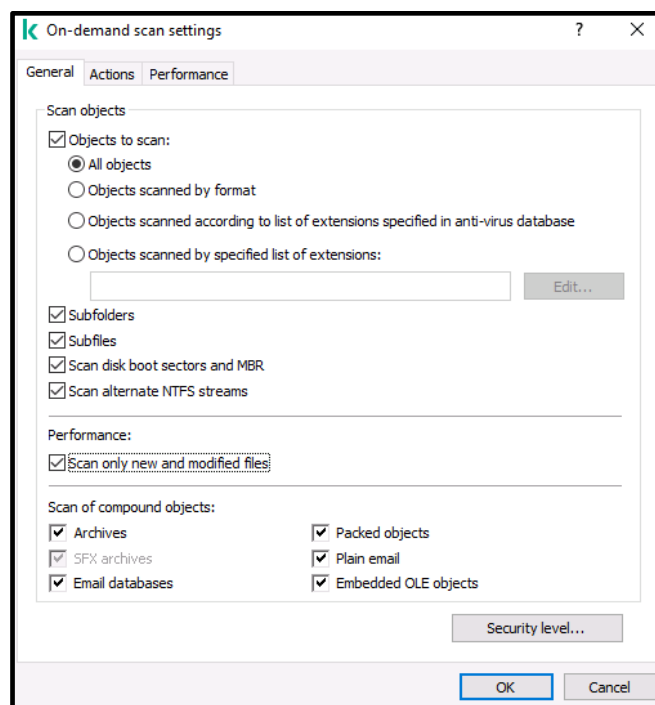
- Configure the **Scan scope** so that it would look as shown below. Select the **Local hard drives** item and double-click on it.



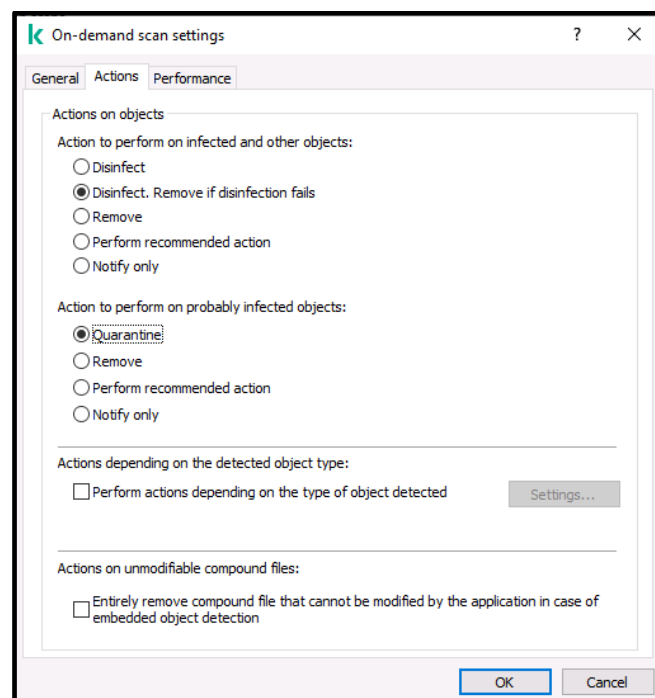
- In the following window that pops up click the **Settings...** button.



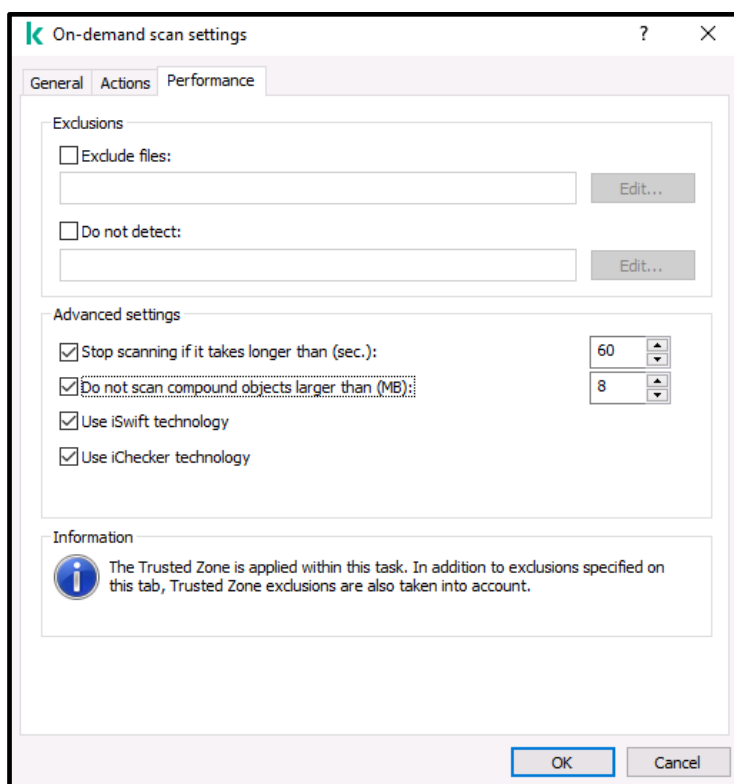
6. In the **On-demand scan settings** window, specify the settings as shown below.



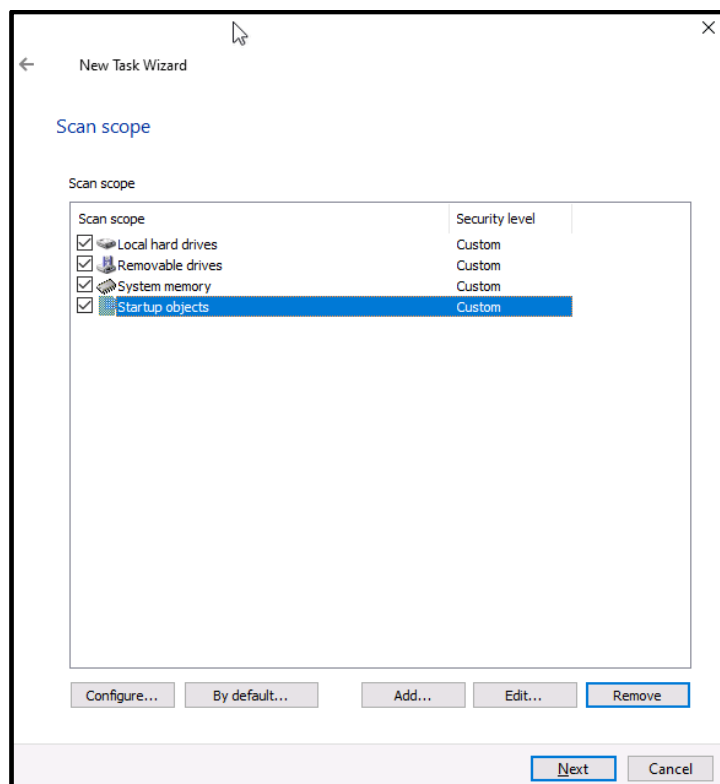
7. Switch over to the **Actions** tab. As a rule, we recommend applying the following settings, which seem quite a good compromise between control system security and its operability. However, your requirements may differ and some “softer” configuration may be chosen. For example, some would rather set up the antivirus engine to solely alert a threat than block or delete any files. Please consider this with extreme care before moving on.



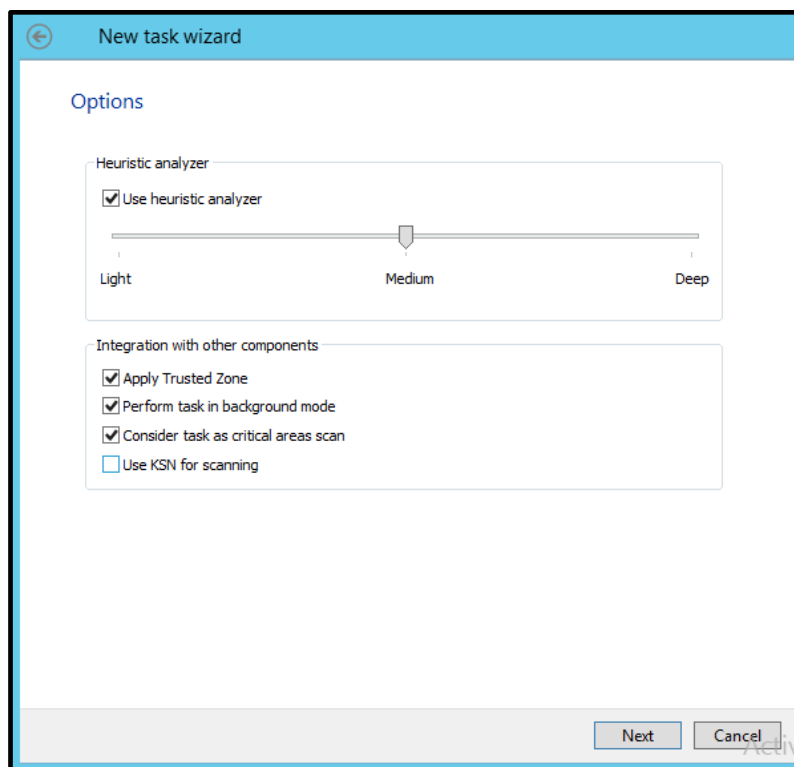
8. Switch over to the **Performance** tab and make the following configuration. Click **OK** when done.



9. Repeat steps 5-8 for the remaining item: **Removable drives**, **System memory** and **Startup objects**. Click **Next** when done.



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



New task wizard

Options

Heuristic analyzer

☒ Use heuristic analyzer

Light Medium Deep

Integration with other components

☒ Apply Trusted Zone

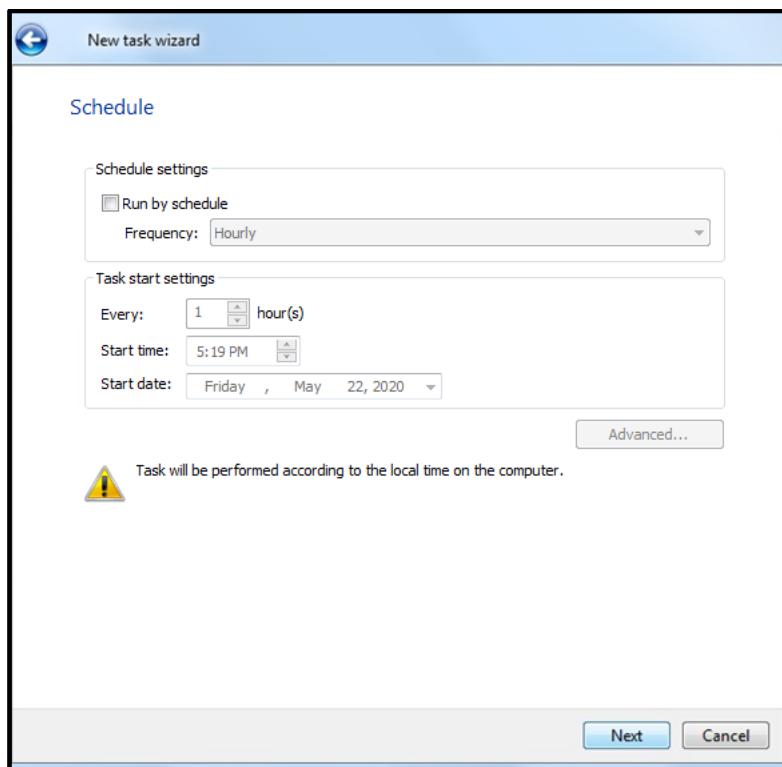
☒ Perform task in background mode

☒ Consider task as critical areas scan

☐ Use KSN for scanning

Next Cancel

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



New task wizard

Schedule

Schedule settings

☒ Run by schedule

Frequency: Hourly


Task start settings

Every: 1 hour(s)

Start time: 5:19 PM

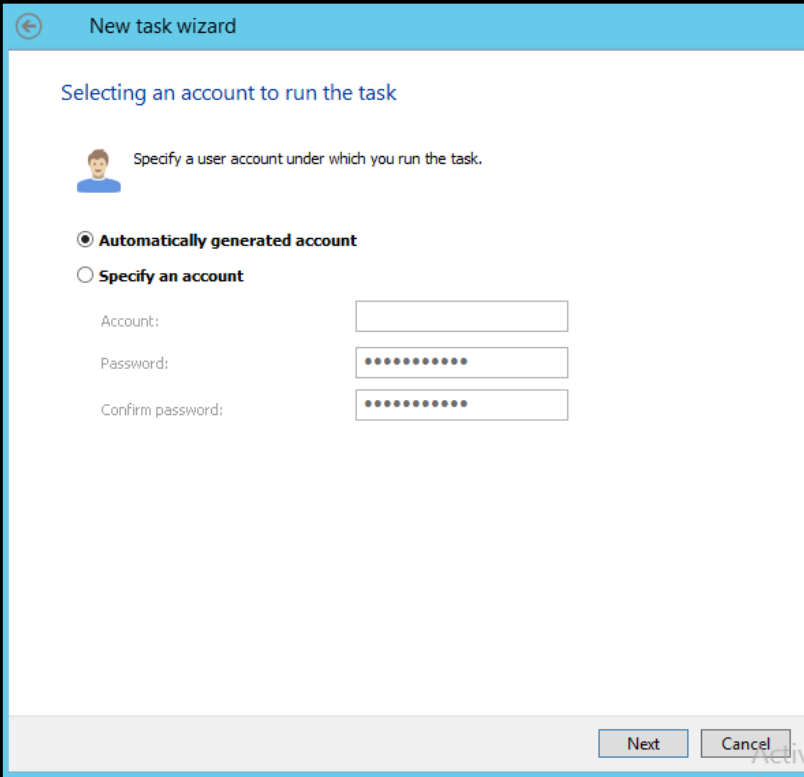
Start date: Friday, May 22, 2020

Advanced...

 Task will be performed according to the local time on the computer.

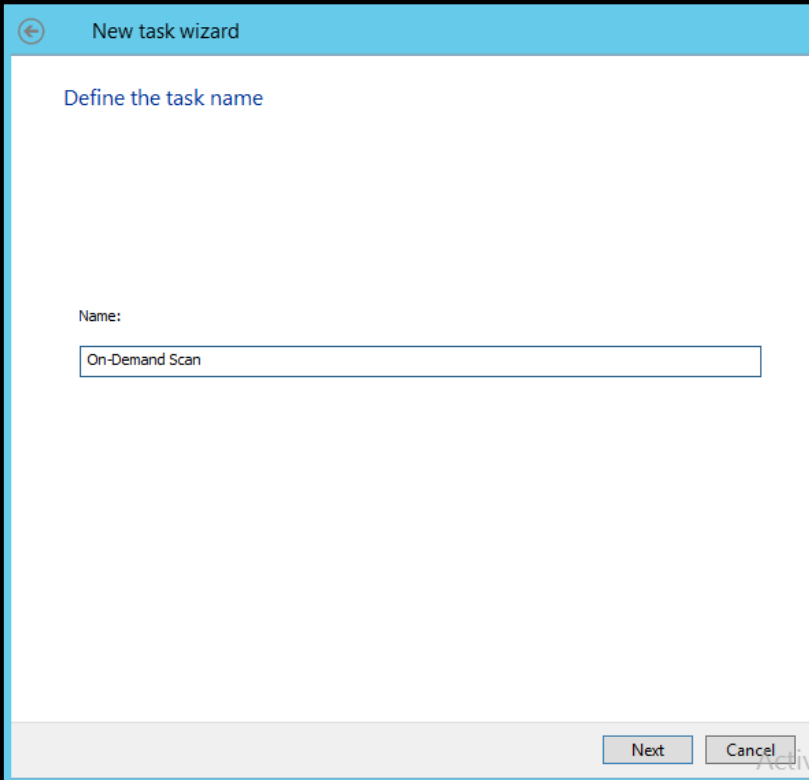
Next Cancel

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



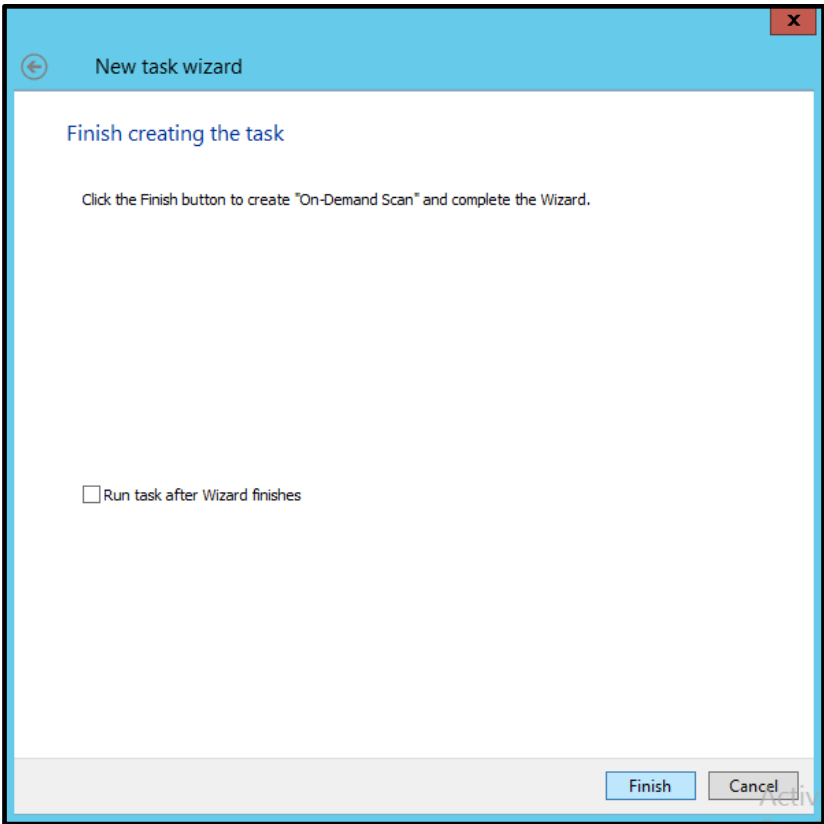
The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Selecting an account to run the task'. Below this, there is a user icon and the text 'Specify a user account under which you run the task.' There are two radio button options: 'Automatically generated account' (which is selected) and 'Specify an account'. Under 'Specify an account', there are three input fields: 'Account:', 'Password:', and 'Confirm password:'. The 'Next' and 'Cancel' buttons are at the bottom right.

13. Give a new name to the task or keep the default one and click **Next**.

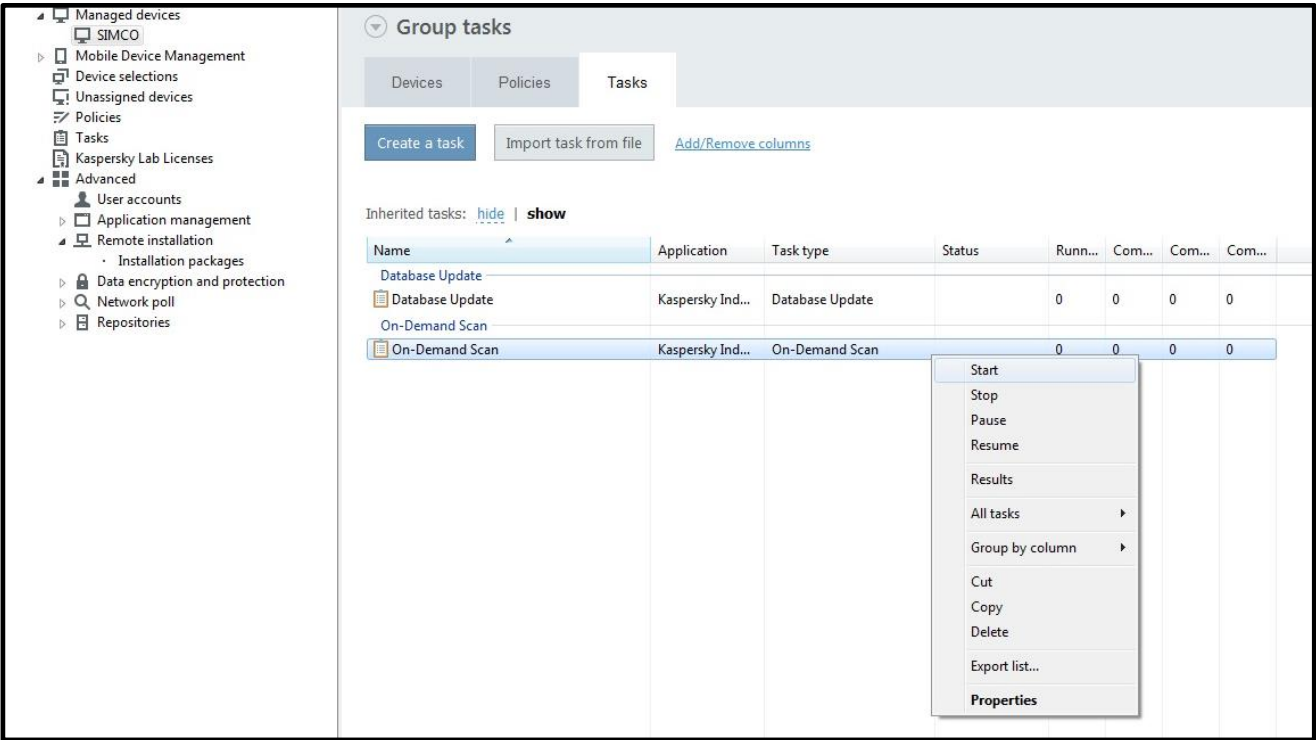


The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Define the task name'. Below this, there is a 'Name:' label and a text input field containing 'On-Demand Scan'. The 'Next' and 'Cancel' buttons are at the bottom right.

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



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



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

Execution of the Generate Rules for Application Launch Control task

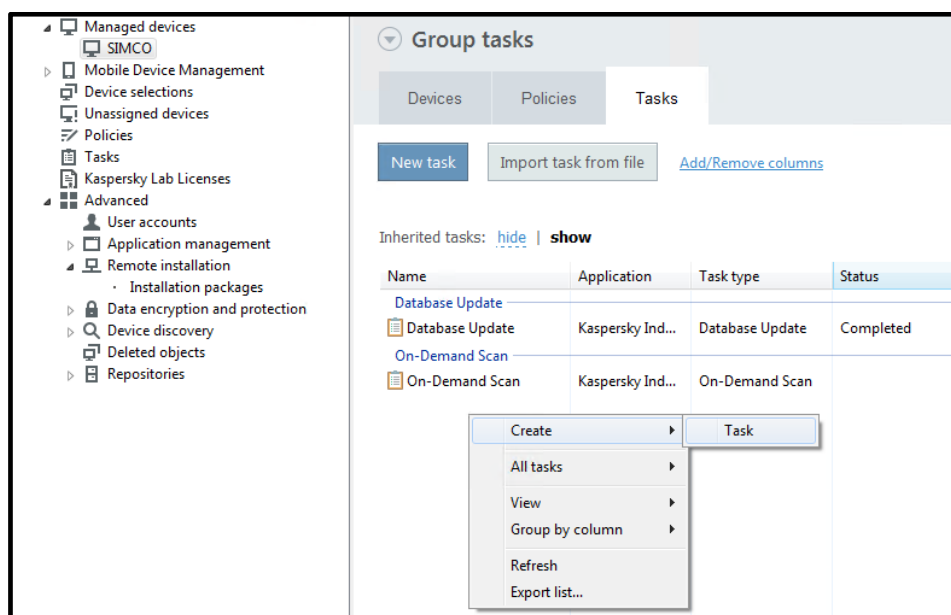
Following its activation, **Application Launch Control** keeps on watching executable files launches by referring to the predefined list of legitimate applications (to the, so called, white list). The module can also process dll calls as well as script runs. **Application Launch Control** can function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

- 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 **Active** mode, the module blocks execution of any file which is not on the white list.

