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

Step-by-step installation and configuration guide

17.11.2021

#### 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	5
Installation of KSC on a management PC	6
Initial configuration of KSC	14
Remote installation of KLnagent onto target computers	24
Installation of the KICS for Nodes management plugin	36
General configuration of the security policy for KLnagent	
Configuring KICS for Nodes instances	42
Creation of the generic policy for KICS for Nodes	43
Settings of KICS for Nodes generic policy	46
Remote installation of KICS for Nodes onto target computers via KLnagent	56
Remote installation of Hotfix onto target computers via KLnagent	71
Rule generation optimization for Application Launch Control	79
Initial update of antivirus databases	86
Performing On-Demand Scanning on target hosts	96
Execution of the Generate Rules for Application Launch Control task	104
Setting up Application Launch Control whitelisting	112
Setting up Device Control whitelisting	116
Setting up File Operations Monitor	122
Setting up PLC Integrity Checker	126
Enabling optional password protection	140
Installing optional KICS for Nodes management console	141
Uninstalling KICS for Nodes and KLnagent	150
FSTEK certification for KICS for Nodes installations within the territory of Russia	160
Recommendations	160

#### What this document is about

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

#### Who would find this document useful

This document might be interesting to the following audience:

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

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

#### What is KICS

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

#### **KICS** software components

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

• **KICS for Nodes**. This component protects Windows-based endpoints such as operator workstations, engineering workstations, historians, HMI-servers, etc. Therefore, it has the potential of interfering with the HMI software and engineering software unless it is configured correctly.

• **KICS for Networks**. This component acts as a real-time analyzer of industrial networks traffic. As opposed to the previous one, this component remains 100% passive and by no means affects the monitored system. It remains invisible from the DCS perspective and architecturally has no mechanisms of interfering with DCS operation.

• Kaspersky Security Center (from now on, KSC). It is an administration tool, which enables management of the KICS components in a centralized and user-friendly manner.

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

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

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

• **Application launch control**. It restricts execution of files and scripts according to the user-defined white list.

• **Device control**. It restricts connection of peripheral devices to the protected host. It solely deals with USB-interface storage devices such as USB memory sticks, USB hard drives, etc.

• Anti-malware protection (real-time file protection). It performs an anti-viral inspection of a file every time it is accessed, modified, moved or copied.

• **On-demand antimalware scanner**. It performs on-demand search for malicious objects in locations specified by users.

- Virus database updater. It is essential for keeping anti-virus databased up to date.
- **Untrusted host blocker**. It blocks network access to shared folders for the remote hosts that show malicious activity.

• Anti-cryptor. It prevents malicious encryption activity. It is designed to work in conjunction with the Untrusted host blocker.

• **Vulnerability scanner**. It is used to obtain comprehensive and up-to-date information on software vulnerabilities found on the managed hosts.

• File integrity monitor. It is designed to track/alert modifications made to the specified files and folders of the monitoring scope according to the task settings. You can use the task to detect file changes that may indicate a security breach on the protected computer.

• Log inspection. It is designed to monitor the integrity of the protected environment based on the results of an inspection of Windows Event Logs. The application notifies the administrator upon detecting abnormal behavior in the system, which may be an indication of attempted cyber-attacks.

• **Exploit prevention.** Kaspersky Industrial CyberSecurity for Nodes 2.6 provides the ability to protect process memory from exploits. You can change the component activity status and configure process protection settings.

• PLC Integrity Checker. It periodically verifies consistency of control logic, executed by the monitored PLC. It reacts to any modification of a process control program. At present, this module supports SIMATIC S7-300, S7-400(H) series controllers.

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

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

#### **Distribution package composition**

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



The Hotfix folder contains Hotfix 12<sup>2</sup> for KICS for Nodes 2.6. The Hotfix is cumulative and in most cases its installation is compulsory<sup>3</sup>.



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



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

₲ ksc\_12.2\_full\_en.exe

 $<sup>^{2}</sup>$  As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a subsequent version has become available.

<sup>&</sup>lt;sup>3</sup>If **KICS for Nodes** is deployed onto critical infrastructure production sites located in Russia, the **Hotfix** installation may not be compulsory. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section.