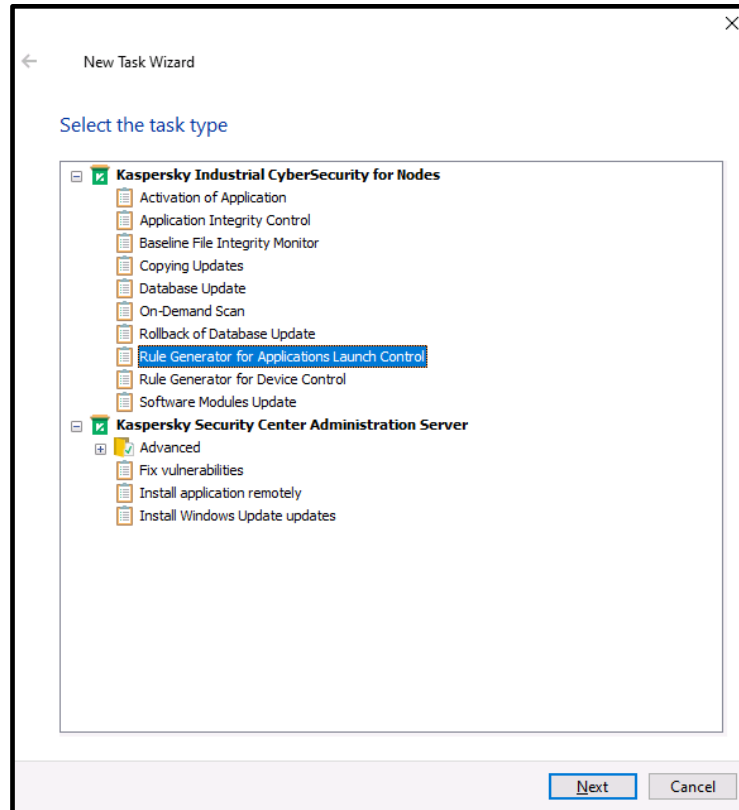
Please note, that the **Statistic only** mode is the most appropriate option for industrial control systems as it provides an optimal balance between preserving DCS performance/robustness, on the one hand, and providing the sufficient cyber protection level, on the other.

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

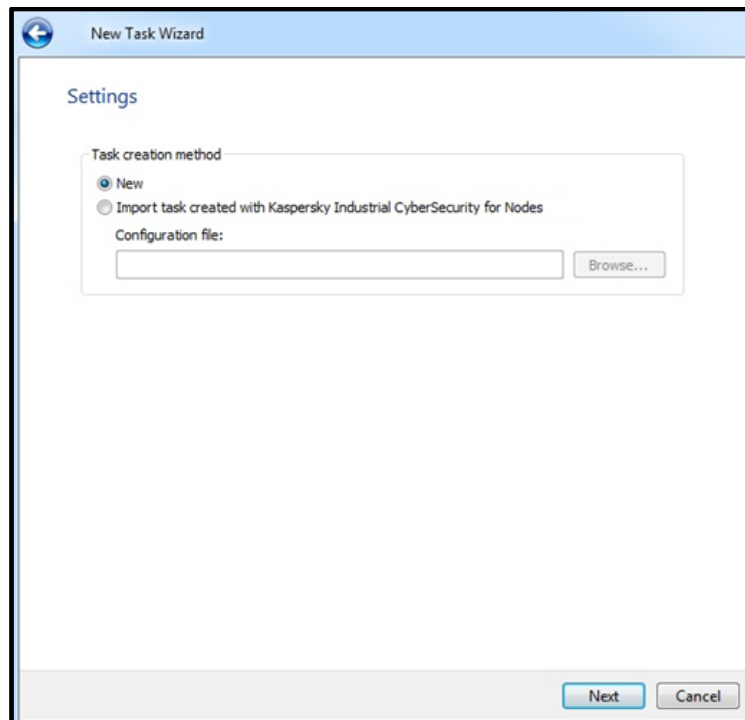
1. Remain in our managed devices group (**SIMCO**, in our case) and enter the **Tasks** tab. Right-click on the **Tasks** list and in the context menu choose **Create->Task**.



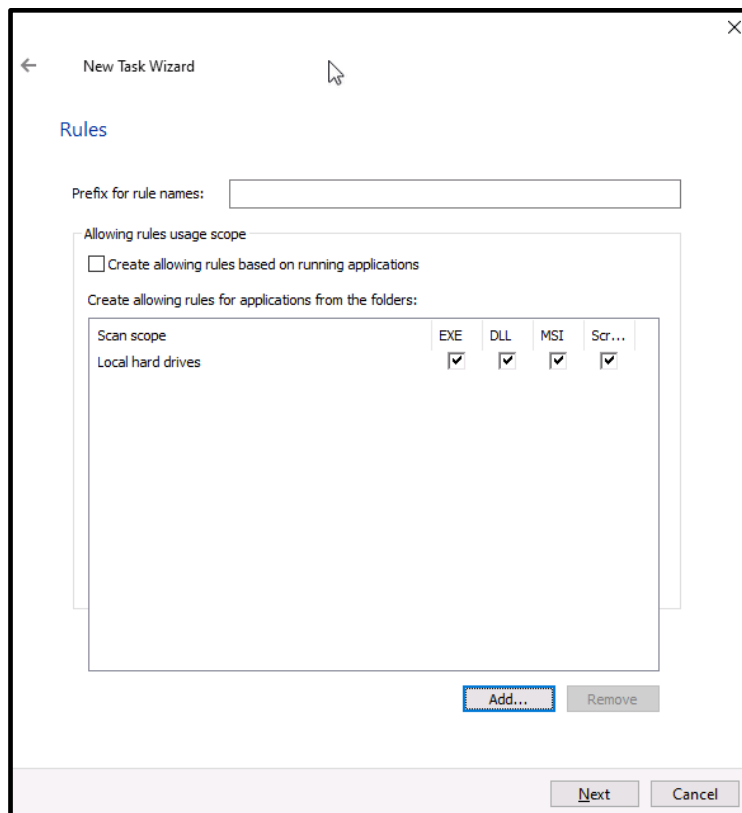
2. In the **Select the task type** window that pops up select **Rule Generator for Application Launch Control**. Click **Next**.



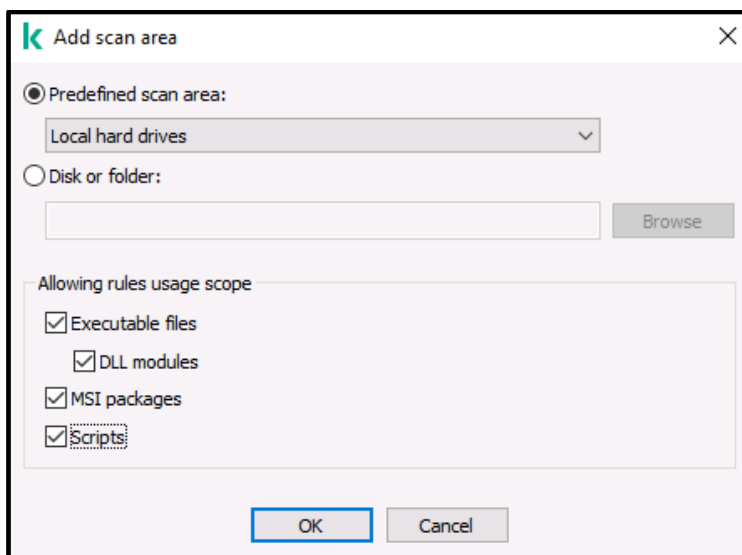
3. Leave the **Task creation method** selected as **New** and click **Next**.



- In the **Rules** window that follows click the **Add...** button to specify the scan scope.

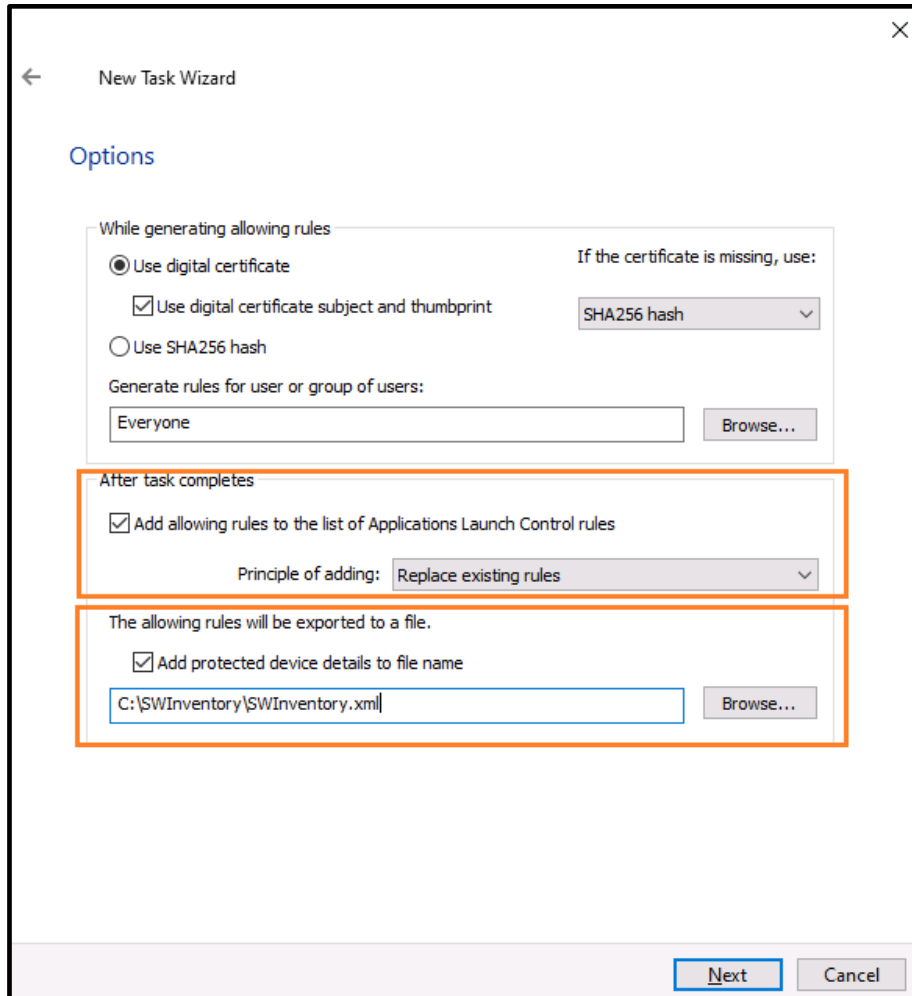


- Define the scan area as **Local hard drives** and tick all the checkboxes as shown below. Click **OK**.



- In the following window, complete the settings as shown in the example below. In our study case, we have previously created the **SWInventory** folder on the **C:** drive of our **SIMCO** station. It is where the automatically generated rule list (in a format of the XML-file) will be put onto 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 **Replace allowing rules to the list of**

Application Launch Control list. This option facilitates the module configuration so that we will not practically need to deal with an XML-file (this file will be created though). Click **Next**.



New Task Wizard

Options

While generating allowing rules

☒ Use digital certificate If the certificate is missing, use:

☒ Use digital certificate subject and thumbprint SHA256 hash

☐ Use SHA256 hash

Generate rules for user or group of users:

Everyone Browse...

After task completes

☒ Add allowing rules to the list of Applications Launch Control rules

Principle of adding: Replace existing rules

The allowing rules will be exported to a file.

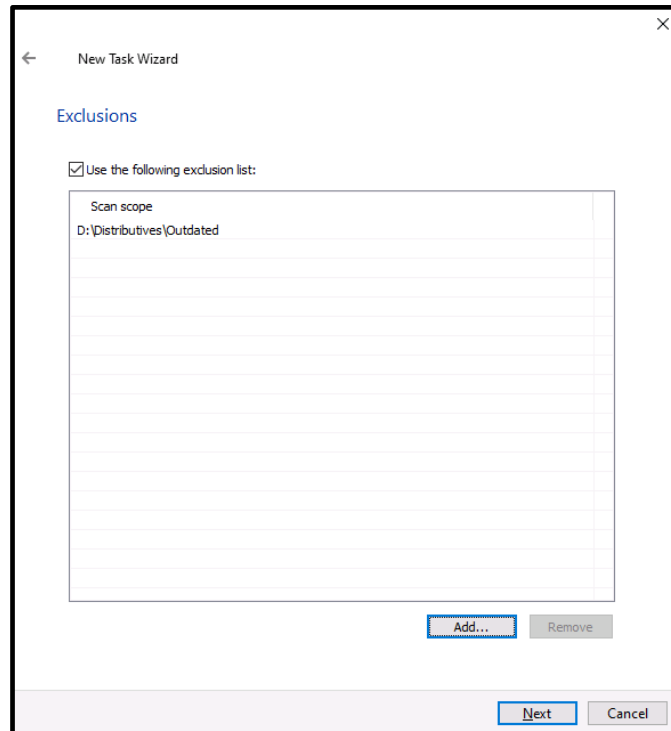
☒ Add protected device details to file name

C:\\$WInventory\\$WInventory.xml Browse...

Next Cancel

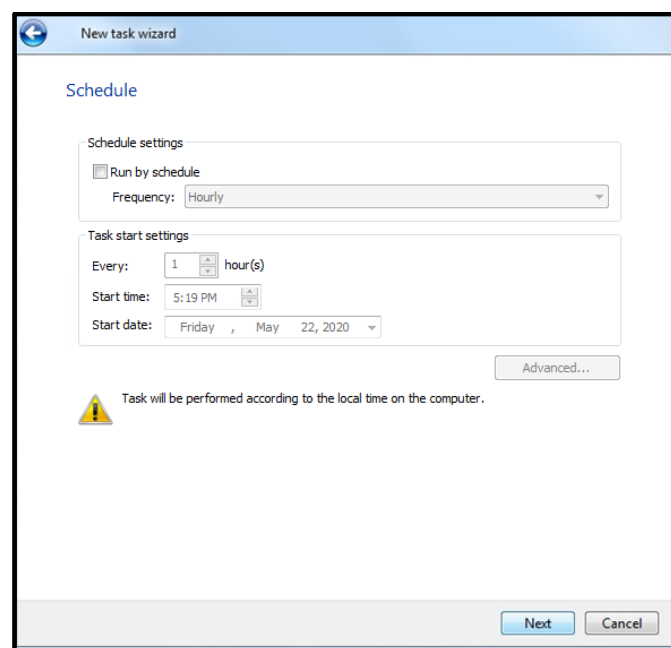
7. According to the architectural limitations of **Application Launch Control**, the rule list can not contain more than 65532 rules. However, the fewer items there are on the list, the better it is from the performance point of view. That is why it is good to keep the white list as compact as possible by excluding those executable files which are 100% not going to be utilized. In particular, it is relevant to file storages.

For example, it is assumed that in our study case we have a collection of outdated software distributives which are hardly ever used: these are located in D:\Distributives\Outdated. So, we would not want to litter our white list with those files.

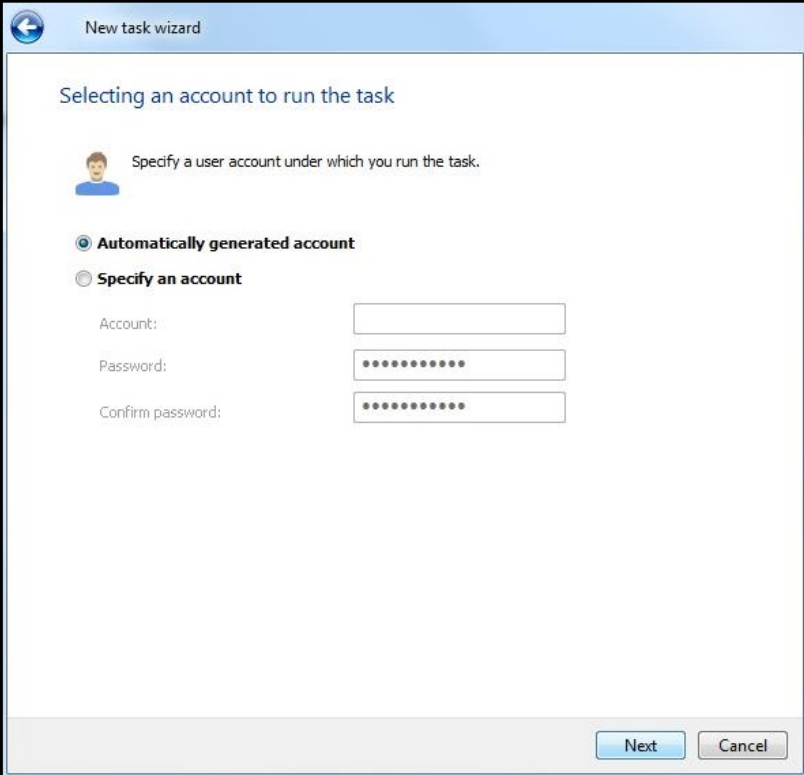


Please note that, as per our research, engineering workstations of SIMATIC PCS7 v9.1 always require the following exclusion to the generation scope to be considered: C:\Program Files (x86)\SIEMENS\STEP7\s7hlp*.js

8. In the **Schedule** window simply click **Next**.

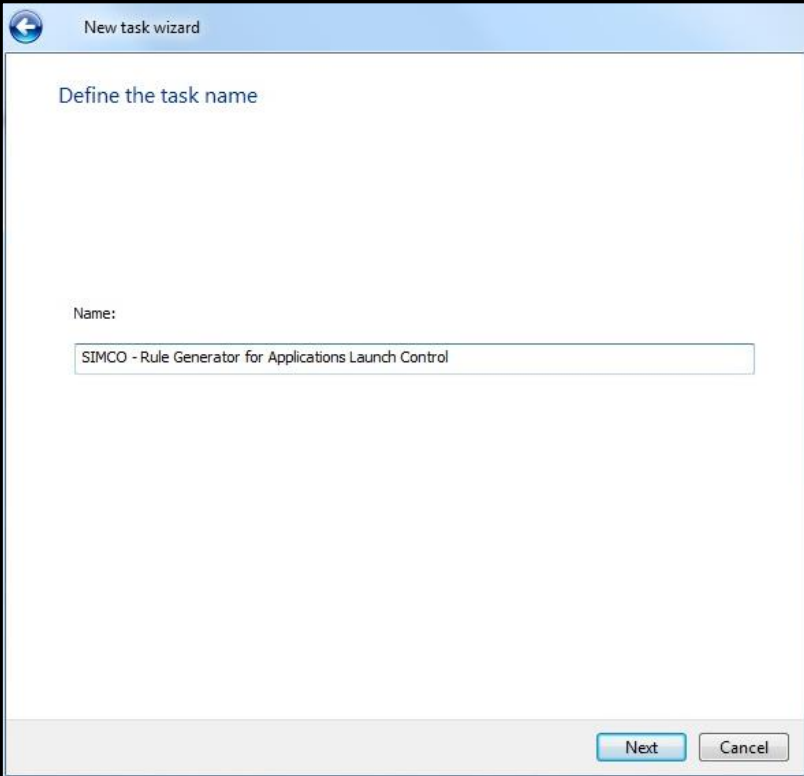


9. In the **Selecting an account to run the task** window select **Automatically generated account** and click **Next**.



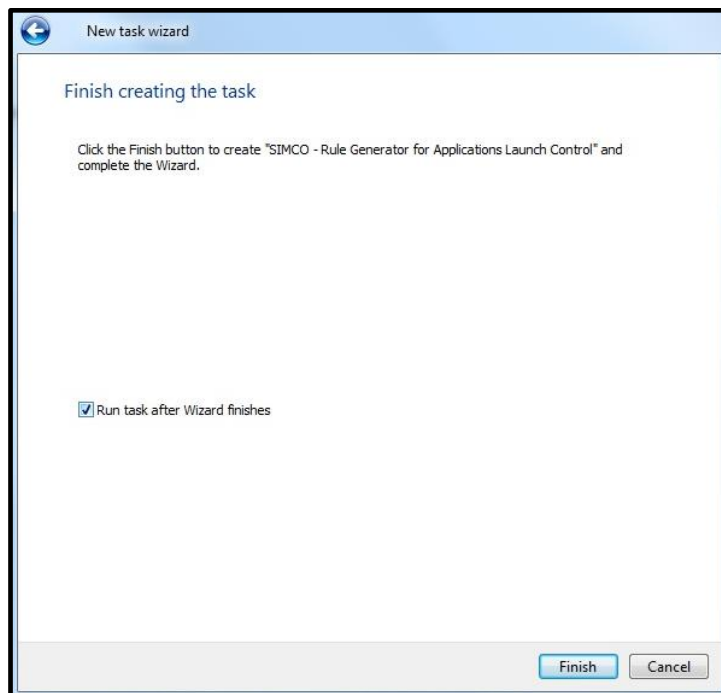
The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Selecting an account to run the task'. Below this, there is a user icon and the text 'Specify a user account under which you run the task.' There are two radio button options: 'Automatically generated account' (which is selected) and 'Specify an account'. Under 'Specify an account', there are three input fields: 'Account:', 'Password:', and 'Confirm password:'. The 'Next' and 'Cancel' buttons are at the bottom right.

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

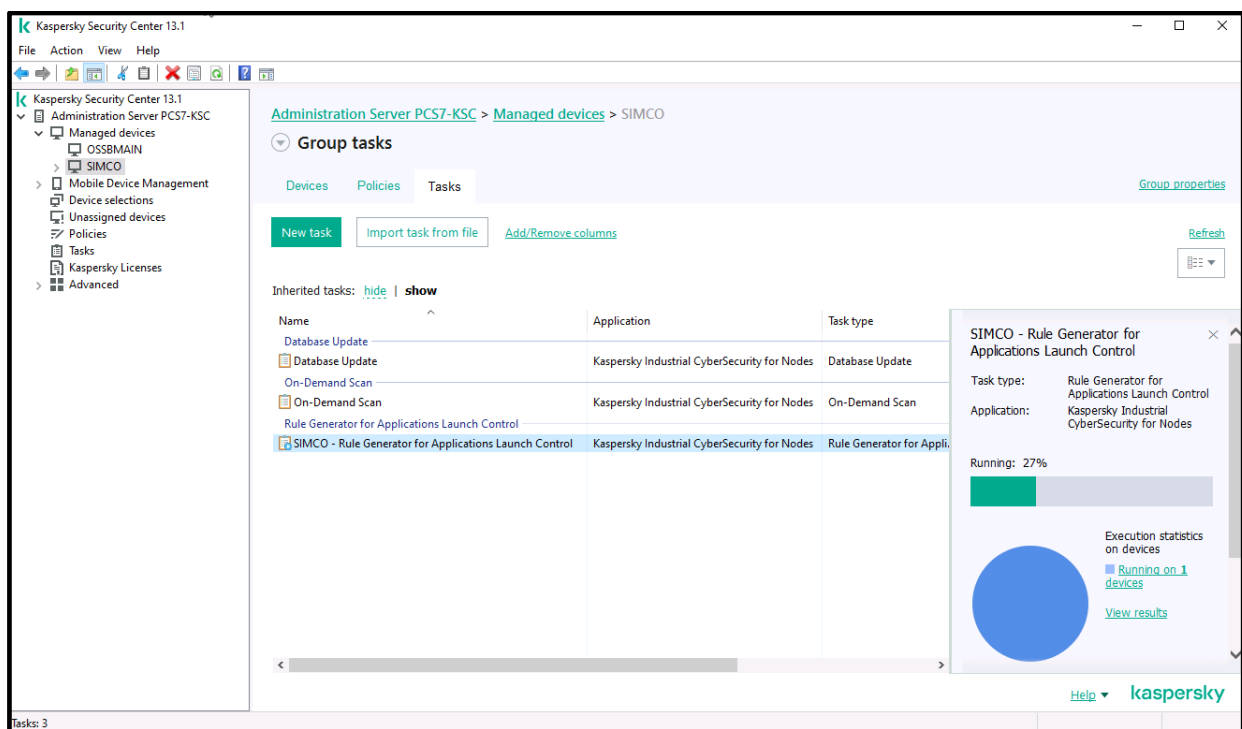


The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Define the task name'. Below this, there is a 'Name:' label and a text input field containing the text 'SIMCO - Rule Generator for Applications Launch Control'. The 'Next' and 'Cancel' buttons are at the bottom right.