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



The Generic\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp file is a preconfigured set of the high-level security settings optimized for Simatic PCS 7 9.1. These predefined settings, which KSC makes use of, significantly facilitate the KICS for Nodes deployment process. The similar file (KLNagent\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp) aids the KLnagent configuration.

#### System requirements

We recommend installing **KSC** on a separate PC designated for the centralized management of **KICS for Nodes** instances. Please make sure that this computer conforms to the software and hardware requirements as specified in <a href="https://support.kaspersky.com/KSC/12/en-US/96255.htm">https://support.kaspersky.com/KSC/12/en-US/96255.htm</a>.

Every target station hosting **KICS for Nodes** should be compliant with the system requirements as specified in pages 29-30 of the supplied "**KICS for Nodes 2.6 Administration Guide**" (**kics\_admin\_guide\_en.pdf**). The following ports should also be open for normal KICS for Nodes infrastructure management from KSC:

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

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

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

Optionally, the **KSC** server may utilize network access to the **Kaspersky Lab download servers** via port TCP: 80 (HTTP).

For correct external name resolution, it is recommended to grant the **KSC** server full access to DNS servers via TCP: 53 and UDP: 53.

To ensure smooth interaction between the **KSC** server and target stations, Ethernet connection with at least 10Mbit/s throughput is required.

#### Installation and configuration steps

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

- Installation of KSC on a management PC.
- Initial configuration of KSC.
- Remote installation of the network agent KLnagent onto target computers.
- Installation of the KICS for Nodes management plugin on the top of KSC.
- Import of the security policy for the network agent KLnagent from a file.
- Import of the generic security policy for KICS for Nodes from a file.
- Remote installation of **KICS for Nodes** onto target computers via **KLnagent**.

• Remote installation of **Hotfix 12**<sup>4</sup> onto target computers via **KLnagent**. Please note that in some specific cases no **Hotfix** should be installed and this deployment step should be omitted. Please refer to the "**FSTEK** certification for **KICS for Nodes** installations within the territory of Russia" section for details.

- Optional activation of KICS for Nodes delayed startup.
- Optional remote installation of KICS for Nodes management console.
- Initial update of antivirus databases.
- Launching the **On-Demand virus scan** task to inspect target computers.
- Setting up **Application Launch Control** and **Device Control** whitelisting and fine-tuning the generic security policy.
- Configuration of **PLC Integrity Checker**.

#### Installation of KSC on a management PC

The **KSC** deployment is commenced with installation of **MS SQL Server 2016 Express Edition** or a later version (for small and medium-size control systems including less than 100 nodes). The **MS SQL** installer is available at <a href="https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-">https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-</a>

<u>52470555DB90/ENU/SQLEXPR\_x64\_ENU.exe</u>. However, for the larger systems we recommend installing full functional **MS SQL Server**.

Please perform the following operations:

- 1. Log in on your PC using an account with administrative privileges.
- 2. Install **MS SQL Server Express Edition** or **MS SQL Server** depending on your system scale. Follow Microsoft installation guideline.
- 3. Copy ksc\_12.2\_full\_en.exe from the supplied distribution package to the desktop and launch it.
- 4. Acknowledge UAC for the file launch if requested.

<sup>&</sup>lt;sup>4</sup> As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a newer **Hotfix** version has become available.

5. The following component selection window should pop up.

kaspersky	Kaspersky Security C	enter 1	12 – ×
• :	<u>Install Kaspersky Security</u> <u>Center 12</u>		Install only Kaspersky Security Center 12 Administration Console Install only Kaspersky Security Center 12 Network Agent
	(Mobile Device Management) Serve	r 🛧 E	extract installation packages
Install Exchange	<u>e Mobile Device Server</u>		

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



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



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



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

Kaspersky Security Center 12 Administration Server —	×
End User License Agreement and Privacy Policy Please carefully read the License Agreement and Privacy Policy.	
Kaspersky Security Center 12 END USER LICENSE AGREEMENT; AND Products and Services PRIVACY POLICY	^
KASPERSKY LAB END USER LICENSE AGREEMENT ("LICENSE AGREEMENT")	
IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.	
	¥
I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement	
I am aware and agree that my data will be handled and transmitted (including to third ✓ countries) as described in the <u>Privacy Policy</u> . I confirm that I have fully read and understand the <u>Privacy Policy</u> .	
© 2020 AO Kaspersky Lab. All Rights Reserved.	
< Back Next > Cancel	

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

Kaspersky Security Center 12 Administration Server —	×
Installation type Select the installation type that best suits your needs.	
Select the installation type that best suits your needs.	
Standard installation allows you to install the default set of components and configure the database. No changes will be made to any settings outside the described scope. The Mobile Device Management feature is unavailable in standard installation mode. Custom installation allows you to select additional components and manage an extended set of application installation settings.	2.1
Standard	1
◯ Custom	
- © 2020 AO Kaspersky Lab. All Rights Reserved.	
< Back Next > Cancer	

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



Page 9 of 161

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



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



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

Kaspersky Security Center 12 Administrat	tion Server -	· 🗆	×
Connection settings Specify the Microsoft SQL Server setting	js.		
<ol> <li>Make sure that the relevant version You can download Microsoft SQL Se another supported version from the Microsoft SQL Server are available</li> <li>Specify the Microsoft SQL Server so</li> </ol>	n of Microsoft SQL Server is install erver 2014 Express SP2 (recomme e <u>Microsoft website</u> . Other versior on <u>this website</u> . ettings:	led. Inded) or Ins of	
SQL Server instance name:	SIMCO\SQLEXPRESS	Browse	
Database name:	KAV		
– © 2020 AO Kaspersky La < <u>B</u> ack	ab. All Rights Reserved.	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 12 Adminis	tration Server	_		×
SQL Server Authentication mode.	le			
Choose the authentication mode tha Server. If you select SQL Server Aut and confirm the password.	t you want to use for connectio hentication, you are prompted	n to Micro to enter t	soft SQL he account	
<ul> <li>Microsoft Windows Authentication</li> </ul>	n mode			
○ SQL Server Authentication mode				
Account:				
Password:				
Confirm password:				
- © 2020 AO Kaspersky	y Lab, All Rights Reserved. ack <u>N</u> ext >		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. Only check **Start as MMC-based Administration Console** and click **Finish**.



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

Administration Server has handed its certificate:	
- Fingerprint: A7F570543A3D14B5F567FA2234C66666A8B55D66	
- Subject: CN = WIN-LPJARCQOGPK	
- Alternative subject name: DNS: WIN-LPJARCQOGPK	
Do you want to continue connection to this Administration Server?	
Yes No	

#### Initial configuration of KSC

The **KSC** Administration Console automatically starts up after the **KSC** server core components are installed<sup>5</sup>. Please note that the screenshots presented hereafter mainly refer to **Kaspersky Security Center 11**. You should not be confused by the version mismatch since all the settings are applicable and identical for version **12**. Please perform the following operations to apply basic settings to **KSC**:

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



<sup>&</sup>lt;sup>5</sup> The other way of calling **KSC Administration Console** is using the **Kaspersky Security Center 12** shortcut located on the **Start** menu.

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

🐾 Kaspersky Security Center 11								
File Action View Help								
🗢 🔿 🖄 🐻 🗙 🕤 🛛 🖬								
Kaspersky Security Center 11  Carter Administration Server KSC  Managed devices	Administration Server KSC (KSC\Administrator)							
Unassigned devices	Monitoring	Statistics	Reports	Events				
Tasks	-							
Advanced	🔻 Deployme	nt						
	Enable protection							
	Manage keys							
	Protection deployment report							
	Protection settings     A software uninerability has been detected on devices							
	Edit protection policy for workstations							
	Edit Virus Scan task for workstations							
	Manage applications on devices							
	▼ Monitoring							
	Critical events registered on Administration Server.							
	View protection status							
	View user reg	uests (new: 0)						
	Configure not	ifications						