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



12. 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!**



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

Setting up Application Launch Control whitelisting

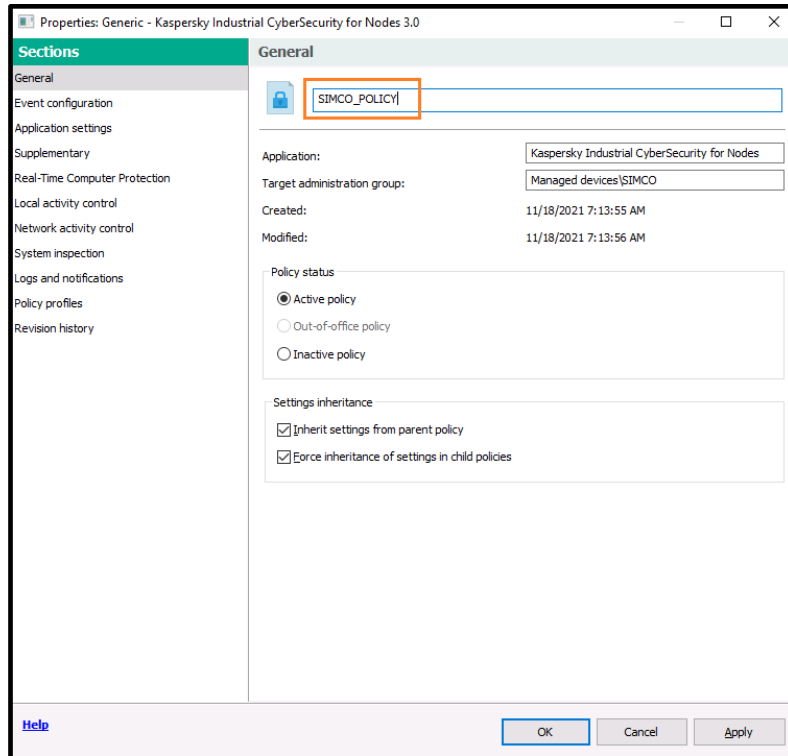
Now we are ready to fine-tune our generic (“backbone”) policy, which we have created and applied to the **SIMCO** host earlier.

Please perform the following steps to rectify the **Application Launch Control** settings:

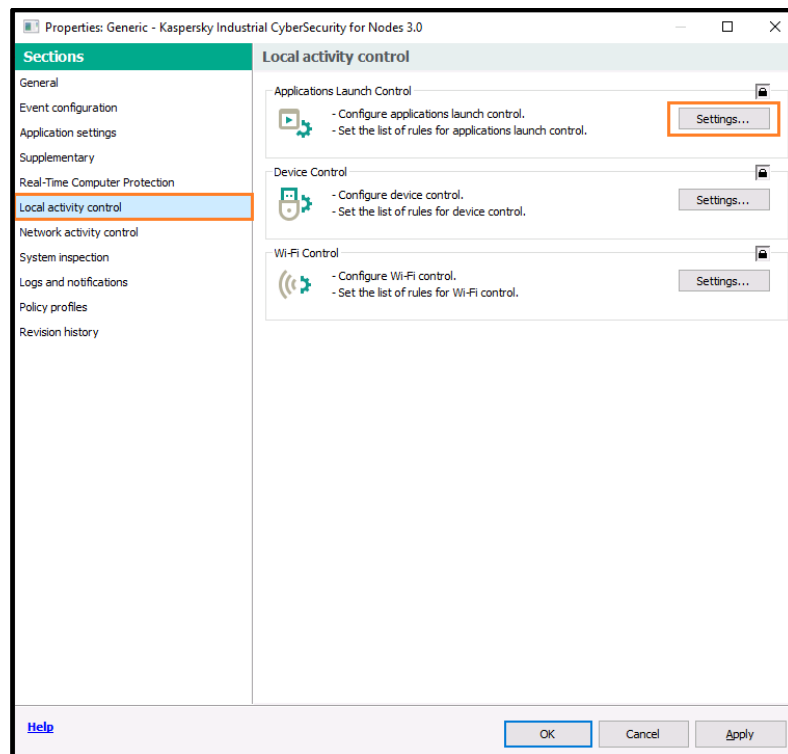
1. Remain in the **SIMCO** subgroup and switch to the **Policies** tab.
2. Locate the **Generic – Kaspersky Industrial CyberSecurity for Nodes 3.0** policy, which we have created before, and enter its **Properties**.

The screenshot displays the Kaspersky Security Center 13.1 interface. The left sidebar shows the navigation tree with 'SIMCO' selected under 'Managed devices'. The main pane is titled 'Administration Server PCS7-KSC > Managed devices > SIMCO' and shows the 'Policies' tab. A table lists policies, with 'Generic - Kaspersky Industrial CyberSecurity for Nodes 3.0' selected. A context menu is open over this policy, showing options like 'Active policy', 'Compare policy to another policy', 'Export', 'All tasks', 'Group by column', 'Cut', 'Copy', 'Delete', 'Export list', and 'Properties' (which is highlighted). On the right, a details pane for the selected policy shows its application, creation and change dates, and a green circle indicating enforcement status. The status text reads: 'Affected: 1 device(s)', 'Enforcement successful: 1 device(s)'. At the bottom, there are links for 'Configure policy', 'Configure notifications', and 'Export policy to file'.

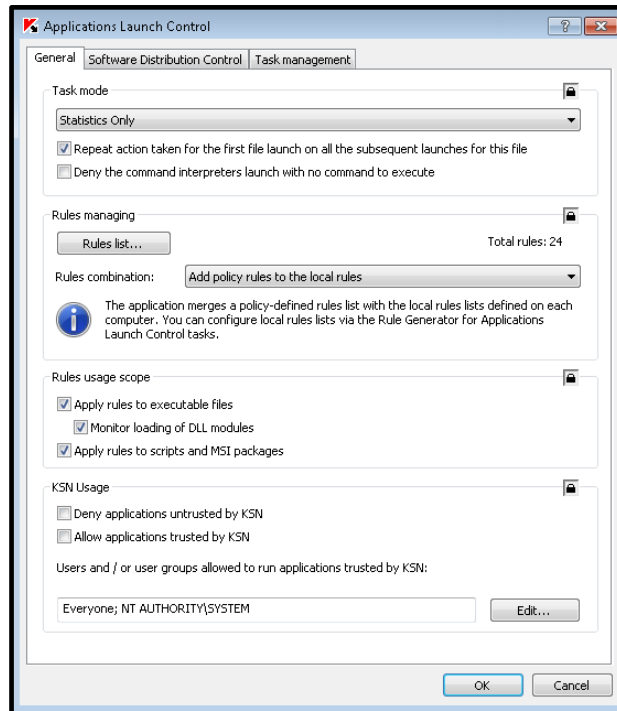
- In order to avoid confusion, give the policy some more specific name by editing the text field as shown below.
In our case, we will rename the policy to **SIMCO_POLICY**. Press **Apply** to save changes.



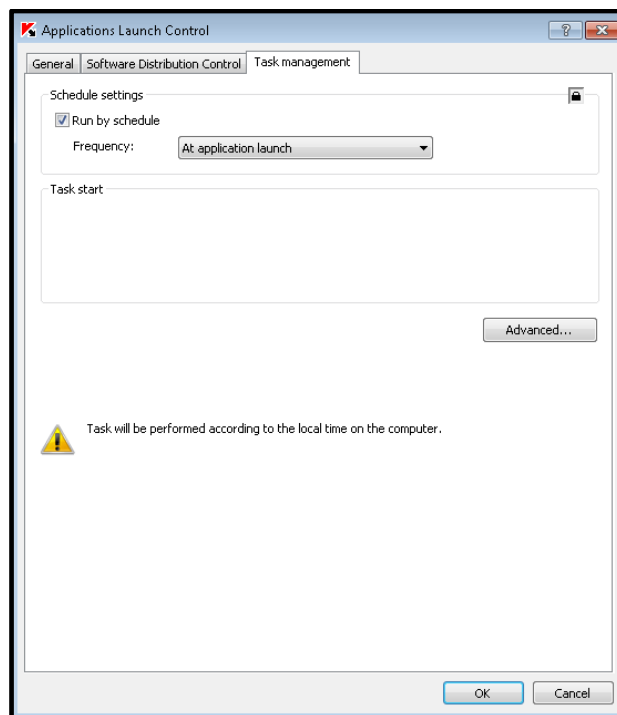
- Move on to **Local activity control**, press the **Settings...** button located on the **Application Launch Control** panel.




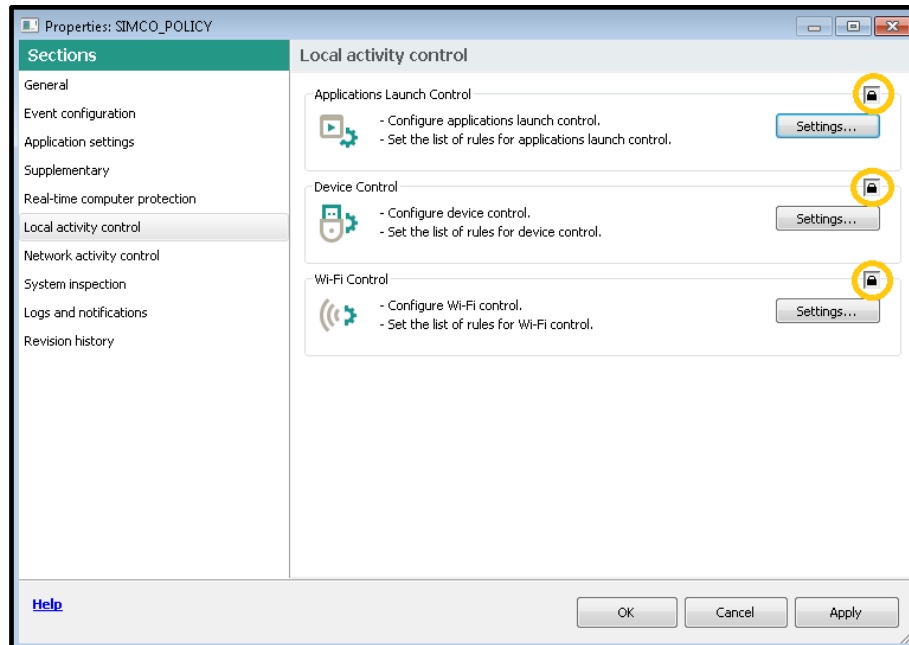
- One you have got the **General** tab, make sure all the settings match those shown in the screenshot below. Please note that the host-specific rule list (white list), which has been generated by the **Generate Rules for Application Launch Control** task, is stored on the target host locally: you will not see it here.



- Now switch to the **Task Management** tab and specify the settings as shown below. In particular, make sure that **At application launch** is selected from the **Frequency** drop-down list. Click **OK** to close the window. This will finally put **Application Launch Control running** into operation.



- Once you have reverted to the main window, close all **locks** , press **Apply** and then **OK** to exit editing the **SIMCO_POLICY** properties.



As a result, 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, as an example, we are going to add a removable storage device to the white list of legitimate devices. Please go through the following steps:

- 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 will be **SIMCO**.
- Wait for some minutes and then unplug the USB device.

- 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.

Administration Server KSC (KSC\Administrator)

Monitoring Statistics Reports Events

Selection events **Recent events** ★

Run selection Selection properties Create a selection Import/Export ▼

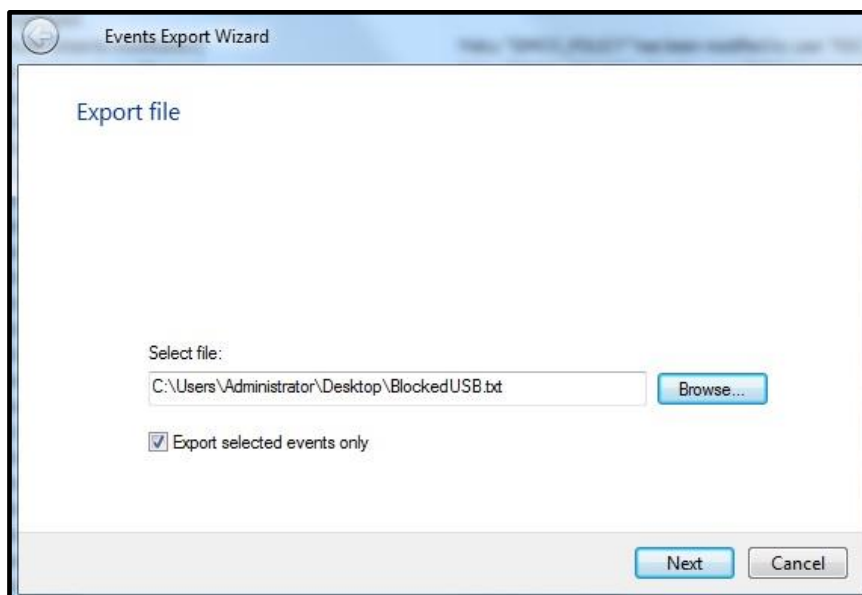
Add/Remove columns

Time	Device	Event	Description	Group
20.02.2018 18:34:58	SIMCO	Statistics Only: untrusted mass storage detected	("Vendor": "VID_090C", "Product": "PID_1000", "SerialNum"...	SIMCO
20.02.2018 18:32:29	SIMCO	Running		SIMCO
20.02.2018 18:33:22	SIMCO	Modified		SIMCO
20.02.2018 18:33:21	SIMCO	Modified		SIMCO
20.02.2018 18:33:22	Administration Server <K...	Audit (changes to the object's status)	Group task "Managed devices/SIMCO/SIMCO - Rule Gen...	Managed devices
20.02.2018 18:33:21	Administration Server <K...	Audit (objects modification)	Group task "Managed devices/SIMCO/SIMCO - Rule Gen...	Managed devices
20.02.2018 18:33:22	SIMCO	Scheduled		SIMCO
20.02.2018 18:33:21	SIMCO	Scheduled		SIMCO
20.02.2018 18:26:42	Administration Server <K...	Audit (objects modification)	Policy "SIMCO_POLICY" has been modified by user "KSC\...	Managed devices
20.02.2018 18:02:11	Administration Server <K...	Audit (objects modification)	Policy "SIMCO_POLICY" added by user "KSC\Administrator"	Managed devices
20.02.2018 17:44:58	Administration Server <K...	Audit (objects modification)	Policy "Kaspersky Security Center 10 Network Agent" ad...	Managed devices
20.02.2018 17:43:35	Administration Server <K...	Device status is Critical	Status of device "SIMCO" changed to Critical: Windows u...	Managed devices
20.02.2018 17:34:49	SIMCO	Real-time protection security level has changed		SIMCO
20.02.2018 17:35:44	SIMCO	Completed	Remote installation has been successfully completed on t...	SIMCO
20.02.2018 17:34:38	SIMCO	Running	Setup started.	SIMCO

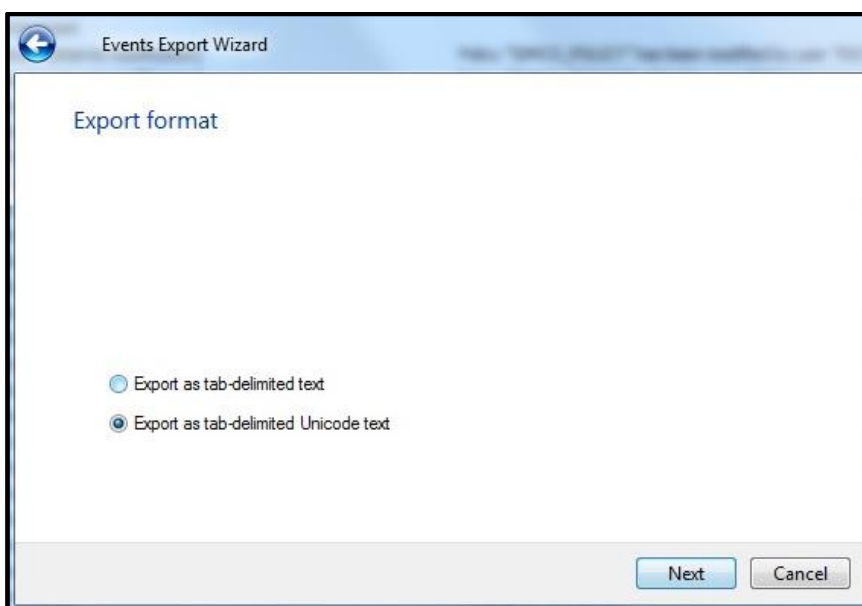
- Looking through the **Events** list, find the recent notification **Statistics Only: untrusted mass storage detected**. This behavior is correct because our **Device Control** white list is still empty. That is why any USB device connected to the target host is treated as an untrusted one.
- Select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

Time	Device	Event	Description	Group
20.02.2018 18:34:58	SIMCO	Statistics Only: untrusted mass storage detected	("Vendor": "VID_090C", "Product": "PID_1000", "SerialNum"...	SIMCO
20.02.2018 18:32:29	SIMCO	Running		SIMCO
20.02.2018 18:33:22	SIMCO	Modified		SIMCO
20.02.2018 18:33:21	SIMCO	Modified		SIMCO
20.02.2018 18:33:22	Administration Server <K...	Audit (changes to the object's status)	devices/SIMCO/SIMCO - Rule Gen...	Managed devices
20.02.2018 18:33:21	Administration Server <K...	Audit (objects modification)	devices/SIMCO/SIMCO - Rule Gen...	Managed devices
20.02.2018 18:33:22	SIMCO	Scheduled		SIMCO
20.02.2018 18:33:21	SIMCO	Scheduled		SIMCO
20.02.2018 18:26:42	Administration Server <K...	Audit (objects modification)	" has been modified by user "KSC\...	Managed devices
20.02.2018 18:02:11	Administration Server <K...	Audit (objects modification)	" added by user "KSC\Administrator"	Managed devices
20.02.2018 17:44:58	Administration Server <K...	Audit (objects modification)	ity Center 10 Network Agent" ad...	Managed devices
20.02.2018 17:43:35	Administration Server <K...	Device status is Critical	O' changed to Critical: Windows u...	Managed devices
20.02.2018 17:34:49	SIMCO	Real-time protection security level has changed		SIMCO
20.02.2018 17:35:44	SIMCO	Completed	has been successfully completed on t...	SIMCO
20.02.2018 17:34:38	SIMCO	Running	Setup started.	SIMCO
20.02.2018 17:35:26	Administration Server <K...	Audit (changes to the object's status)	Task for specific devices "Deploy KICS4NODES_HotFix8" ...	Managed devices
20.02.2018 17:35:26	Administration Server <K...	Audit (objects modification)	Task for specific devices "Deploy KICS4NODES_HotFix8" ...	Managed devices
20.02.2018 17:35:26	SIMCO	Running	Copying files to the specified device...	SIMCO
20.02.2018 17:35:26	SIMCO	Scheduled	Waiting for connection	SIMCO
20.02.2018 17:35:26	SIMCO	Scheduled		SIMCO

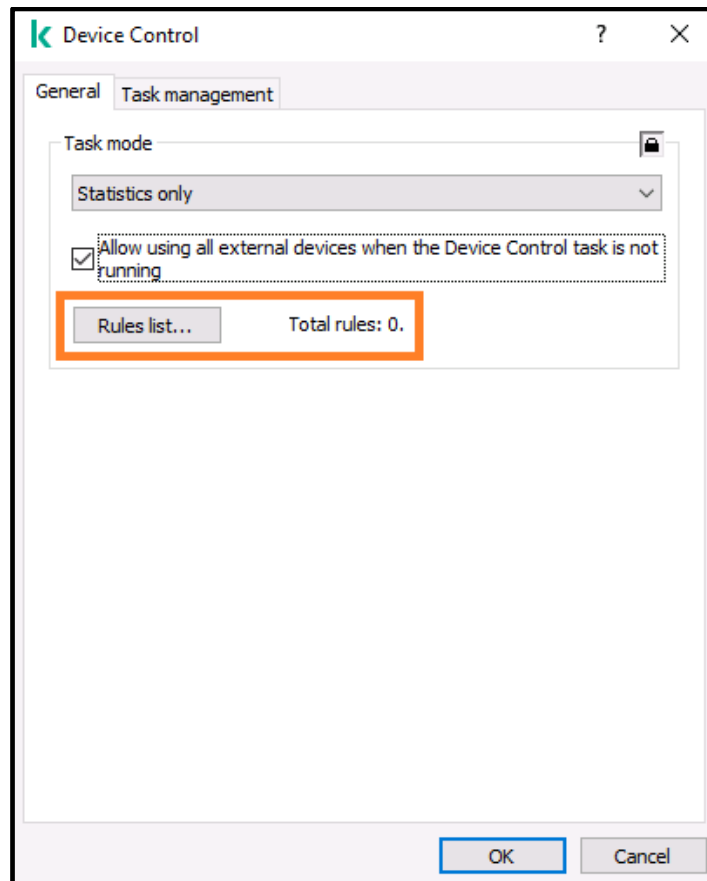
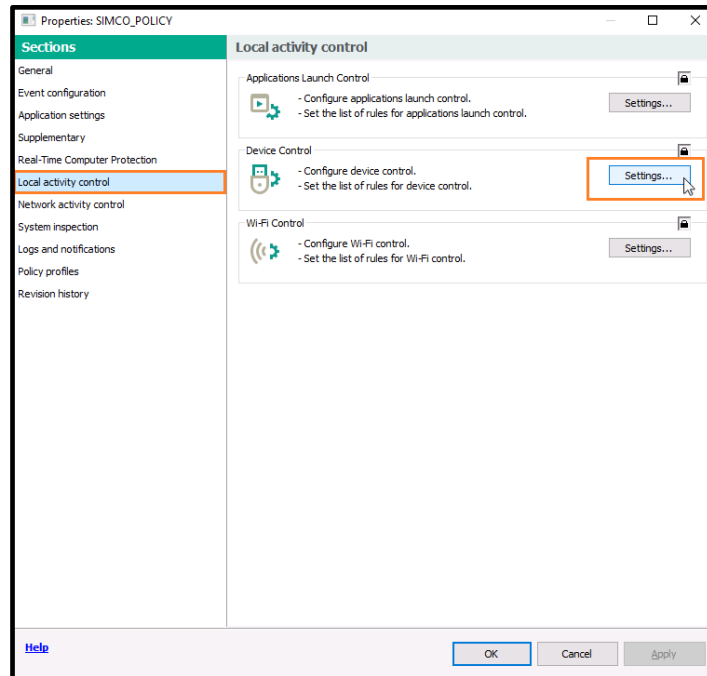
6. In the **Events Export Wizard** that pops up, check **Export selected events only** and specify the destination file you want to export data to. Click **Next**.