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



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

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

Add Key Wizard	KL_Dis	tributives 🕨 License			▼ 4 <sub>7</sub>	Search License		
	Organize 🔻 New fo	older				80	• 🗇	(
Selecting a key	☆ Favorites	Name	Date modified	Туре	Size			
Specify key file:	📃 Desktop	<ul> <li>Unspecified (1)</li> </ul>						
Browse	Downloads	KICS-2018-08-09-long.key	22.11.2017 12:01	KEY File	1 KB			
☑ Automatically deploy key to managed devices	<ul> <li>➢ Libraries</li> <li>➢ Documents</li> <li>➢ Music</li> <li>➢ Pictures</li> <li>➢ Videos</li> <li>➢ Computer</li> <li>▲ OSDisk (C:)</li> <li>— Removable Disk (I</li> <li>♀ Network</li> </ul>	₽;)						
Nex	File	e name: KICS-2018-08-09-long.key			- K	Cey files for Kasper	sky Lab a Canc	opl el

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

0	Add Key Wizard	*
	Selecting a key	
	Specify key file:	
	C: \Users \Administrator \Desktop \KL_Distributives \License \KICS-2018-08-	Browse
	Automatically deploy key to managed devices	
		Next Cancel

8. Please Finish to complete adding your key file.



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

Administration Server Kaspersky Lab Keys in storage.	KSC > Advanc licenses	ed > <u>Application</u>	<u>n management</u> > k	(aspersky Lab lic	enses	
Add key Deploy ke	ey to managed d	evices Additio	onal actions 🔻			
Key	License type	Restriction	License term (da	End date of key	License expiratio	Application
4 250A-00065C-55F87D14	Commercial	14	353	09.08.2018	09.08.2018 3:00:00	Kaspersky Industrial CyberSecurity International Edition. 10-14 Node 1 year

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



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



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

🗇 🏟 🙎 💼 🖾 🙆 🖬				
<ul> <li>Administration Server KSC</li> <li>Administration Server KSC</li> <li>Chain Server Kerner</li> <li>Chain Server</li> &lt;</ul>	Administration Server KSC > IP subnets Displays results of IP subnet poll or Actions Add subnet Configure polling Pol now	Advanced > Network poll > IP s Properties: IP subnets Sections General	General   General   Subnets   Poll now	
		нер	OK Cancel	Apply

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

Kaspersky Security Center 11			
File Action View Help			
🗢 🔿 📶 🗊 🙆 📓 🖬			11
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server KSC</li> <li>Managed devices</li> <li>Device selections</li> <li>Onevice selections</li> <li>Policies</li> <li>Tasks</li> <li>Advanced</li> <li>User accounts</li> <li>Application managemer</li> <li>Remote installation</li> <li>Network poll</li> <li>Active Directory</li> <li>Pomains</li> <li>Active Directory</li> <li>Repositories</li> </ul>	Administration Server KSC > Advanced > Network poll > IP subnets IP subnets Displays results of IP subnet poll on the network by sending an ICMP packet. Poling network: 31% Actions Add subnet > Configure polling > Pol now		
( ) )		<u>Help</u> •	KA\$PER\$KY
IP subnets: 3			

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

Kaspersky Security Center 11							
File Action View Help	1						
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server KSC</li> <li>Managed devices</li> <li>Device selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Advanced</li> <li>User accounts</li> <li>Application managemer</li> </ul>	Administration Server MyPCS7 Show group properties Name	KSC > Advance Perform ac Type of operat	ed > <u>Ne</u> tion ▼ Wind	twork poll > [ Add/Remove co Agent installed No	P subnets	s > MyPCS7 BACKUP	<u>Refresh</u> ×
<ul> <li>Remote installation</li> <li>Network poll</li> <li>Domains</li> <li>Active Directory</li> <li>IP subnets</li> <li>MyPCS</li> <li>Repositories</li> </ul>	Coscient Socient S		WOR WOR WOR WOR WOR WOR WOR WOR WOR	<ul> <li>No</li> </ul>	<ul> <li>No</li> </ul>	Device status: Unkn Properties IP address: Actions Move to Group Instal application Remove from group	iown 192.168.0.200

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

<sup>&</sup>lt;sup>6</sup> Please note that in this document the terms "device", "host" and "target computer" have the same meaning and are interchangeable.