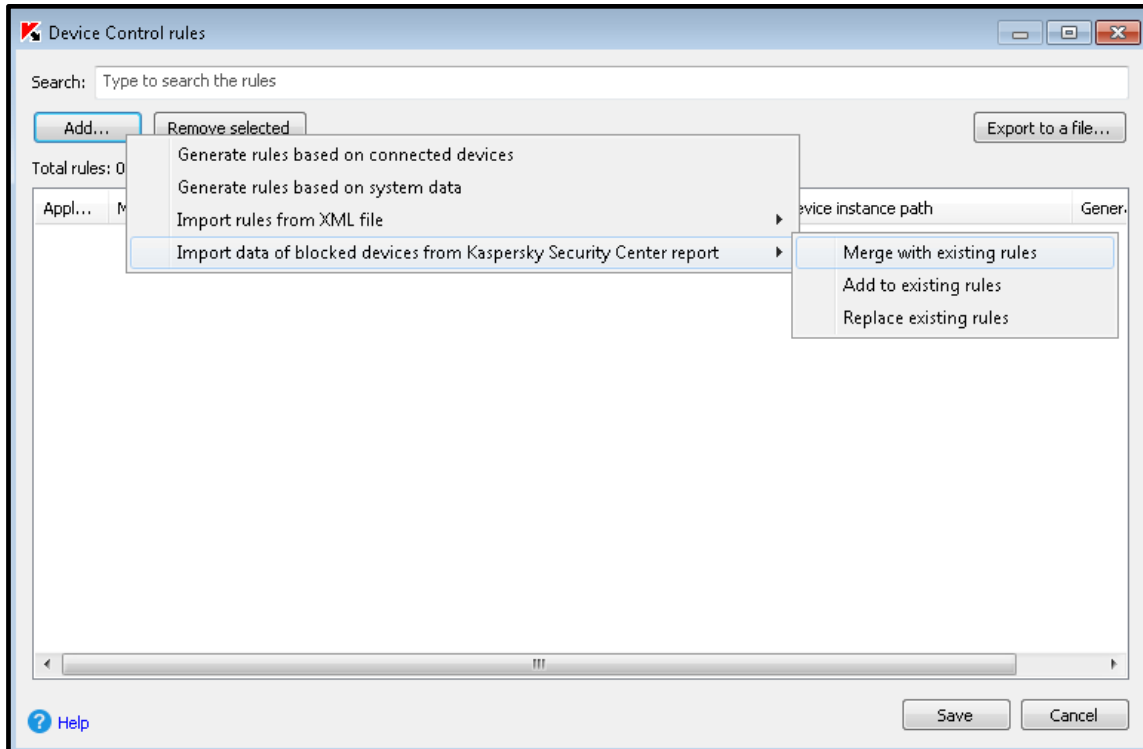
7. Specify the export format as shown below. Click **Next**.



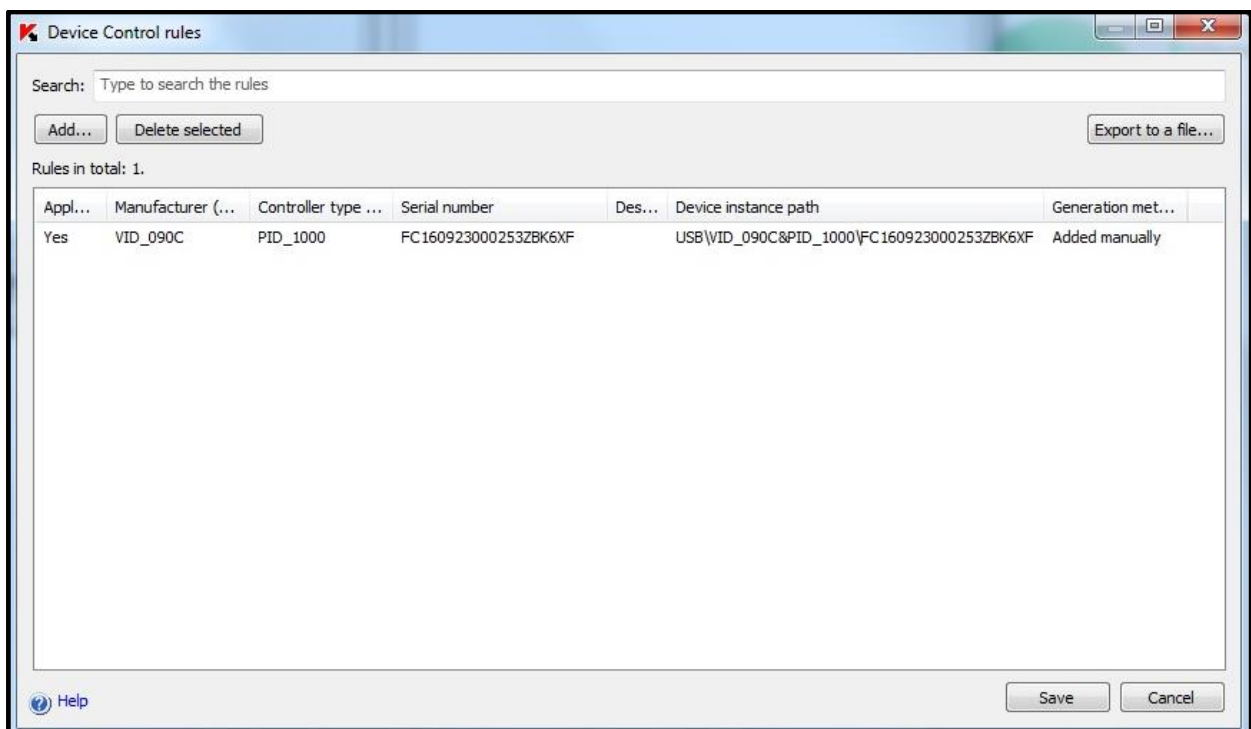
8. Now revert to the recently created **KICS for Nodes** policy and enter its **Properties** again.
9. Proceed to **Local activity control->Device Control**. Click the **Settings...** button. In the popup window, click **Rules list...**



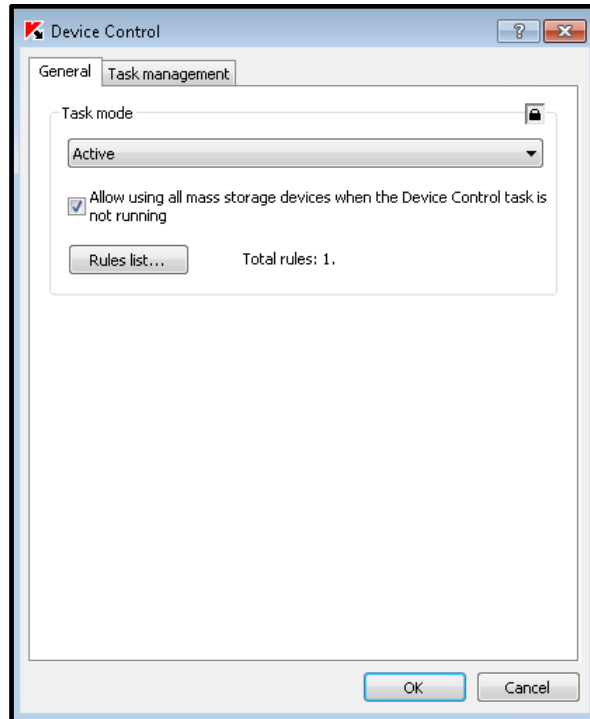
- In the **Device Control rules** window, click the **Add...** button and select **Import data of blocked devices from Kaspersky Security Center report->Merge with existing rules**.



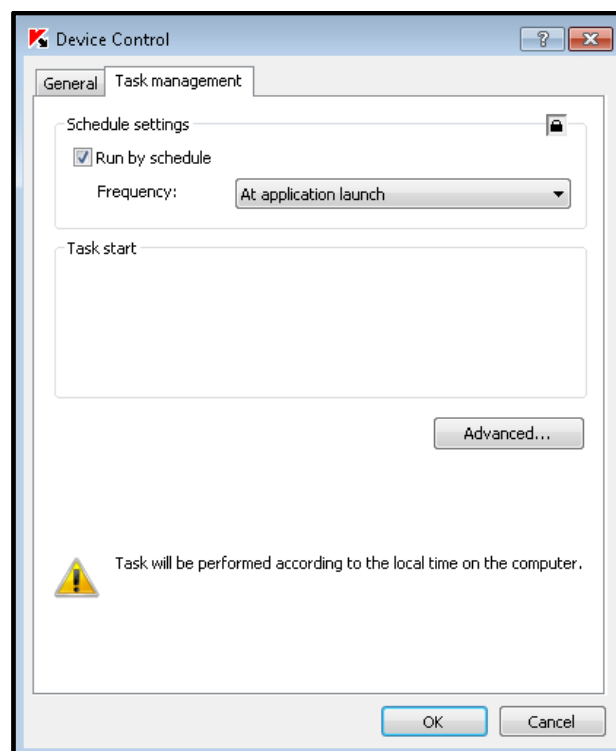
- Using the file browser window, find the recently created file containing the blocked device information. In our example, it is **BlockedUSB.txt**. As a result, we have got one rule added to the **Device Control** white list as shown below. Click **Save** in the **Device Control rules** window.



12. Now set the **Task mode** to **Active** and click **OK**. From this moment on, any unknown USB thumb drive or other storage device will be rejected by **Windows**.



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.



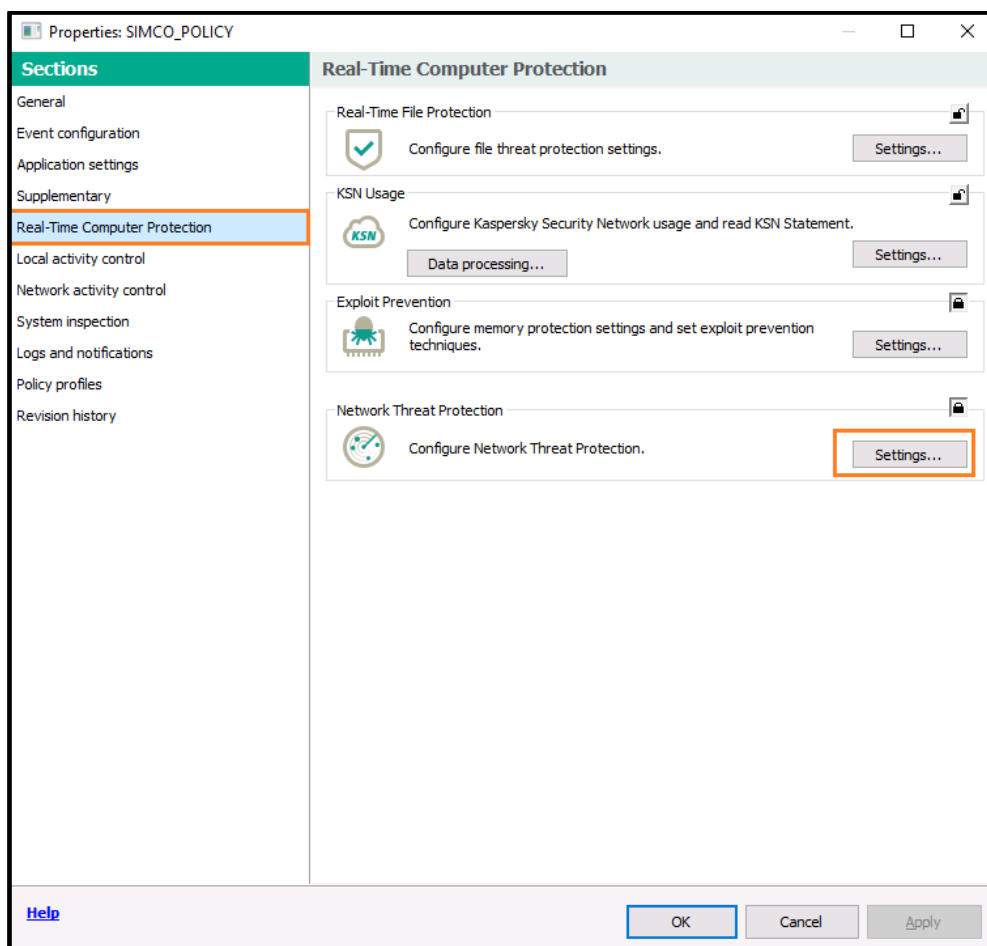
- Click **Apply** and **OK** in the policy **Properties** window. Wait until the policy enforcement finishes.

Setting up Network Threat Protection

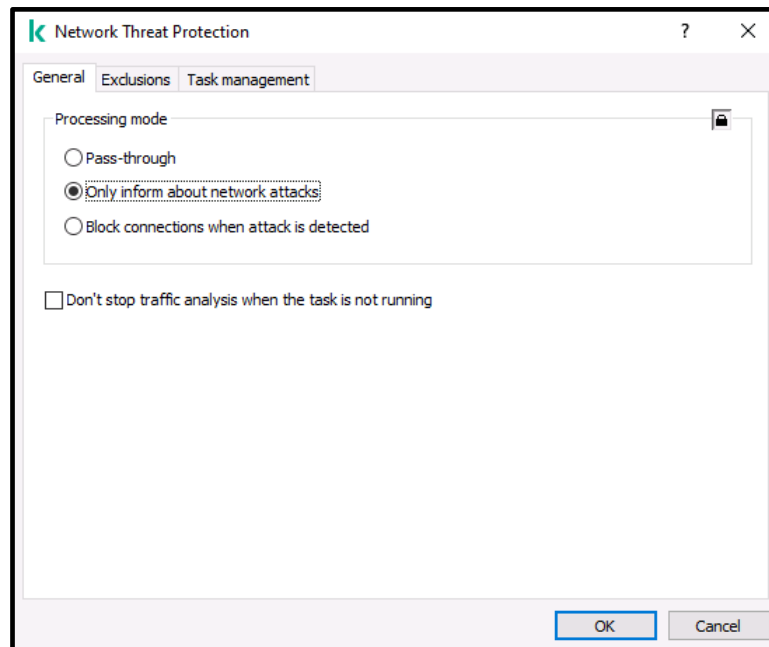
This protection module functions pretty much like a host-based IDS/IPS. Its operation is based on network intrusion signatures (patterns of malicious network activity) developed by **Kaspersky** experts. The signatures are updated along with the virus definitions every time you launch the **Database Update** task (please refer to the section “Initial update of antivirus databases”).

In fact, we have already taken a glance at some of this module settings, but there is still one minor improvement left to be made:

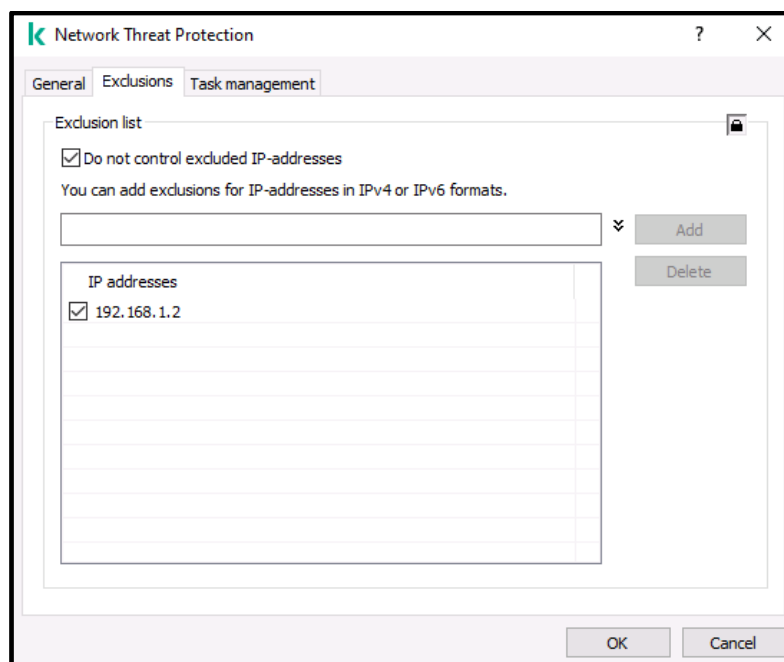
- Revert to the recently created **KICS for Nodes** policy and enter its **Properties** again.
- Proceed to **Real-Time Computer Protection->Network Threat Protection**. Click the **Settings...** button.



3. In the **General** tab we can see that the **Network Threat Protection** is set up to work in the passive mode, which seems a reasonable and fairly safe option for most of the critical sites. However, you are free to change the **processing mode** at your discretion taking in account all the risks.



4. Move over to the **Exclusion** tab. Here we suggest that you add every PLC available on you control network to the trust-list. The point is that you would rather be attacked from a compromised workstation/server than have your PLC involved in spreading the threat. Anyway, despite the fact that false alerts are extremely rare in this protection module, such a configuration further reduces the risk of them. As you can see, in our study case we have just one PLC (**192.168.1.2**) on our industrial network, so we put it on the exclusion list.



5. Click **OK** to finalize the module configuration.
6. Once you have returned to the **policy properties** window, click **Apply** and then **OK** for the changes to take effect.

Setting up File Integrity Monitor

In most cases, it is necessary to adapt the configuration of the **File Integrity 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. Remember to activate **File Integrity Monitor** by going to the task management tab (as we did before).

Please refer to the “**KICS for Nodes 3.0 Administrator’s Guide**” for details.

Setting up PLC Integrity Checker

PLC Integrity Checker controls the integrity of a 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) or Modicon M340/580 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.

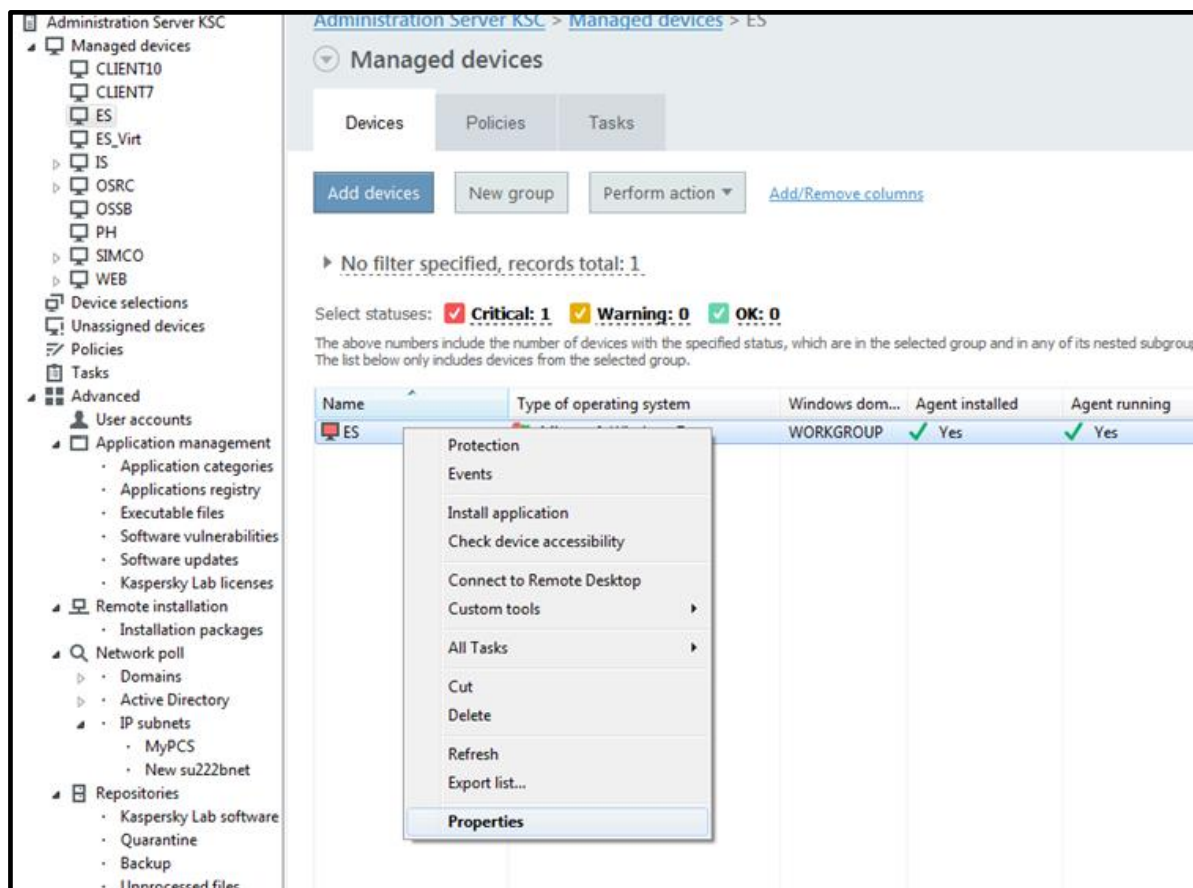
PLC Integrity Checker is not customized by means of security policies. Its configuration is carried out by parametrizing respective tasks.

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

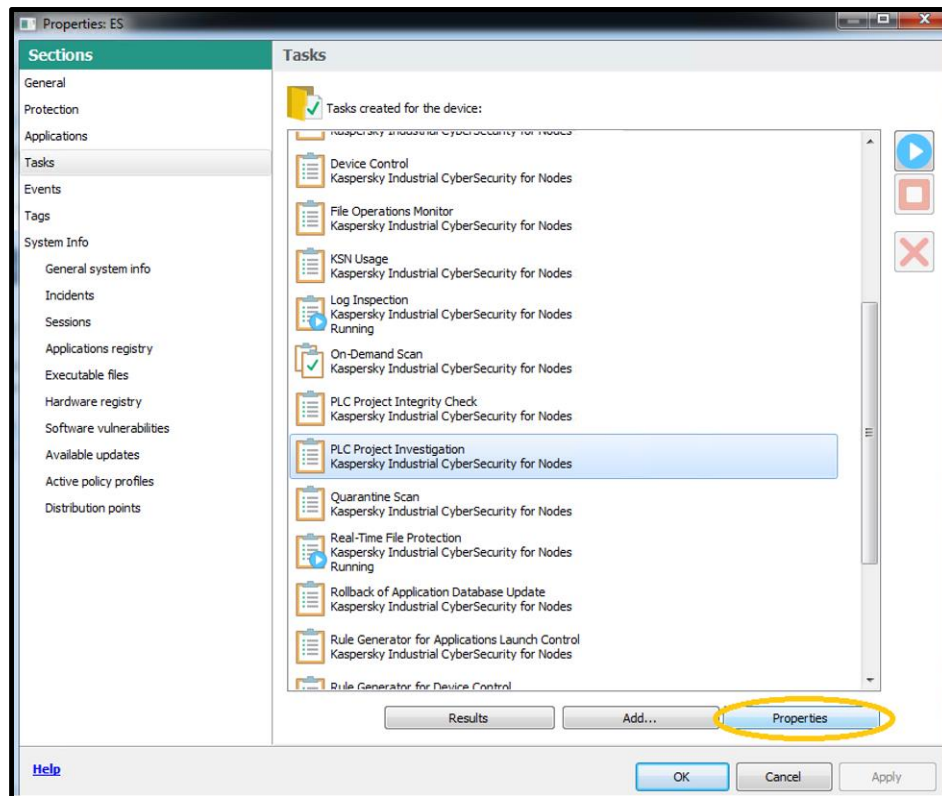
In this guide we will show you how to work with a Siemens S7-400 series PLC. For the other PLC models please refer to “**KICS for Nodes 3.0 Administrator’s Guide**”.

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

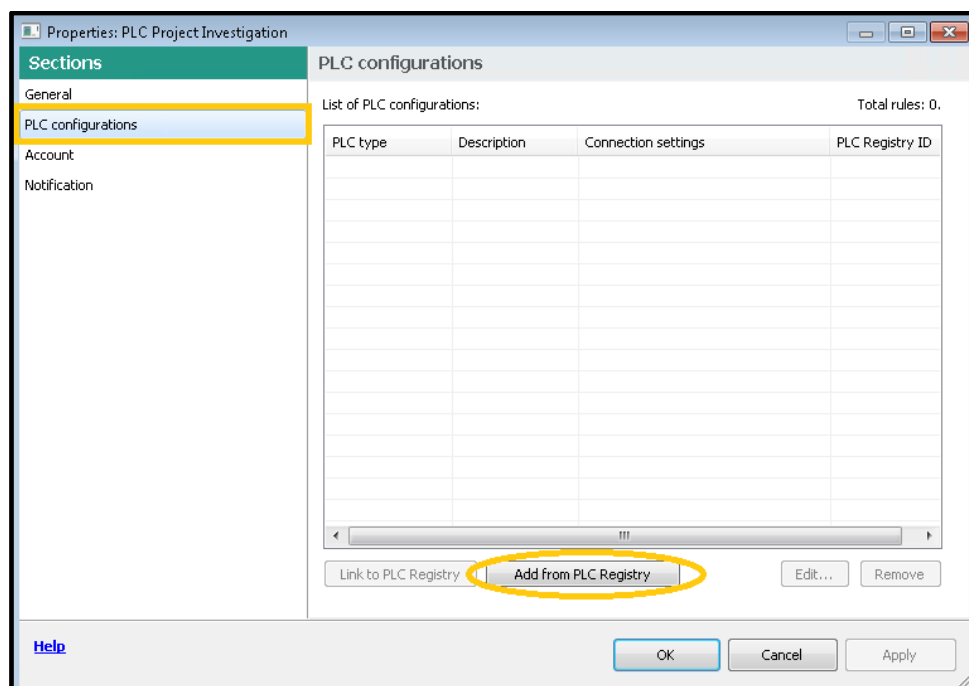
1. Go to **Administration Server->Managed devices->ES** and switch to the **Devices** tab. Right click on **ES** and select **Properties**.