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

🔀 Kaspersky Security Center 11			
File Action View Help			
🗢 🔿 🖄 🗊 🖺 🖬 👹			
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>Mobile Device Management</li> <li>Device selections</li> <li>Unassigned devices</li> </ul>	Administration Server WIN-R2FGT0TNH3K > Advan Time Installation packages Installation packages listed below are used for remote deployment	<u>ced</u> > <u>Remote installation</u> > Installation	packages
Policies       Tasks       Kaspersky Lab Licenses       Advanced	Create installation package View the list of stand-alo	ne packages Additional actions <b>v</b>	Refresh
▲ User accounts ► Application management ▲ 모 Remote installation • Installation packages	Name Te iOS MDM Server (11.0.0.1131) Kaspersky Endpoint Security for Windows (11.2.0) (11.2.0.22	Application iOS MDM Server Kaspersky Endpoint Security for Windows (11.2.0)	Microsoft Exchange Mobile Devices × Server (11.0.0.1131)
<ul> <li>A Data encryption and protection</li> <li>Q Device discovery</li> <li>D Deleted objects</li> <li>Repositories</li> </ul>	<ul> <li>Kaspersky Security Center 11 Network Agent (11.0.0.1131)</li> <li>Microsoft Exchange Mobile Devices Server (11.0.0.1131)</li> </ul>	Kaspersky Security Center 11 Network Agent Microsoft F Install application Create stand-alone installation p Show the list of stand-alone pac	Properties Microsoft Exchange Mobile Devices Server 11.0.0.1131 kages 14473 KB
	۲	Group by column Delete Export list	plication     tand-alone installation package     e installation package
Installation packages: 4		rroperues	Help - KASPERSKYS

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

window.



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

Kaspersky Security Center 11						
File Action View Help						
🗢 🄿 📶 🖾 🤷 🚺 📷						
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>Mobile Device Management</li> <li>Device selections</li> <li>Unassigned devices</li> </ul>	Administration Server WIN- Tistallation package Installation packages listed below a	R2FGT0TNH3K > Advar es re used for remote deploym	nced > <u>Remote</u> nent.	<mark>installation</mark> > Installation	packages	
Policies Tasks Kaspersky Lab Licenses Advanced	Create installation package	View the list of stand-al	one packages	Additional actions 🔻		<u>Refresh</u>
<ul> <li>▲ Deprication management</li> <li>▲ Application management</li> <li>▲ Remote installation</li> <li>✓ Installation packages</li> <li>▲ Data encryption and protection</li> <li>♦ Q Device discovery</li> <li>➡ Deleted objects</li> <li>♦ Repositories</li> </ul>	Name	twork Agent (11.0.0.1131)	Application Kaspersky Secur	ity Center 11 Network Agent	Kaspersky Sect Agent (11.0.0. Properties Application: Version: Size: Actions <u>Install application</u>	urity Center 11 Network× 1131) Kaspersky Security Center 11 Network Agent 11.0.0.1131 53138 KB On
	•	III		•	Configure inst	Ilation nackana
						Help - KASPERSKY
Installation packages: 1						

#### 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 <u>\\SIMCO\C\$</u> or <u>\\SIMCO\ADMIN\$</u>). If not, please set it up first and memorize your administrative credentials.

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

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

🔏 Kaspersky Security Center 11		
File Action View Help		
🗢 🄿 🙍 🔲 📮 🧟 📔 📷		
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>Mobile Device Management</li> <li>Device selections</li> <li>Unassigned devices</li> </ul>	Administration Server WIN-R2FGT0TNH3K > Advanced > Remote installation > Installat Tinstallation packages Installation packages listed below are used for remote deployment.	ion packages
Folicies     Tasks     Tasks     Kaspersky Lab Licenses     Advanced	Create installation package         View the list of stand-alone packages         Additional actions ▼           Add/Remove columns         Image: Column State Stat	Refresh
<ul> <li>▲ User accounts</li> <li>→ Application management</li> <li>→ Remote installation         <ul> <li>Installation packages</li> <li>→ Data encryption and protection</li> <li>◇ Device discovery</li> <li>→ Deleted objects</li> <li>&gt; ▲ Repositories</li> </ul> </li> </ul>	Name     Application <ul> <li>Kaspersky Security Center 11 Network Agent (11.0.0.1131)</li> <li>Kaspersky Security Center 11 Network Agent (11.0.0.1131)</li> <li>Create stand-alone installation package</li> <li>Show the list of stand-alone packages</li> <li>Group by column</li> <li>Delete</li> <li>Export list</li> </ul> <li>Properties</li>	Kaspersky Security Center 11 Network× Agent (11.0.0.1131) Properties Application: Kaspersky Security Center 11 Network Agent Version: 11.0.0.1131 Size: S3138 KB Actions Instal application Create stand-alone installation package Configure bets for package
installation packages: 1		