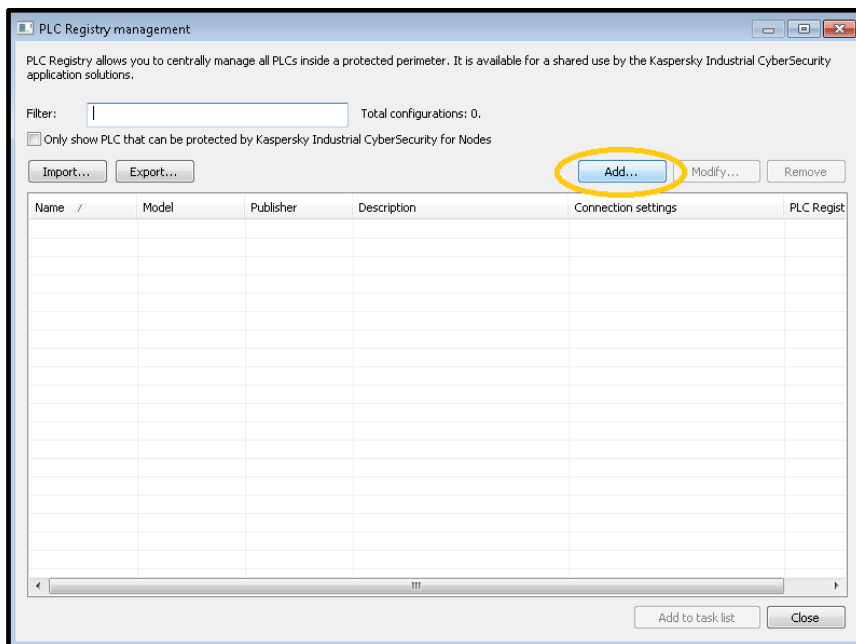
- In the **Properties** window that pops up, go to **Tasks**. Keep scrolling down the **Tasks** list until you find the **PLC Project Investigation** task; select the task and click the **Properties** button. This task is used to form or update a reference control logic snapshot (a sort of an etalon).



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

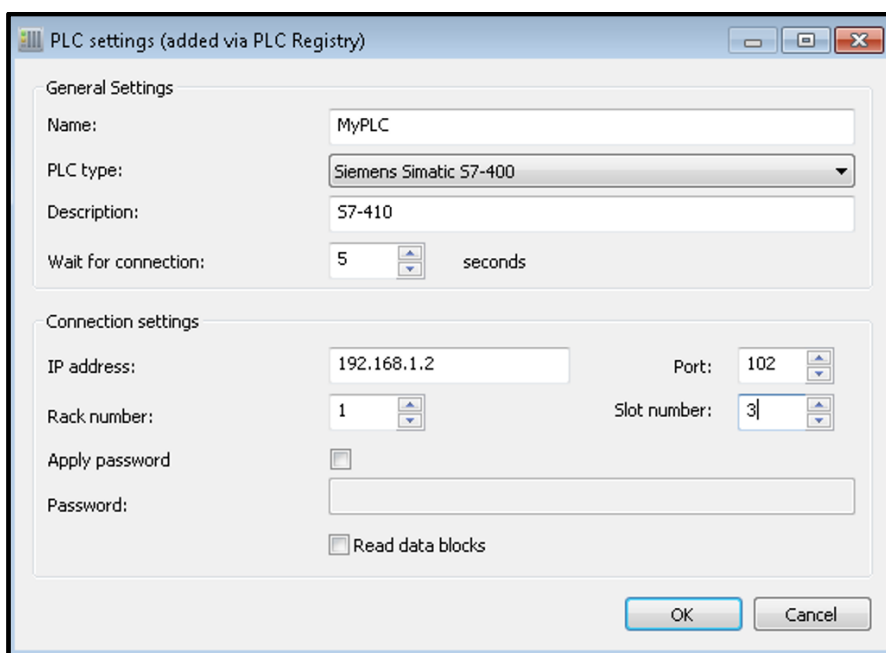


- Now we have to add a monitored PLC to the **PLC Registry**. Press the **Add...** button.

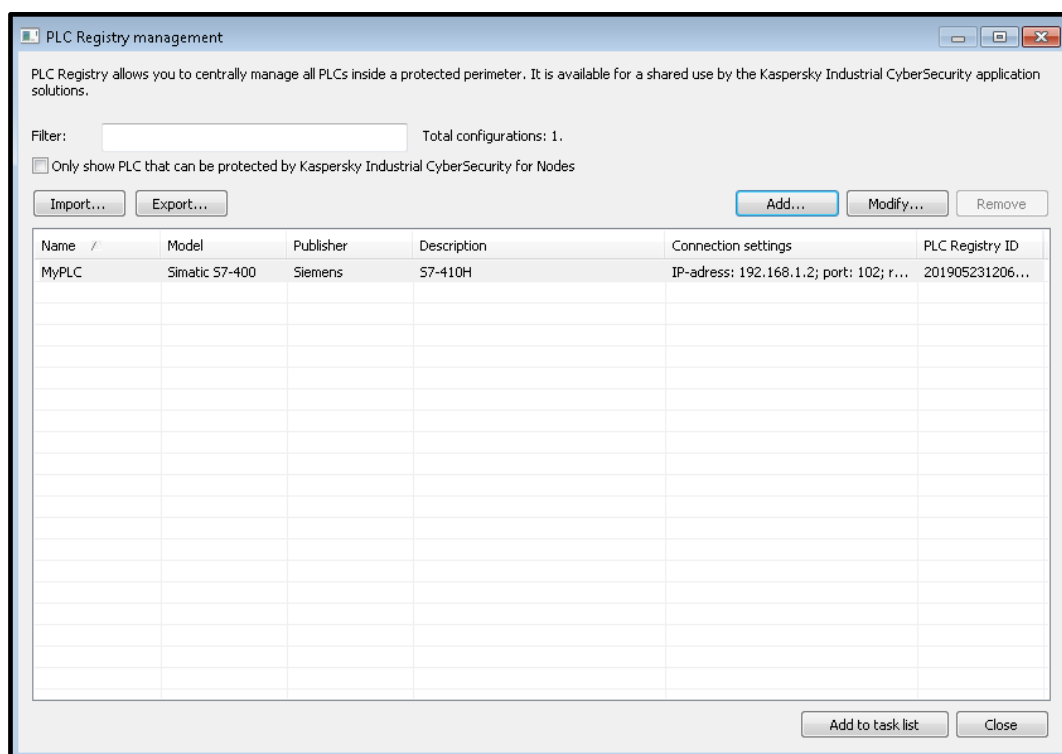


- In the **PLC settings** window that pops up, choose an appropriate **PLC type**, assign an arbitrary name (description) of the PLC and specify the device **IP address**. Among other parameters, you should specify the **Rack number**, **Port** and **Slot number** values depending on your **PLC type** 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** stuff, the MASTER CPU normally has **Rack number=0**, **Port=102**, **Slot number=3**, whereas the STANDBY CPU has **Rack number=1**, **Port=102**, **Slot number=3**.

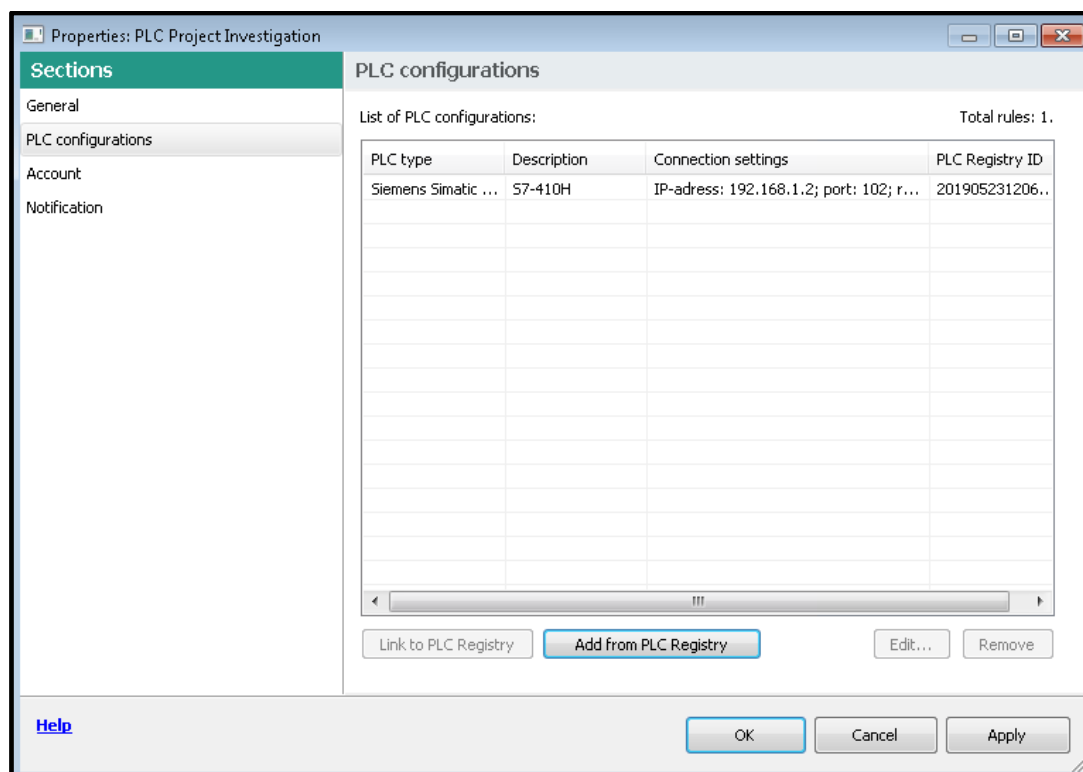
In our example, we have chosen to poll the **S7-400** CPU available at **192.168.1.2**. Click **OK** when done.




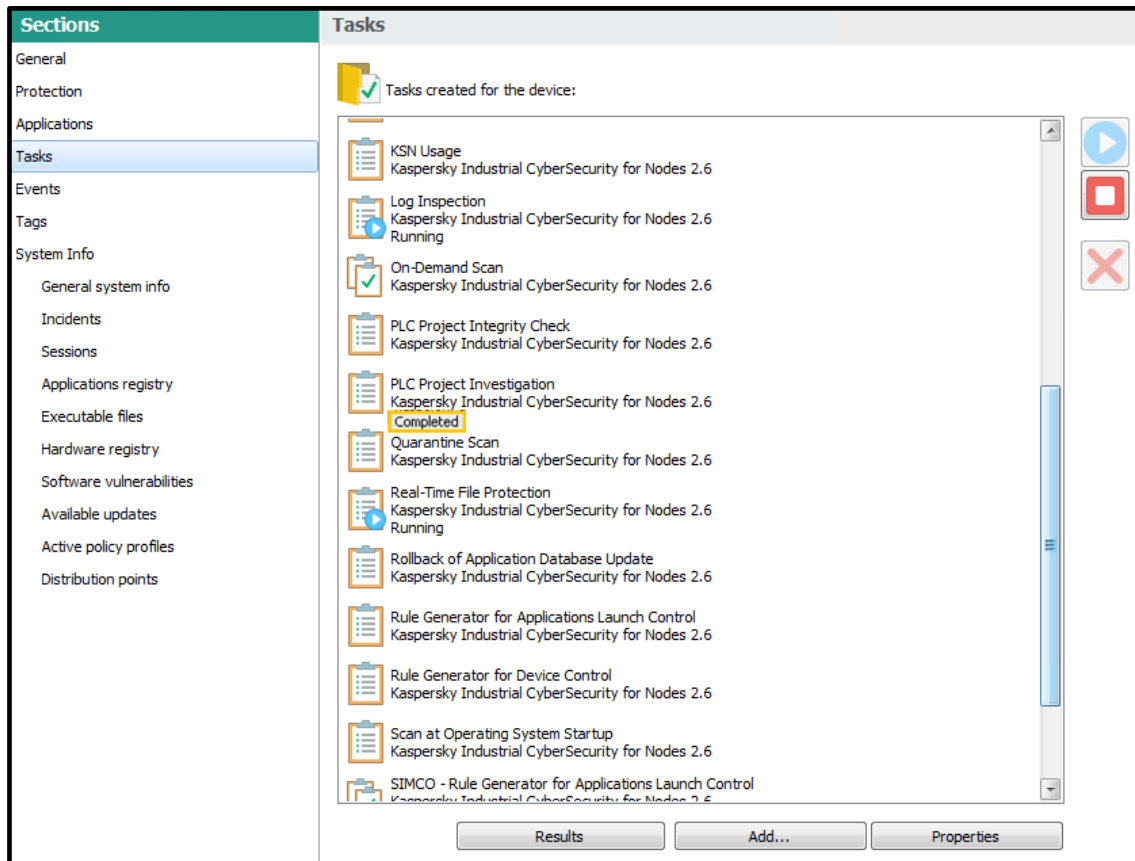
- In the parent window you should now see the just added PLC (as shown below). Revise the PLC configuration by expanding the **Connection settings** column and click **Add to task list** if everything is correct. Click **Close** to hide the window.



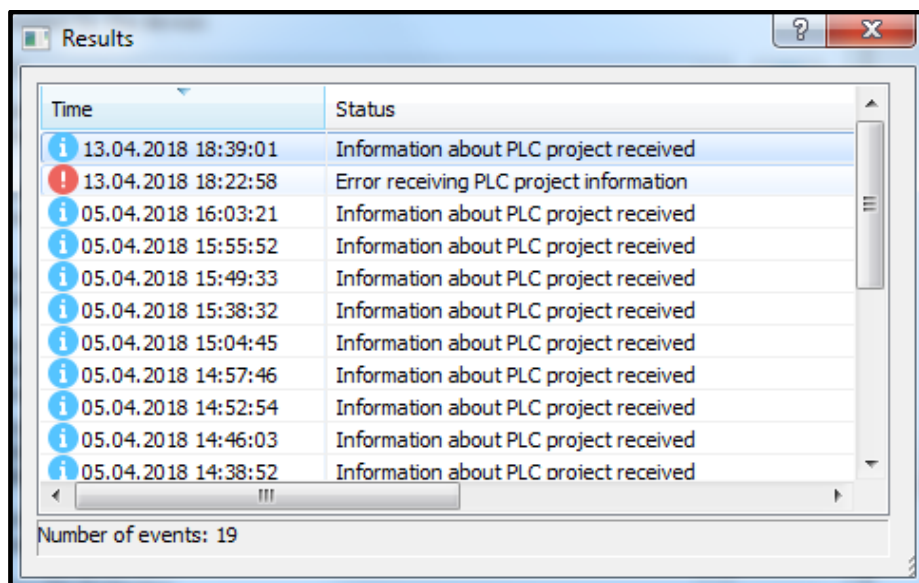
- Click **OK** in the parent window to finalize the task parametrization.



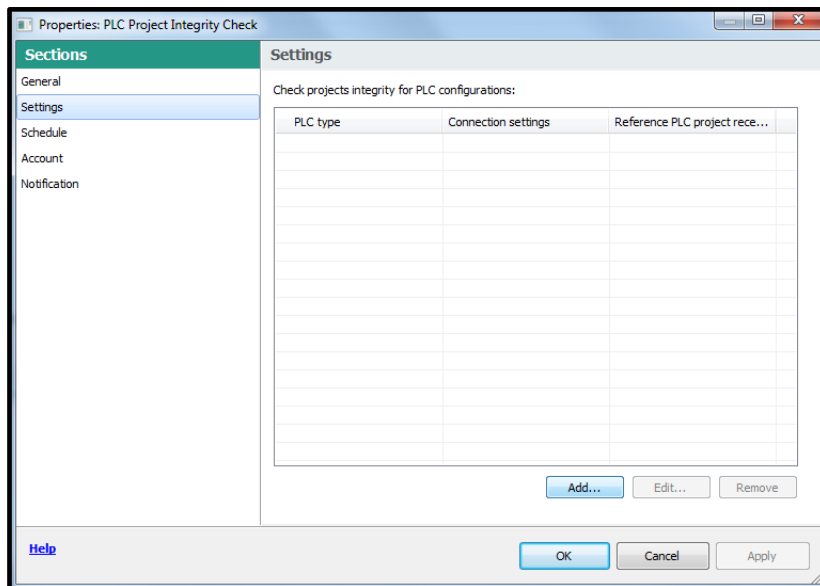
8. Select the just configured **PLC Project Investigation** task and start it by pressing . Wait until the task is displayed as **Completed**.



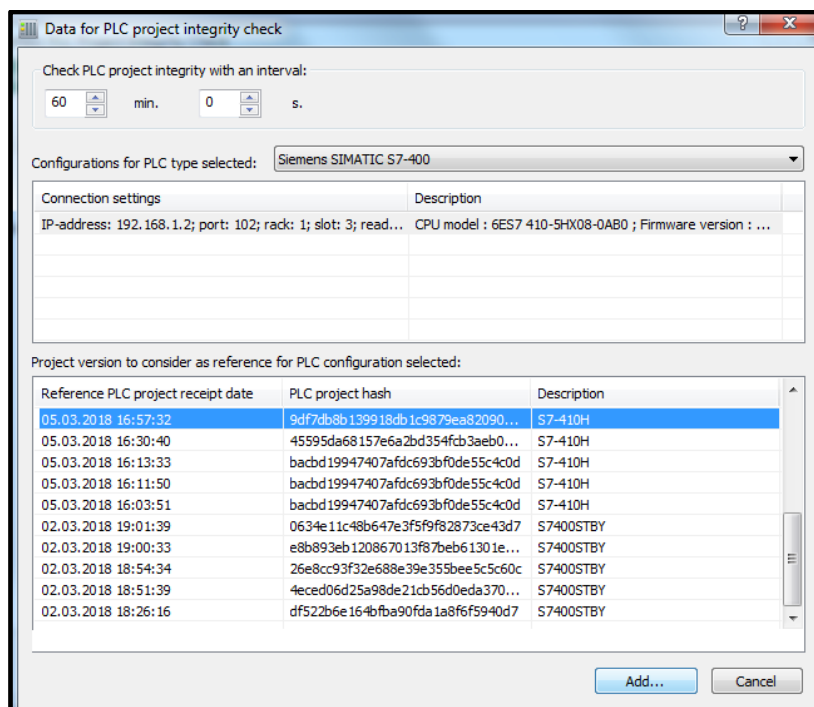
9. In order to make sure that the reference control logic has been successfully retrieved from the PLC, click the **Properties** button. Make sure that in the popup window the most recent status is displayed as **Information about PLC project received**. Close the popup window.



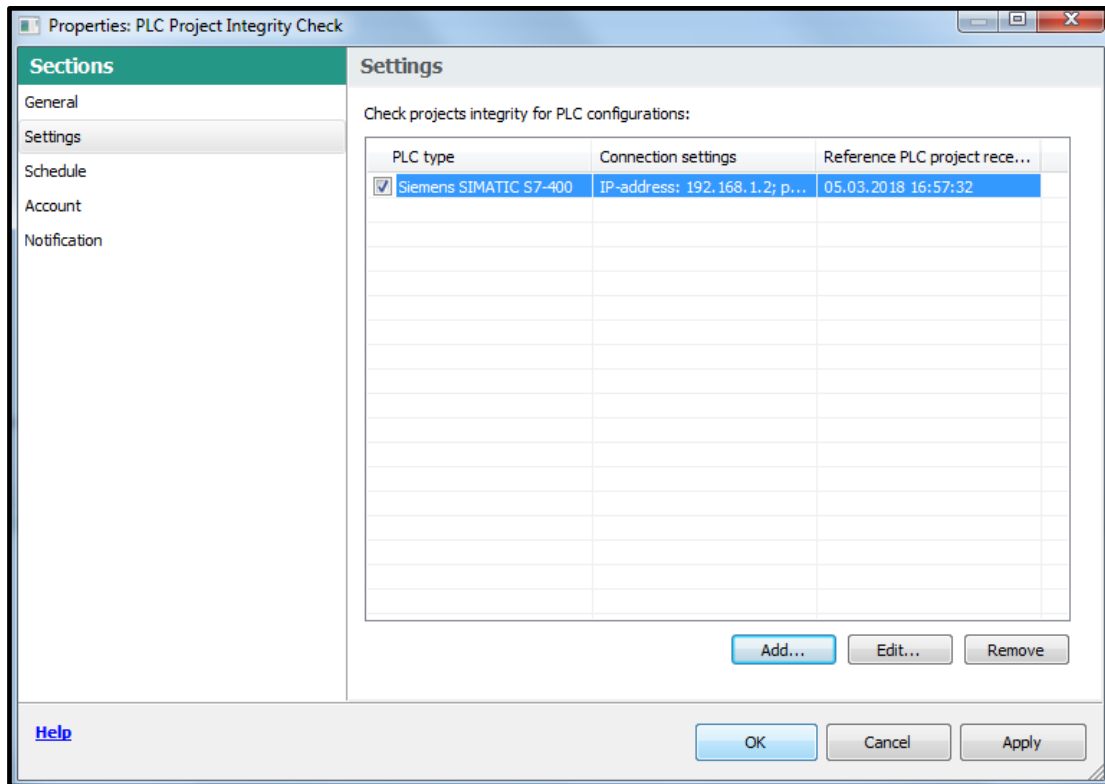
10. Now, wait a little bit until the inter-task synchronization is completed. It takes 15 minutes or so.
11. Select the **PLC Project Integrity Check** task and press the **Properties** button.
12. In the window that appears, go to **Settings**. Click the **Add...** button.



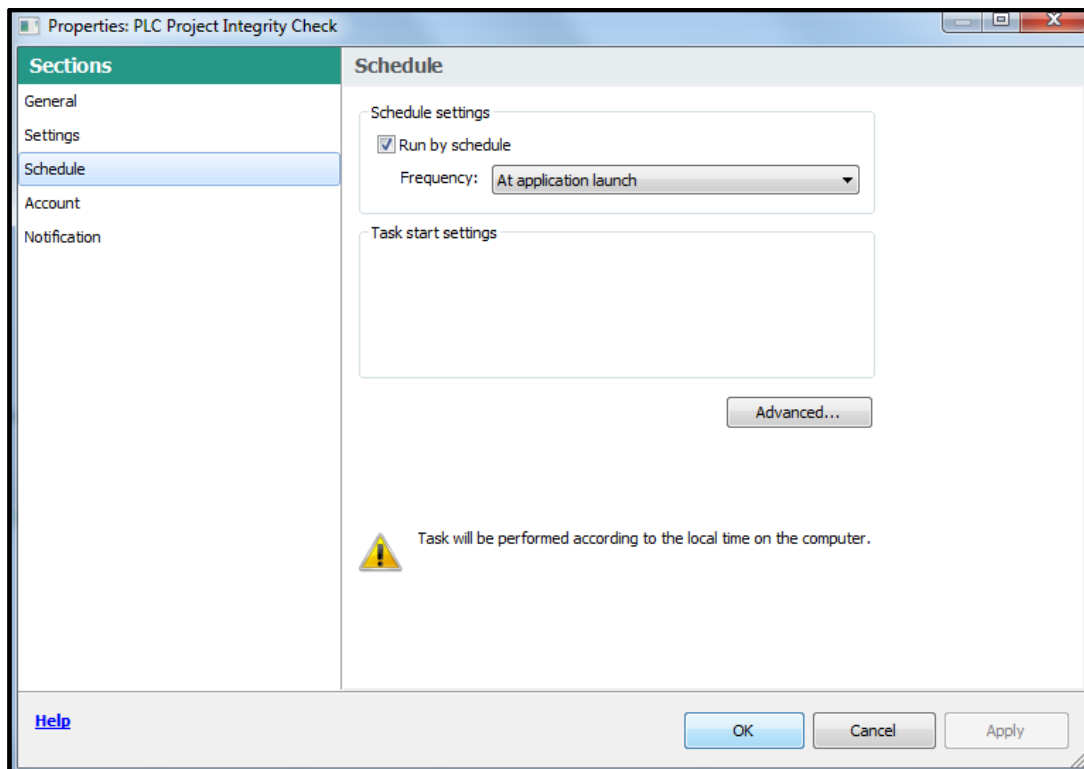
13. In the window that appears, select the **PLC type** and choose the most recent **PLC project snapshot (hash)** which the **PLC Project Investigation** task has previously generated. The selected hash will be a basis for comparing with subsequent PLC polls. Also specify a polling interval, which, according to our estimations, should exceed 30 minutes. It is important to 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.