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

Properties: Kaspersky Sec	curity Center 11 Network Agent (11.0.0	1131)	
Sections	Connection		
General Settings	Server address:	192.168.0.120	
Connection	Port number:	14000	
Advanced	SSL port number:	13000 🔶	
Tags	7.02	34071	
Revision history	<ul> <li>Use Server certificate</li> <li>Certificate fingerprint: A7F570 Subject: CN = WIN-LPJARCQQ Alternative subject name: DNS</li> <li>Use SSL</li> <li>Use UDP port UDP port number:</li> <li>Open Network Agent ports in N</li> </ul>	IS43A3D 1485F567FA2234C66666A885SD66 SGPK : WIN-LPJARCQOGPK IS000 ficrosoft Windows Firewall Con	Infigure connection via proxy server
Help		ок	Cancel Apply

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



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

•	Remote Installation Wizard		
S	Select installation package		
	Kaspersky Security Center 11 Network Agent (11.	0.0.1131)	
	Kaspersky Security Center 11 Network Agent (11.0.0	. 1131)	
		New	Properties
			Next Cancel

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

$\bigcirc$	Remote Installation Wizard
	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 <ul> <li>Install always</li> <li>Install only on devices managed through this Administration Server</li> </ul>
	Do not re-install application if it is already installed  Assign package installation in Active Directory group policies
	Next Cancel

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

◎ No account required (Netw	rork Agent installed)	
Account required (for insta Add accounts with administ domain controller for installa	illation without Network Agent) rator rights on the devices where the applic ation through Active Directory.	ation is to be installed or on th
Account	ି <mark>∞</mark>	Add
Administrator		Properties
Password: Confirm password:	•••••	
	OK Cancel	
		-



7. When done, click Next.

Remote Installation	Wizard	A and a P subset of the Party
Select user accou	nt to access remote device	
🔘 No account require	d (Network Agent installed)	
Account required ( Add accounts with a domain controller for	or installation without Network Agent) Idministrator rights on the devices where t r installation through Active Directory.	the application is to be installed or on the
Administrator		Add
		Properties
L		
		Next Cancel

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

Remote Installation Wizard
Selecting operating system restart option
Select the action that will be performed if application installation requires an operating system restart.
Do not restart device
Restart device
Device will be restarted automatically
Prompt user for action
User will be prompted to restart device Prompt will appear every 5 minutes Device will be restarted in 30 minute(s)
Madify
Force closing the applications in blocked sessions
Next Cancel

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



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



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

Inst	all application		
Ins Clic	talling the application on the devic k View Results to view the installa	e. Please wait tion progress.	
Clio Ka	k Finish if you do not want to wait spersky Security Center 11 Networ	t for installation to complete. Remote i rk Agent (11.0.0.1131)" will keep runr	installation task "Deploy ing.
-	Running		
	View results		

Refresh	se the Refresh button to	display latest results.				
Time	Device	Status	Description		Group	
1 20.02.2018 16:43:48	SIMCO	Running (2%)	Device "SIMCO" has been res	olved to "192.168.0.80" for	WORKGROUP	
umber of events: 1						
SIMCO						
Time	Status	Description		Registration time	Name of virtual Administration	
1 20.02.2018 16:43:48	Running	Device "SIMCO" has be	Device "SIMCO" has been resolved to "192.168.0.80" for			
0 20.02.2018 16:43:45	Scheduled			20.02.2018 16:43:45		
20.02.2018 16:43:45	Scheduled			20.02.2018 16:43:45		
1					•	



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

Application deployment fir Click View results to view	nished. details. Click Finish to complete Remote	Installation Wizard.
Completed		
<u>View results</u>		