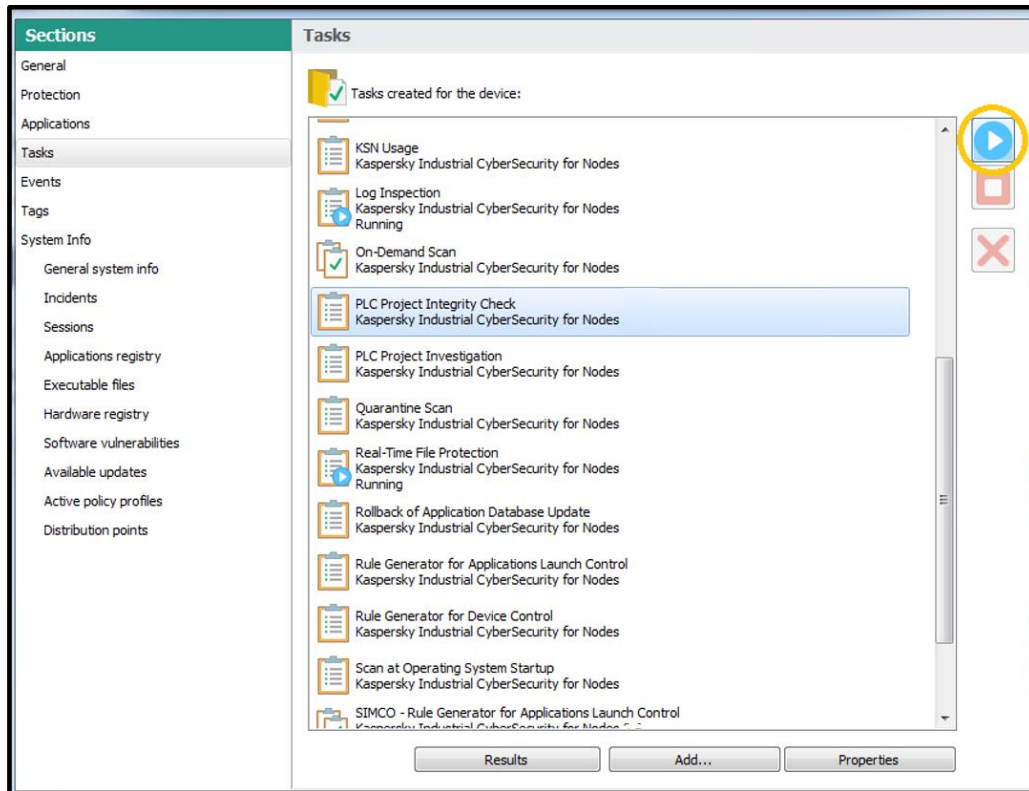
14. In the parent window, check the just added reference project as shown below and proceed to **Schedule**.



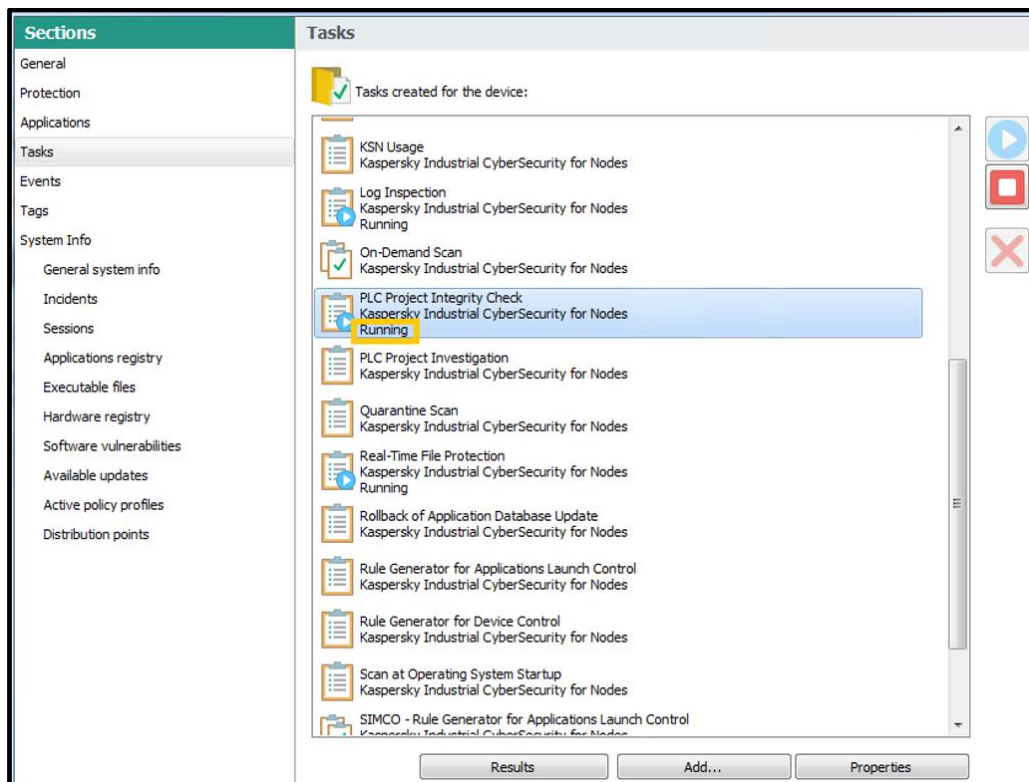
15. In **Schedule** specify the task **Schedule** settings as shown below. Click **OK** to finalize the task parametrization.



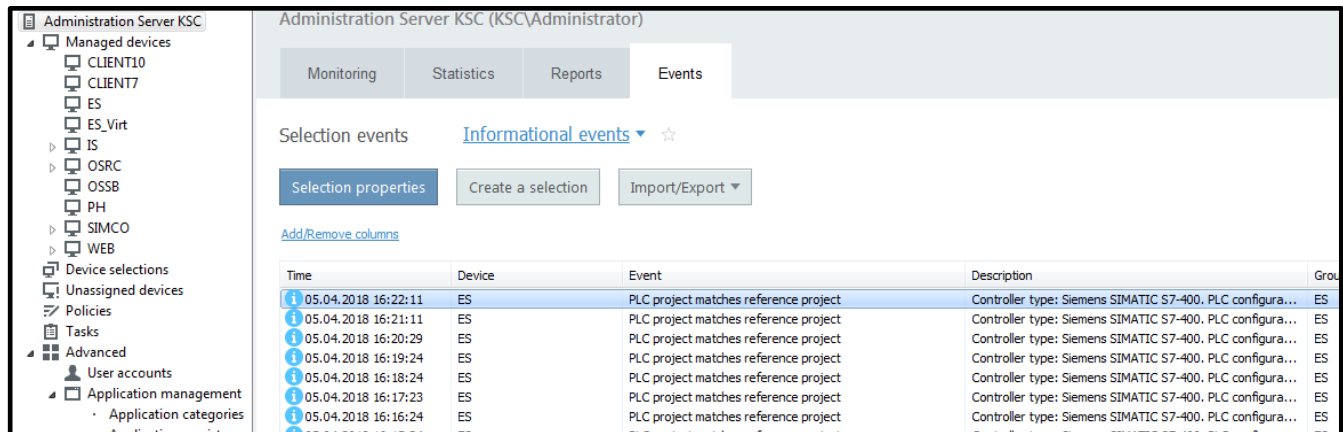
16. Select the **PLC Project Integrity Check** task and click  in order to start it.



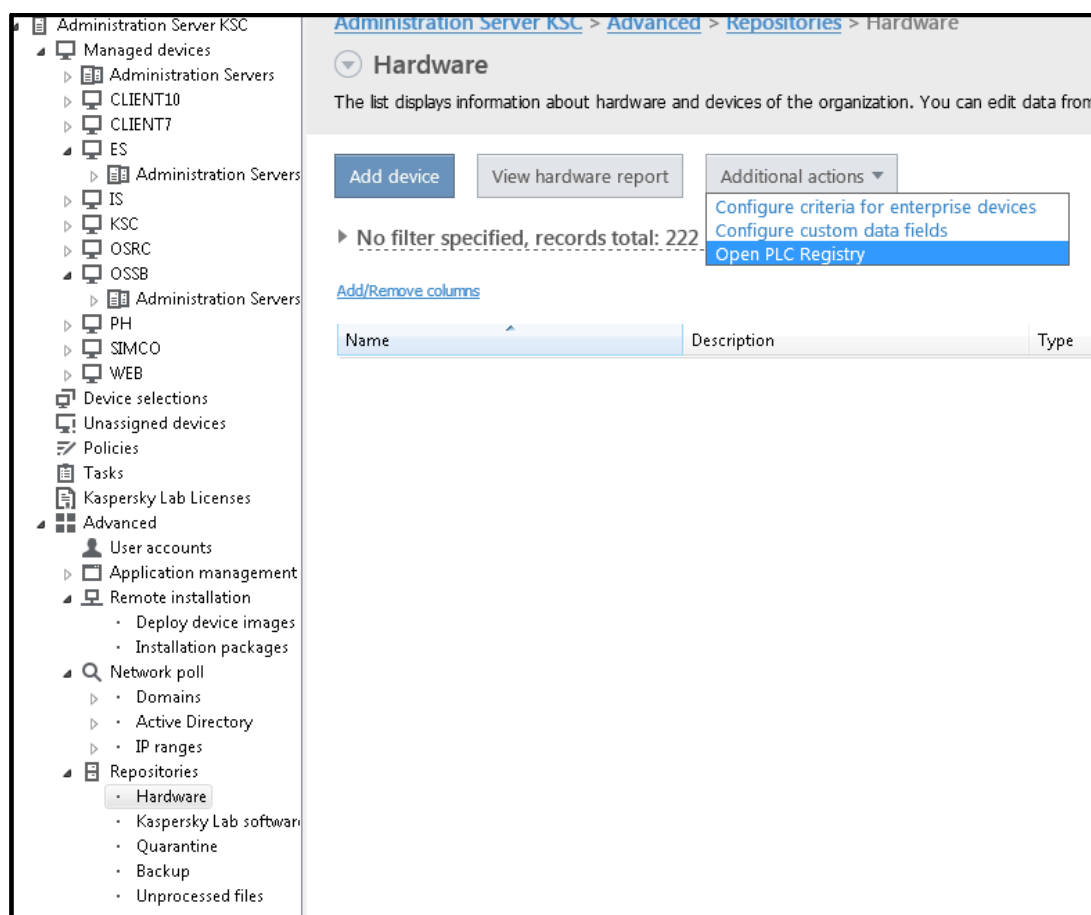
17. Make sure that the task status is now displayed as **Running**. Click **OK** to exit the **ES Properties** window.



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



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



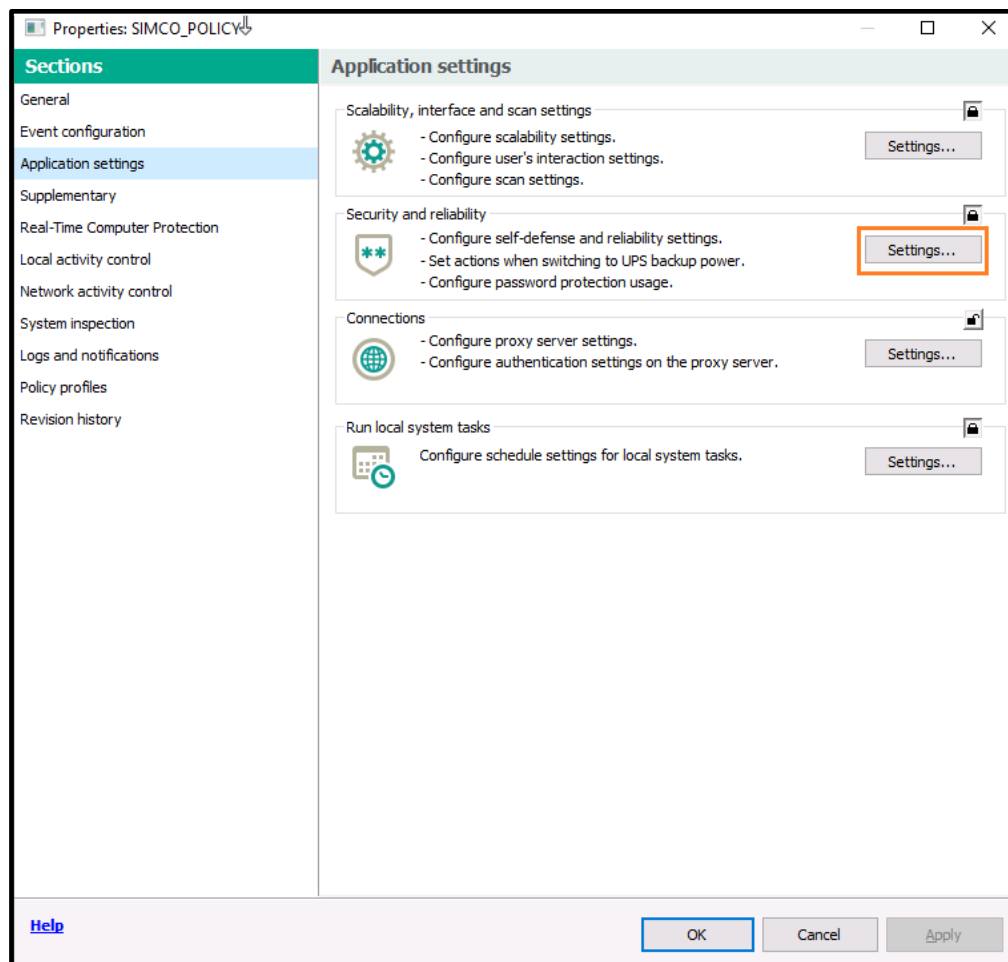
This section completes the **KICS for Nodes** parametrization for a single host. In case of multiple hosts, you should act in absolutely the same manner, making use of the already defined group policies and group tasks.

Enabling optional password protection

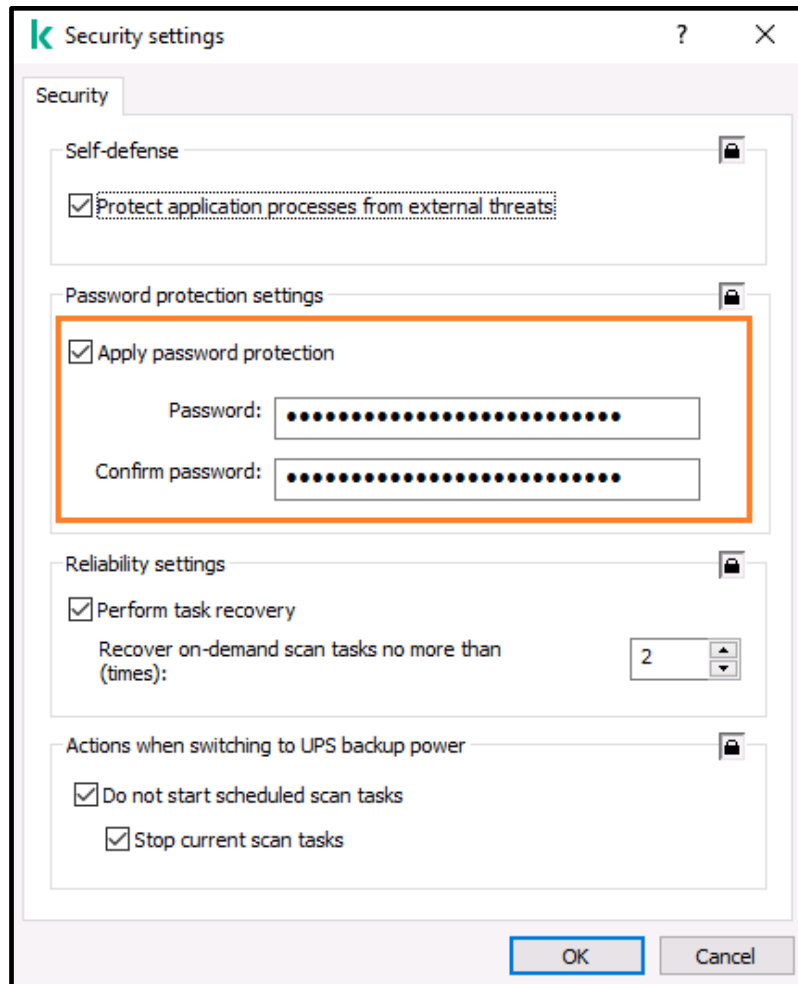
By default, any local user having administrative privileges is allowed to uninstall or modify **KICS for Nodes** even without asking **KSC** permission. Such users can also launch the **KICS for Nodes management console** locally (providing that it is installed) and manipulate with the protection settings at their discretion (unless these settings are overridden and locked by the **KSC** policy). In order to prevent tampering the endpoint security, you can additionally 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.

From now on, any **KICS for Nodes** removal/modification attempt, made by a local user on a local machine, will prompt him/her to enter the protection password. Opening **KICS for Nodes management console** locally (providing that it is installed) will also require entering the valid password.

Installing optional KICS for Nodes management console

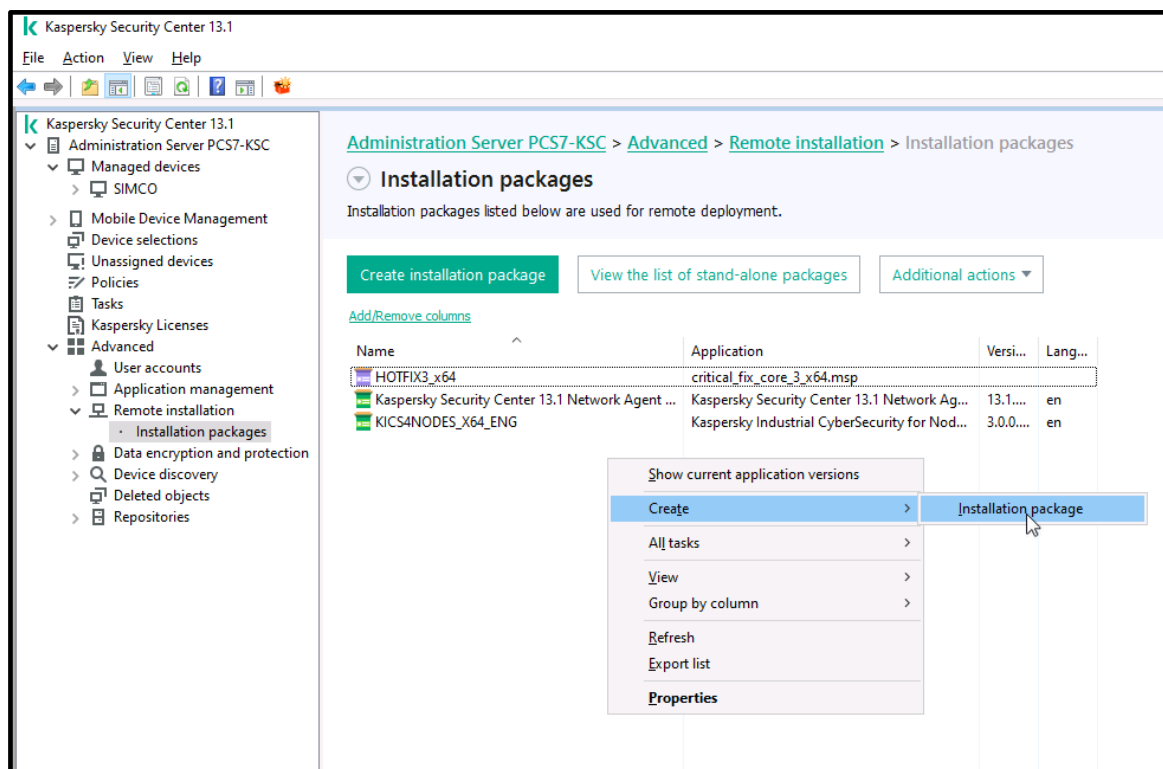
This console enables local management of a **KICS for Nodes** instance. For a few-node or stand-alone installation it could be a good alternative to using **KSC**. We do not mind you using both the tools, of course.

For security purposes, local management capabilities can be centrally restricted by activating corresponding feature locks  while setting up your **KSC** policy and applying it to a target host. In addition to that, the password protection of the local console can be activated in order to prevent unauthorized local users from manipulating with **KICS for Nodes** settings (please refer to the section “Enabling optional password protection”).

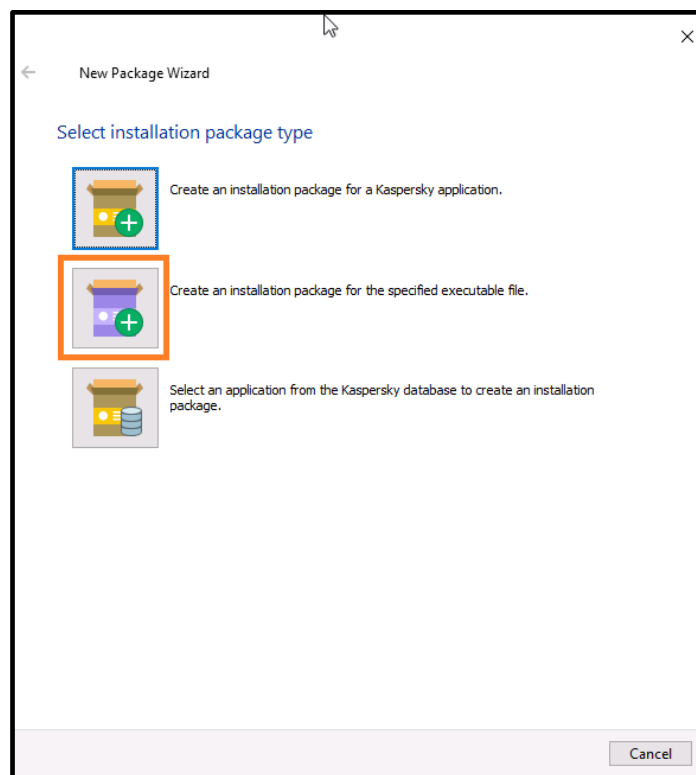
The good thing is that you can install the **KICS for Nodes management console** on one machine and use it to manage a **KICS for Nodes** instance installed on another machine. However, this will require you to open **UDP/TCP 135** ports on both the source and target machines. By default, the console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

In order to install the **KICS for Nodes management console** using **KSC**, please go through the following steps.

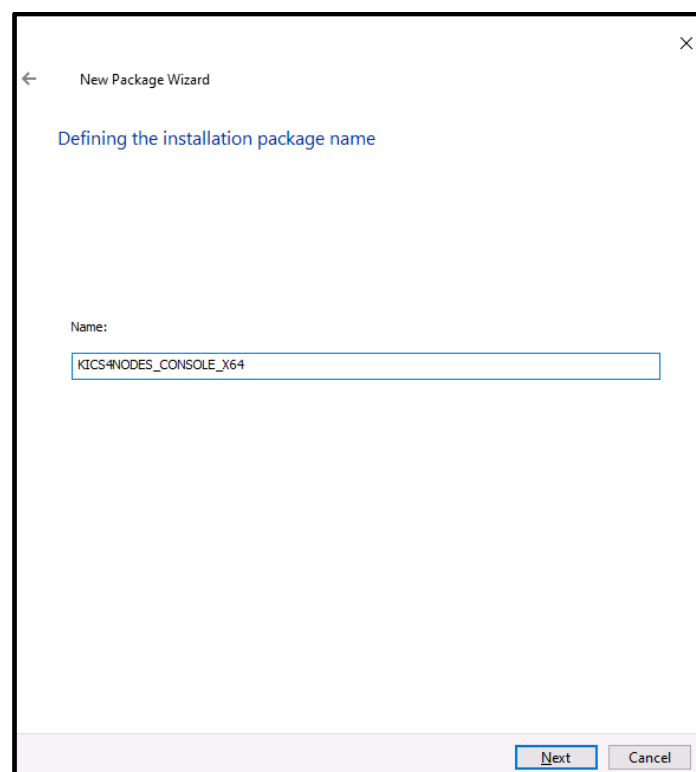
1. Go to **Administration Server->Advanced->Remote Installation**. Right-click on any spare area of the installation packages list. In the context menu choose **Create->Installation package**.



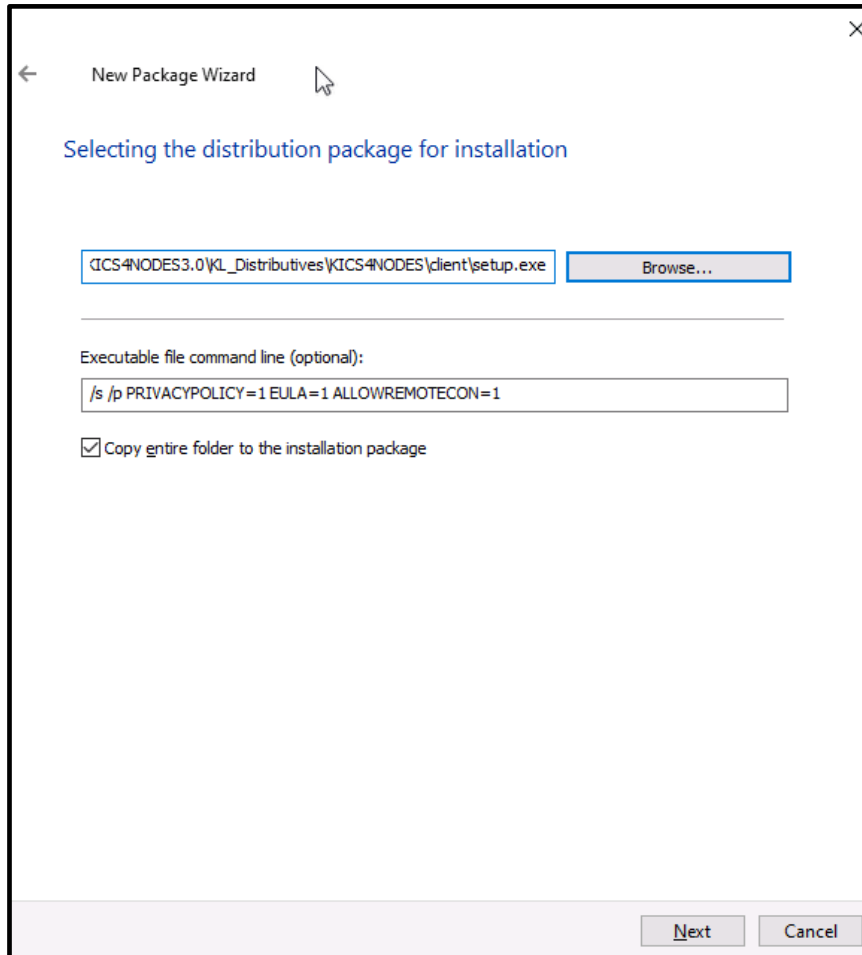
2. In the **Select installation package type** window, click **Create installation package for specified executable file** as shown below.



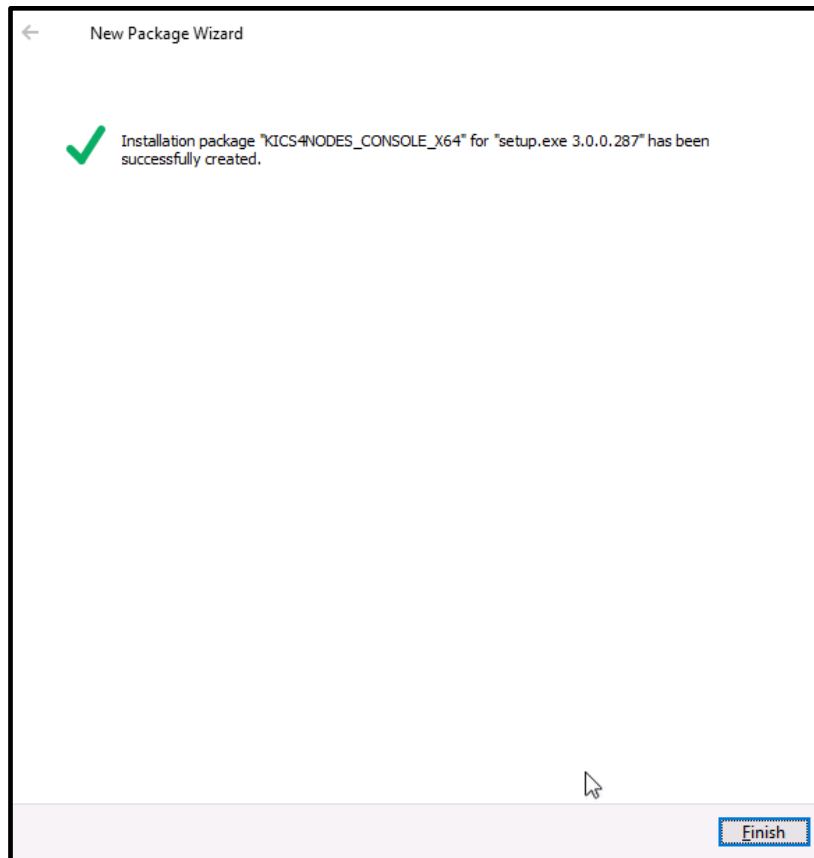
3. Name this new installation package, for example, **KICS4NODES_CONSOLE_X64**. Click **Next**.



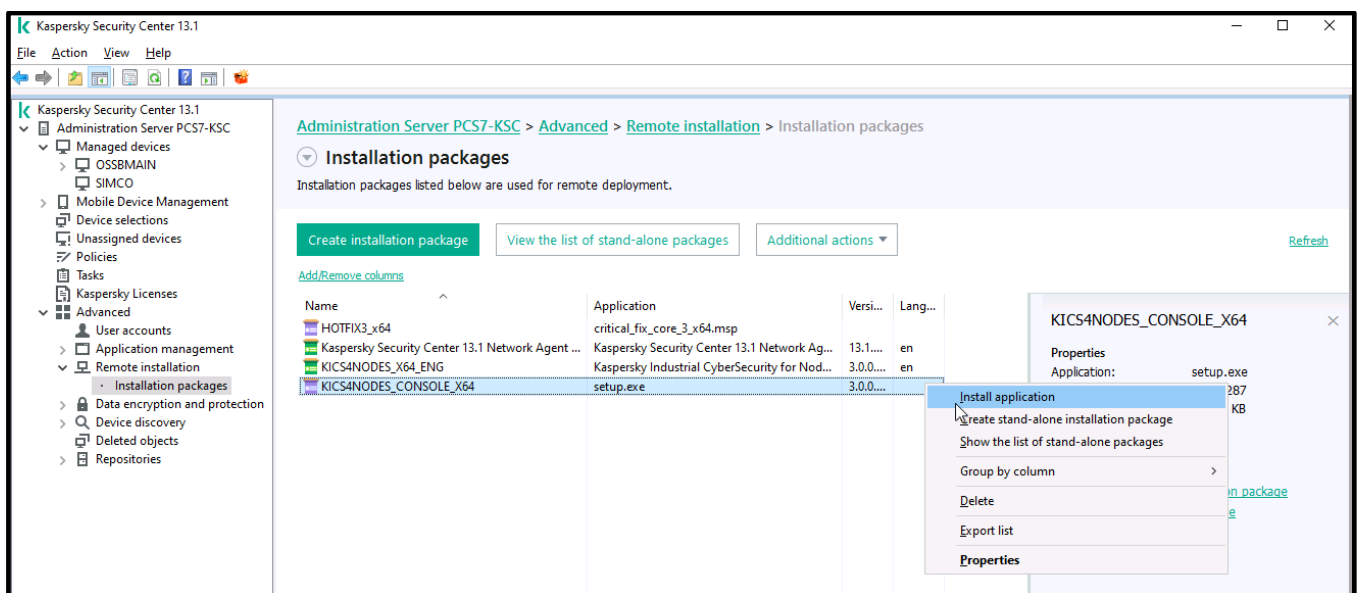
4. In the **Selecting the distribution package for installation** window browse to the **setup.exe** file (located in the subfolder **KICS4NODES\client** of the **KICS for Nodes 3.0** distribution package) and select it. Specify the following command line options: **/s /p PRIVACYPOLICY=1 EULA=1 ALLOWREMOTECON=1 /qn**. Check **Copy entire folder to the installation package**. Click **Next**.



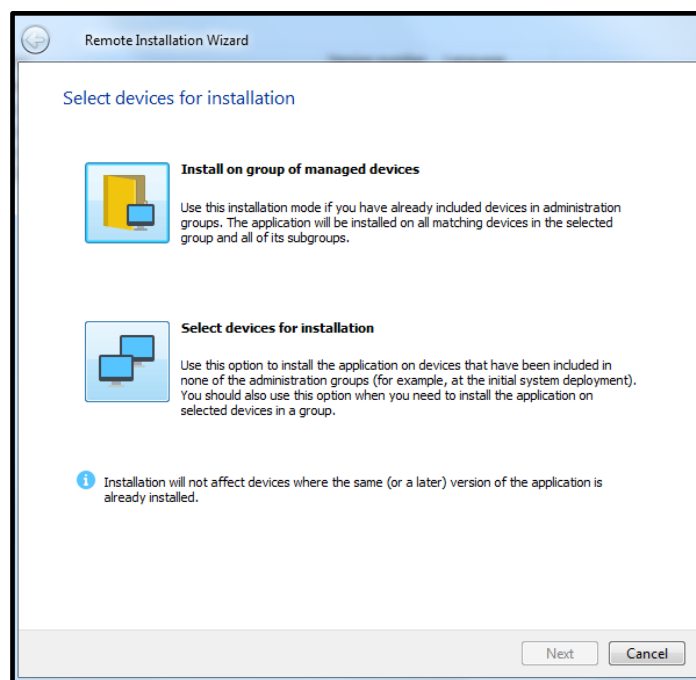
- Click **Finish** to close the **New Package Wizard**.



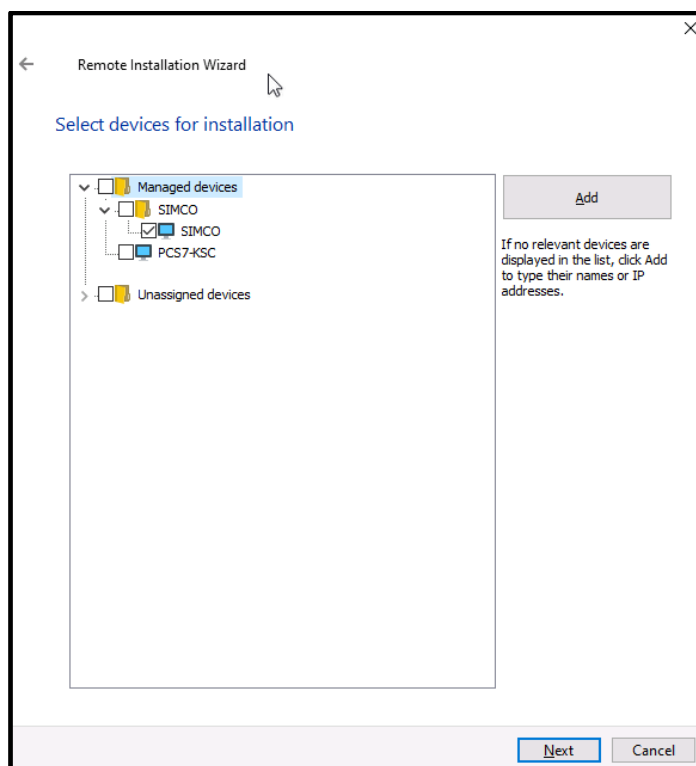
- Select the just created installation package, right-click on it and in the context menu select **Install application** as shown below.



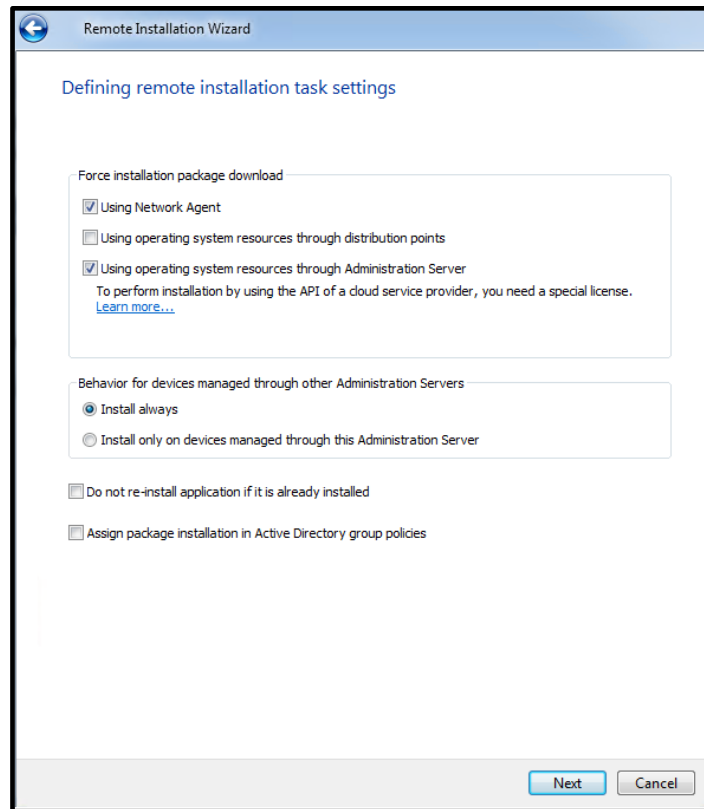
7. In the following window click **Select devices for installation**.



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



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

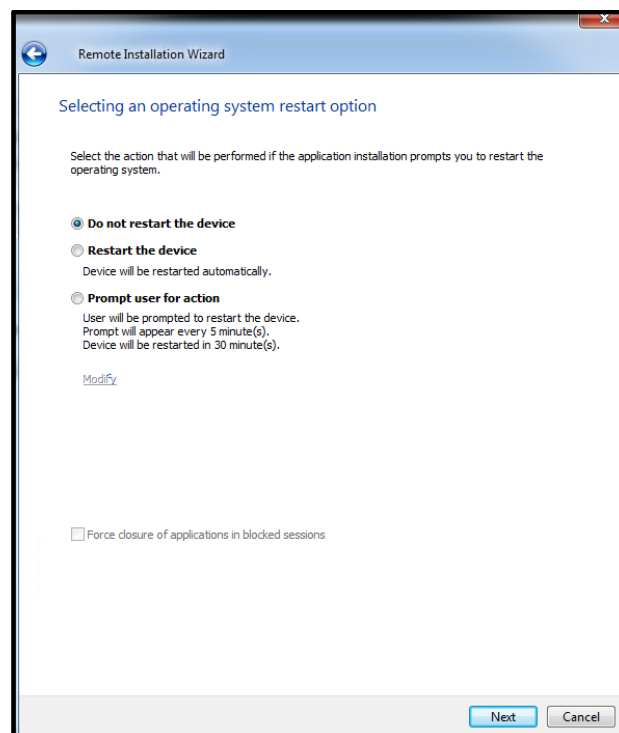


The screenshot shows the 'Remote Installation Wizard' window with the title bar. The main content area is titled 'Defining remote installation task settings'. It contains three sections:

- Force installation package download:**
 - ☒ Using Network Agent
 - ☐ Using operating system resources through distribution points
 - ☒ Using operating system resources through Administration Server
 - To perform installation by using the API of a cloud service provider, you need a special license. [Learn more...](#)
- Behavior for devices managed through other Administration Servers:**
 - ☒ Install always
 - ☐ Install only on devices managed through this Administration Server
- ☐ Do not re-install application if it is already installed
- ☐ Assign package installation in Active Directory group policies

At the bottom right, there are 'Next' and 'Cancel' buttons.

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



The screenshot shows the 'Remote Installation Wizard' window with the title bar. The main content area is titled 'Selecting an operating system restart option'. It contains the following text and options:

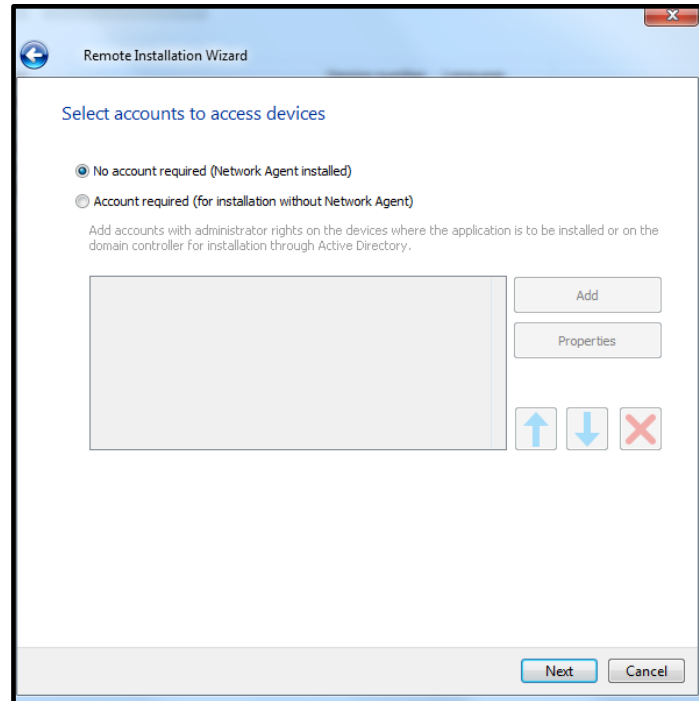
Select the action that will be performed if the application installation prompts you to restart the operating system.

- ☒ **Do not restart the device**
- ☐ **Restart the device**
Device will be restarted automatically.
- ☐ **Prompt user for action**
User will be prompted to restart the device.
Prompt will appear every 5 minute(s).
Device will be restarted in 30 minute(s).
[Modify](#)

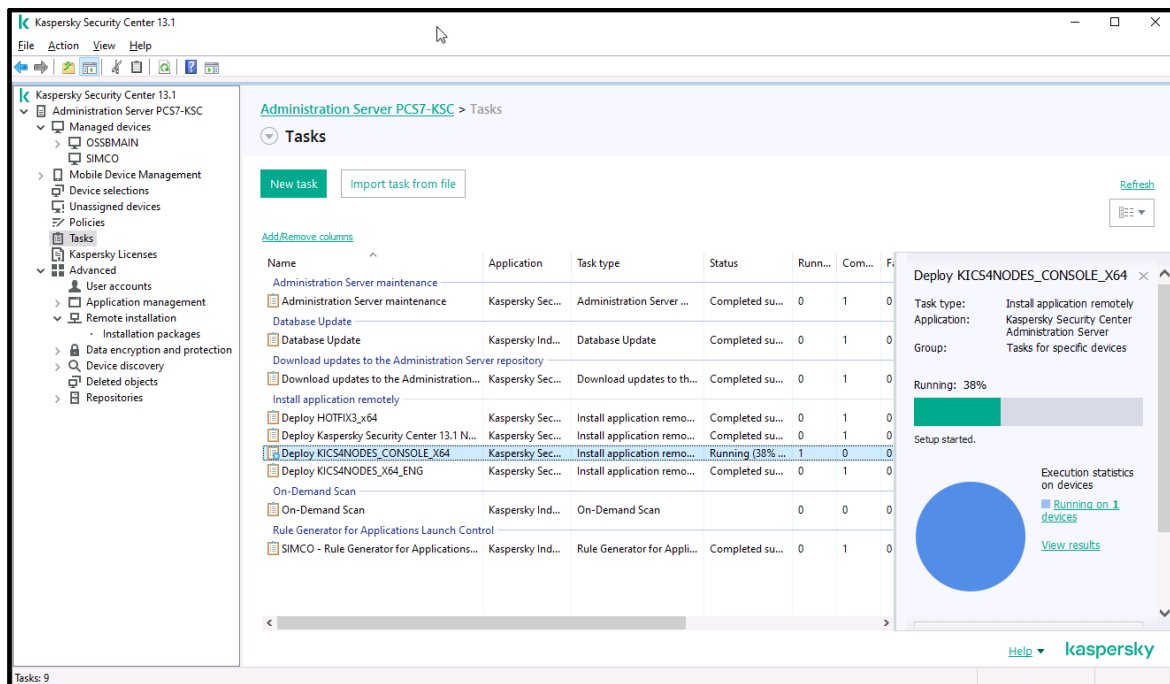
At the bottom, there is an unchecked checkbox: ☐ Force closure of applications in blocked sessions.

At the bottom right, there are 'Next' and 'Cancel' buttons.

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



12. In the **Starting installation** windows that follows, click **Next** and finally **Finish**. So, we have created the task that is about to launch the console installation on the target host.
13. Now you are automatically redirected to the **Administration Server->Tasks** node where you can see the just created task **Deploy KICS4NODES_CONSOLE_X64** running. Wait for its completion.