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

<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server KSC</li> <li>Managed devices</li> <li>Device selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Advanced</li> <li>User accounts</li> <li>Application managemer</li> <li>Remote installation</li> <li>Q Network poll</li> <li>Omains</li> <li>Active Directory</li> <li>IP subnets</li> <li>MyPCS</li> <li>Deleted operts</li> </ul>	Administration	<u>Server KSC</u> > N d devices	lanaged devi	ices			
	Devices	Policies	Tasks				
	Add devices New group Perform action  Add/Remove columns						
	No filter spectrum Select statuses: The above numbers in The list below only in	Critical: 2	total: 2 Warning: 0 devices with the s is selected group.	OK: 0 pedified status, which	h are in the selected	group and in any of its	
Repositories	Name	Type of o	perat Wind	Agent installed	Agent running	Real-time prot	
	📮 KSC	Micro	soft WOR	✓ Yes	✓ Yes	No	
	SIMCO	Micro	soft WOR	🗸 Yes	🗸 Yes	No	

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

⊿ 🔂 Admir	nistration Server KSC anaged devices Move unassigned devic	Administration	devi	KSC >	Manage	ed devi	ces			
	Install application Search Reset Virus Counter Virus Activity		Polici	es	Tasks			A.44/0-		
Þ	New		Gre	oup	Perio	orm acu	on +	Add/Kel	nove columns	
	All Tasks	•								
	View	•	ineu, records total. 2							
	Refresh		Critical: 2 Varning: 0 V. O					ad a		
Þ	Properties			udes devices from the selected group.						cuy
	Help			Type of	operat	Wind	Age	nt installed	Agent runnin	g
		SIMCO	·	Mic Mic	rosoft rosoft	WOR	1 Y	(es (es	<ul><li>✓ Yes</li><li>✓ Yes</li></ul>	

15. Give a name to a new group.

Group name	? <b>X</b>
Enter the name of a new group:	
	OK Cancel

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



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

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

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

Name	Date modified	Туре	Size
🚾 bases.cab	12.12.2019 15:05	WinRAR archive	255 792 KB
📓 config.ini	13.11.2019 10:39	Configuration sett	1 KB
kics.kud	12.12.2019 15:09	KUD File	10 KB
🙀 kics_x64.msi	12.12.2019 15:15	Windows Installer	33 444 KB
🕞 kics_x86.msi	12.12.2019 15:15	Windows Installer	31 008 KB
🌀 klcfginst.exe	12.12.2019 15:16	Application	5 651 KB
license.txt	11.12.2019 16:01	Text Document	61 KB
🏟 setup.exe	12.12.2019 15:16	Application	730 KB

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



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



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

A Administration Server KS	Administration Sonior VSC (VSC)	dmini
Managed devices	Disconnect from Administration Server Install application Search	Repor
	All Tasks	
Tasks	View >	
User accounts	Delete	stalled o
> 모 Remote installatio	Properties	
▲ Q Network poll ▷ · Domains	Help	
<ul> <li>Active Directory</li> <li>IP subnets</li> <li>MyPCS</li> <li>Repositories</li> </ul>	✓ Protection settings Real-time protection application is not instal	led

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

Sections	Details of application management plug-ins installed
General	
Event configuration	iOS Mobile Device Management plug-in
Keys	
KSN Proxy	Kaspersky Endpoint Security for Windows (11.2.0) 11.2.0.2254
Administration Server connection settings	Kaspersky Industrial CyberSequrity for Nodes 2.6
Virus outbreak	2.6.0.785
Traffic	Raspersky Security Center 11 Administration Server
Events repository	11.0.0.1131
Web Server	Kaspersky Security Center 11 Network Agent
Revision history storage	11.0.0.1151
Application categories	Plug-ins for Microsoft Exchange ActiveSync 11.0.0.1131
Distribution points	
Tagging rules	
List of global subnets	
Notification	
Revision history	
Advanced	
Details of Administration Server manageme	
Details of application management plug-ins	
Details of current database	
Administration Server operation statistics	
Administration Server shared folder	
Configuring Internet access	
	Export to file Details
Help	OK Cancel Apply

#### General configuration of the security policy for KLnagent

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

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

<ul> <li>Administration Server WIN-LPJARCQOGPK</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mabile Davies Management</li> </ul>	Administration S	erver WIN-LPJARCQOC	<u>аРК</u> > Ма	maged devices
Mobile Device Management	Devices	Policies Tasks		
Tasks	Create a policy	Import policy from file	Add/R	lemove columns
<ul> <li>User accounts</li> <li>Application management</li> <li>Remote installation</li> </ul>	Name	*	Status	Application
<ul> <li>Installation packages</li> <li>Data encryption and protection</li> <li>Q Network poll</li> </ul>		Import	_	
Repositories		Create All tasks	•	
		View Group by column	•	
		Refresh Export list		
	1			

2. Using the file browser, go to the distribution package and locate the **KLNagent\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp** file as shown below. Click **Open**.