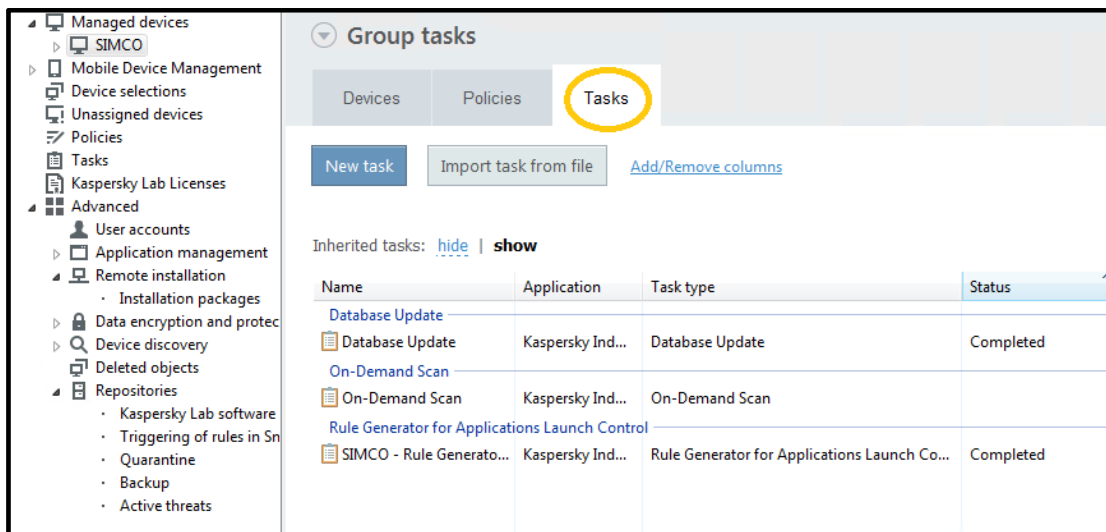


Uninstalling KICS for Nodes and KLnagent

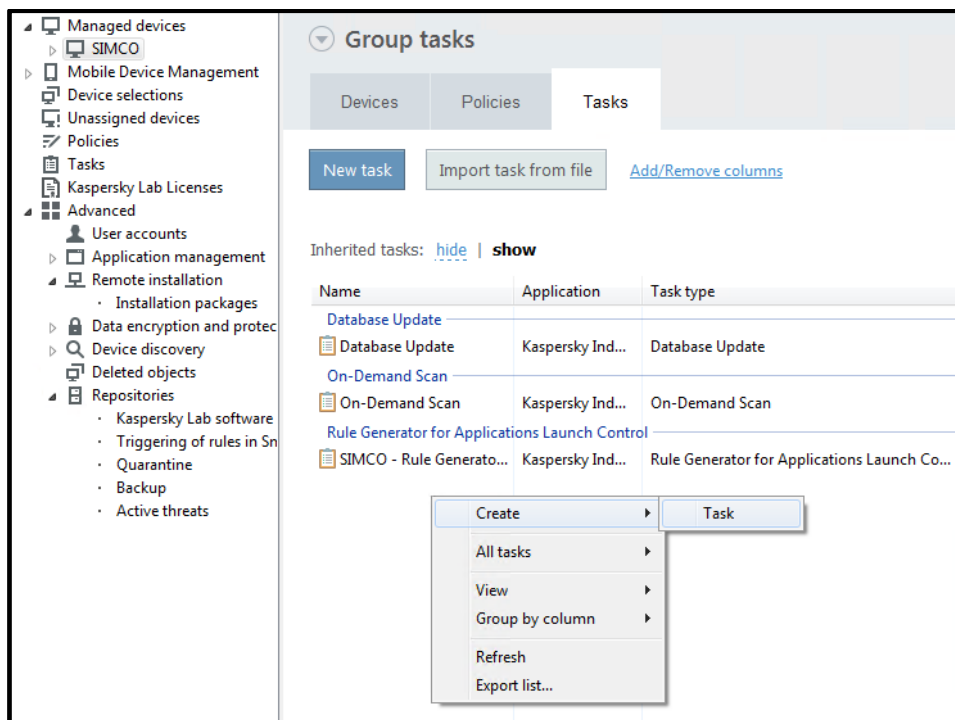
We hope that you will never encounter a situation that would make you do this. However, if it is necessary, you can perform software removal even without having to shut down your control system runtime.

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):

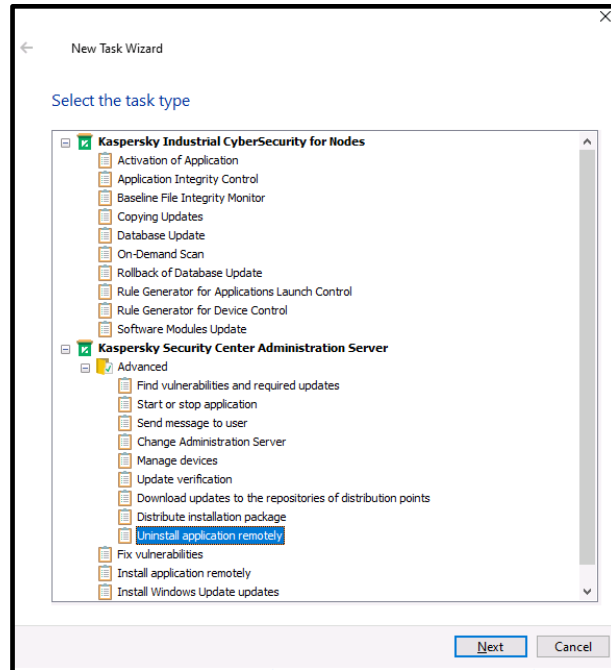
1. Go to the **SIMCO** node and switch over to the **Tasks** tab as shown below.



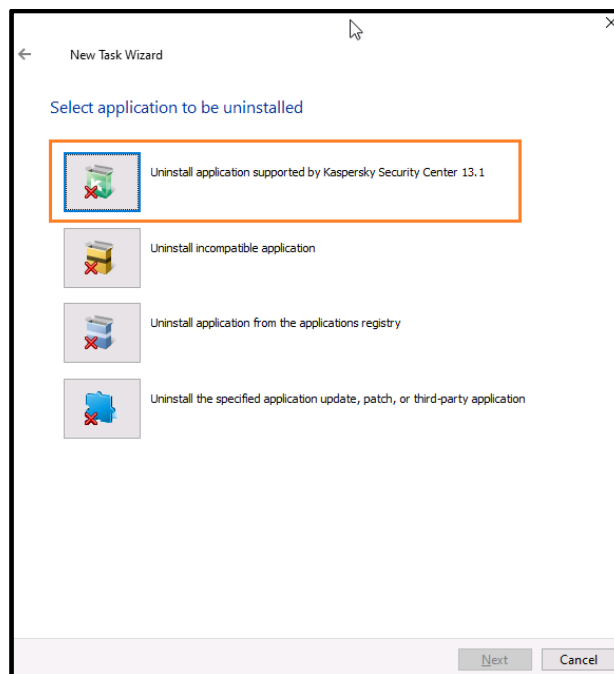
2. Right-click on any spare area of the **Tasks** list and in the context menu choose **Create->Task**.



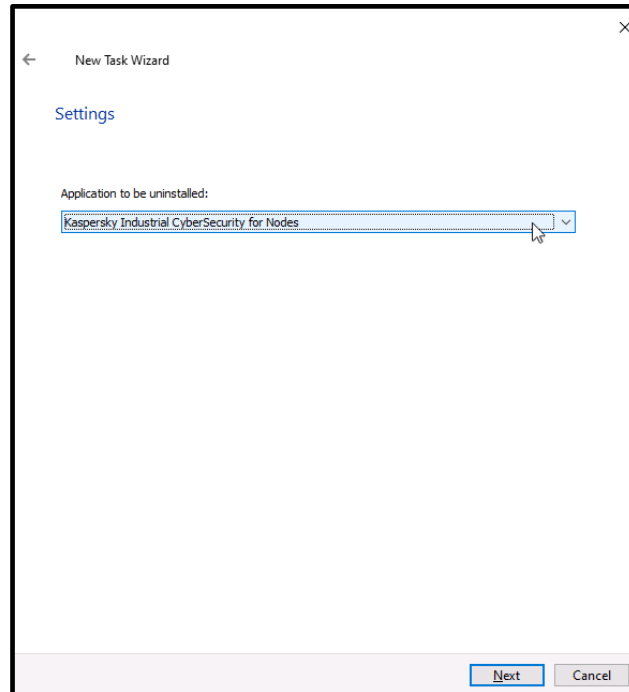
3. In the **New task wizard** window that appears, select **Kaspersky Security Center Administration Server->Advanced->Uninstall application remotely** as shown below. Click **Next**.



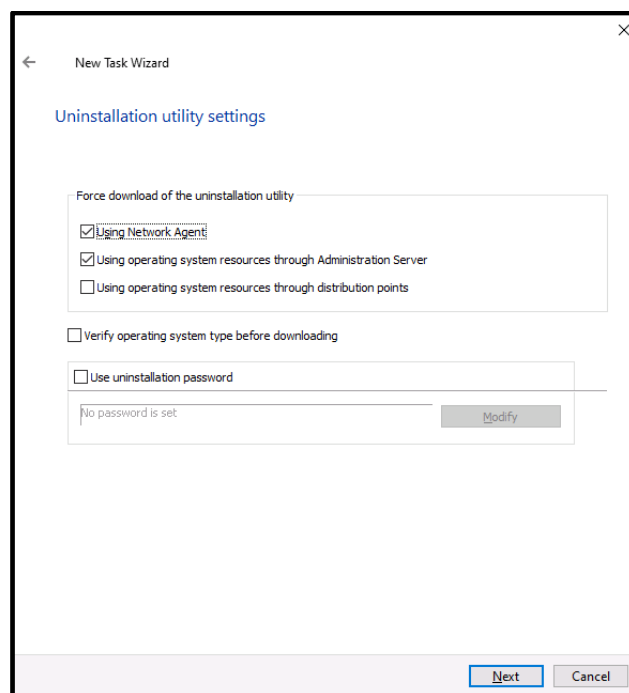
4. In the next window click **Uninstall application supported by Kaspersky Security Center 13.1** as shown below.



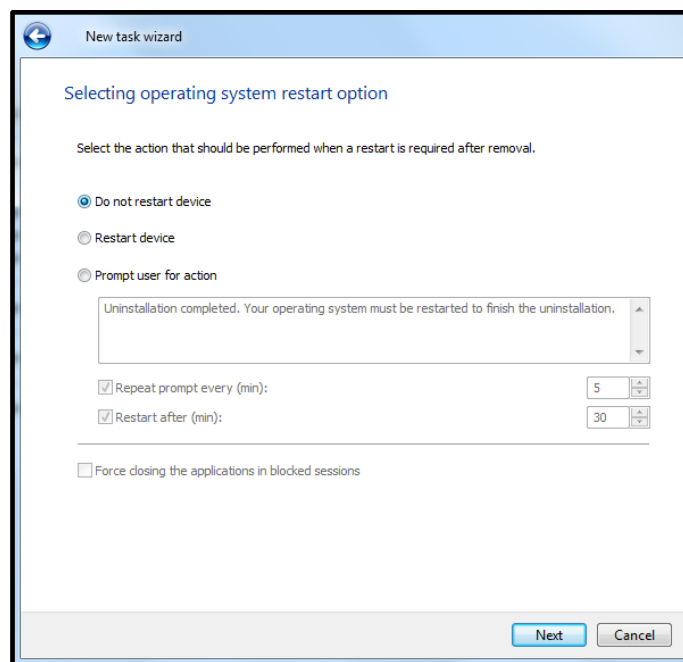
- In the window that appears specify **Kaspersky Industrial CyberSecurity for Nodes** as an application to be removed. Click **Next**.



- In the **Uninstall utility settings** window specify the settings as shown below. Additionally, you need to enter your protection password in the **Uninstall password** field unless you have the password protection disabled (please refer to section “Enabling optional password protection”). As you can see, in our case we have not enabled the password protection, which is not good, to be honest.

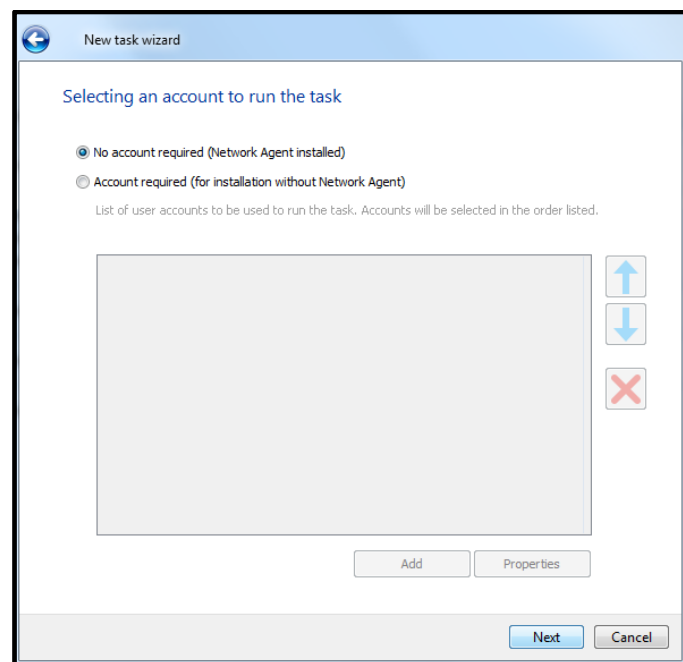


7. In the **Selecting operating system restart option** window specify the settings as shown below and click **Next**.



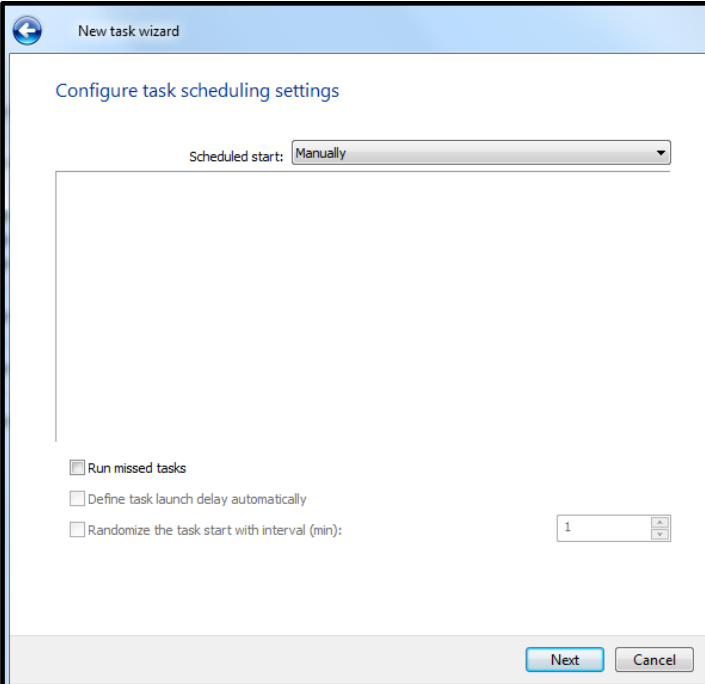
The screenshot shows the 'New task wizard' window with the title 'Selecting operating system restart option'. The instruction reads: 'Select the action that should be performed when a restart is required after removal.' There are three radio button options: 'Do not restart device' (selected), 'Restart device', and 'Prompt user for action'. Below the radio buttons is a text box containing the message: 'Uninstallation completed. Your operating system must be restarted to finish the uninstallation.' Below the text box are two checked checkboxes: 'Repeat prompt every (min):' with a value of 5, and 'Restart after (min):' with a value of 30. There is also an unchecked checkbox for 'Force closing the applications in blocked sessions'. At the bottom right are 'Next' and 'Cancel' buttons.

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



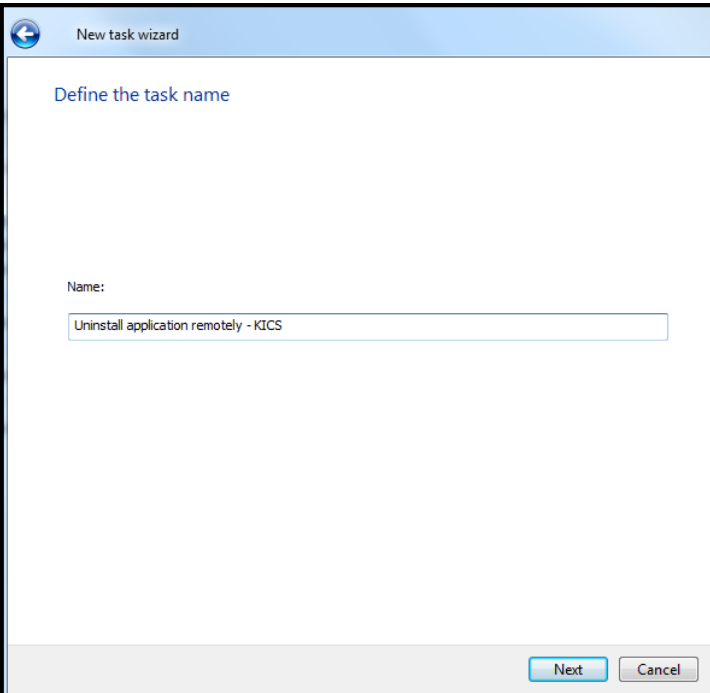
The screenshot shows the 'New task wizard' window with the title 'Selecting an account to run the task'. There are two radio button options: 'No account required (Network Agent installed)' (selected) and 'Account required (for installation without Network Agent)'. Below the radio buttons is a text box containing the instruction: 'List of user accounts to be used to run the task. Accounts will be selected in the order listed.' Below the text box is a large empty rectangular area for listing accounts. To the right of this area are three buttons: an up arrow, a down arrow, and a red 'X'. Below the list area are 'Add' and 'Properties' buttons. At the bottom right are 'Next' and 'Cancel' buttons.

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



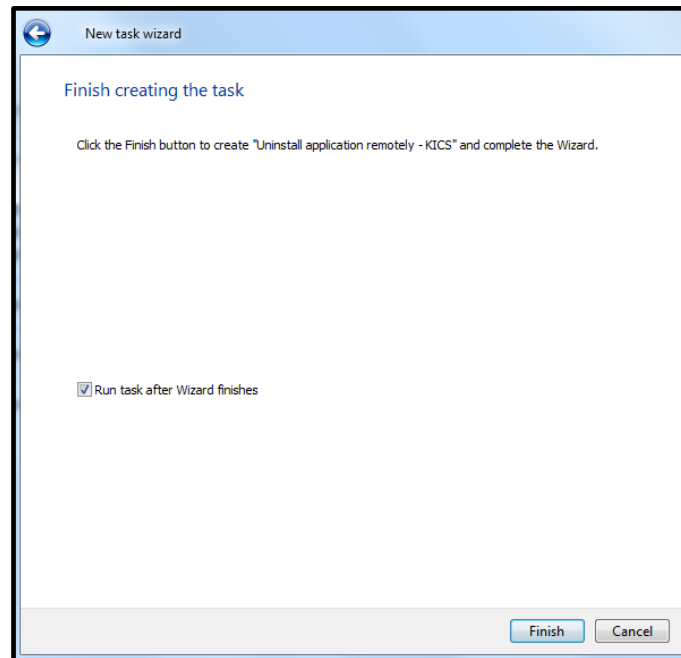
The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Configure task scheduling settings'. Below this, there is a 'Scheduled start:' label followed by a dropdown menu set to 'Manually'. A large empty rectangular box is positioned below the dropdown. At the bottom of the window, there are three checkboxes: 'Run missed tasks', 'Define task launch delay automatically', and 'Randomize the task start with interval (min):'. The 'Randomize' checkbox is followed by a small input field containing the number '1'. At the very bottom right, there are 'Next' and 'Cancel' buttons.

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

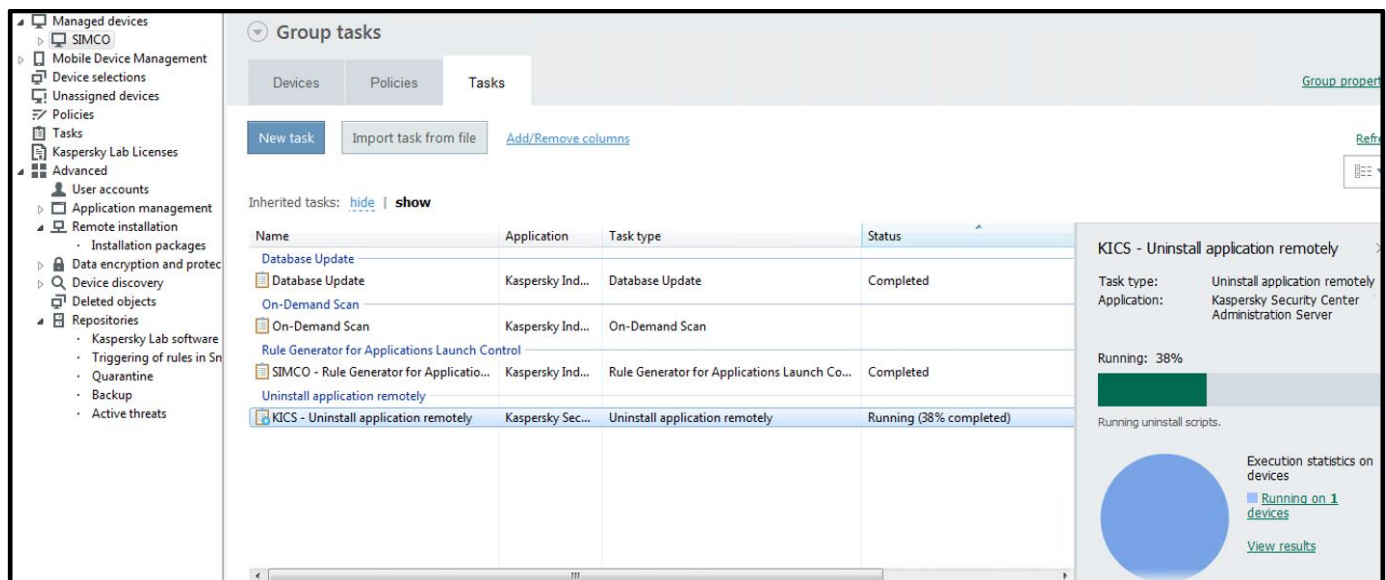


The screenshot shows the 'New task wizard' window with the title bar 'New task wizard'. The main heading is 'Define the task name'. Below this, there is a 'Name:' label followed by a text input field. The input field contains the text 'Uninstall application remotely - KICS'. At the bottom right, there are 'Next' and 'Cancel' buttons.

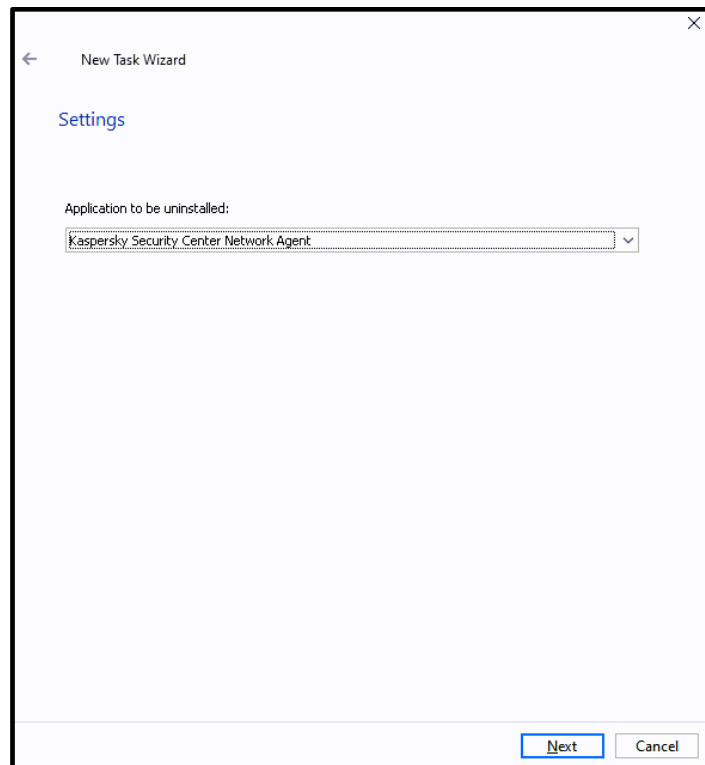
11. In the **Finish creating the task** window check **Run task after Wizard finishes**. Click **Finish**. This will start **KICS for Nodes** removal immediately.



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 3.0**, you may also want to uninstall the management agent **KLnagent** from your host (do not uninstall **KLnagent** prior to **KICS for Nodes 3.0!**). In order to get **KLnagent** removed, please perform exactly the same sequence of actions as was described in steps **1-11**. The only difference is that as you come to step **5** again, you will need to select **Kaspersky Security Center Network Agent** as an application to uninstall (as shown below).



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 3.0** shortcut.
- Run **Modify or Remove Kaspersky Industrial CyberSecurity for Nodes 3.0** 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 (3.0.0.287)** 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 3.0**, 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 the **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 enabling **Application Launch Control** and setting it to the **Statistics** only mode, it is required to perform a limited time trial run involving regular process supervision/engineering operations on your DCS (such as viewing real-time and historical trends, adjusting setpoints, switching between mimics, generating reports, acknowledging process alarms, doing PLC diagnostics or even making modifications in a process control logic). The said technique ensures enhanced discovery of dynamically created executable files: those that did not exist while the **Generate Rules for Application Launch Control** task was running. Generally, the trial run period must not be less than 12 hours but you can make this “fine tuning” of **Application Launch Control** a lot easier by rebooting your computer (as long as it is practically possible). If you encounter any alerts on 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 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 the validation (in case of a 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 are running. 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 clearance (by using the **On-demand scanning** task, for example).
- It is 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.



www.kaspersky.com/

www.securelist.com

© 2021 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owner