C Open					×
← → ~ ↑ 🔒 → Th	is PC > Desktop > KL_Distributives >	~	Ö Search k	(L_Distributives	<i>م</i>
Organize 🔻 New folde	er			III 🔻 🔟	?
📙 KL_Distributives \land	Name	Date modified	Туре	Size	
📙 WinBootPe	HotFix	5/20/2021 1:46 AM	File folder		
len OneDrive	KICS4NODES	5/20/2021 1:47 AM	File folder		
_	KSC .	5/20/2021 1:46 AM	File folder		
💻 This PC	License	5/20/2021 1:46 AM	File folder		
🧊 3D Objects	Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp	5/20/2021 1:46 AM	KLP File	72 KB	
📃 Desktop	KLNagent_policy-KICS4NODES_2.6_PCS7_9.1.klp	5/20/2021 1:46 AM	KLP File	8 KB	
🔮 Documents					
🖶 Downloads					
🁌 Music					
Pictures					
📑 Videos					
🏪 Local Disk (C:)					
🕳 Local Disk (D:)					
i Network					
File <u>n</u> :	ame: KLNagent_policy-KICS4NODES_2.6_PCS7_9.1.klp		✓ Policy F	iles (.klp)	$\sim$
	L		Or	en Cance	1

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

File Action View Help					
🗢 🔿 🙍 🗊 📋 🗐 🥥 🗾 🖚					
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices         <ul> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> </ul> </li> </ul>	Administration	n Server WIN-	R2FGT0TNH	1 <u>3K</u> > Mana	ged devices
Upassigned devices	Devices	Policies	Tasks		
<ul> <li>Policies</li> <li>Tasks</li> <li>Kaspersky Lab Licenses</li> <li>Advanced</li> </ul>	New policy	Import policy	/ from file	<u>Add/Remove</u>	<u>columns</u>
	Name	+		Status	Application
	Kaspersky Secu Kaspersky Sec	rity Center 11 Net curity Center 11 Ne	work Agent		Kaspersky Security Center 11 Network Agent

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

File Action View Help								
🗢 🔿 🔁 📰 📋 🖼 🖬								
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> </ul>	Administration	<u>) Server WIN-</u>	R2FGT0TN	<u> H3K</u> >	Mana	ged devices		
Mobile Device Management     Device selections     Inassigned devices	Devices	Policies	Tasks					
·가 Policies 首 Tasks 당 Kaspersky Lab Licenses ▷ 〓 Advanced	New policy	Import policy	from file	<u>Add/</u>	Remove	<u>columns</u>		
	Name	<b>*</b>			Status	Application		Inh
	Kaspersky Secur	ity Center 11 Net	vork Agent					_
	📓 Kaspersky Sec	urity Center 11 Ne	twork Agent			Kaspersky Security Cente	r 11 Network Agent	Not
				Act	ive policy	y		
				Cor Exp	mpare po ort	licy to another policy		
				All	tasks		•	
				Gro	up by co	lumn	•	
				Cut Cop	у			
	•			Exp	ete ort list			Þ
				Pro	perties			

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

File Action View Help										
🗢 🔿 🔁 🖬 📋 🖾 🔍 🖬										
Kaspersky Security Center 11     Administration Server WIN-R2FGT0TNH3K     Administration Server WIN-R2FGT0TNH3K     Managed devices     Sup SIMCO     SIMCO	Administration	<u>ı Server WIN-</u>	- <u>R2FGT0TNH</u>	<u>3K</u> > Mana	ged devices					
Device selections     Quantum Unassigned devices	Devices	Policies	Tasks							Group properties
<ul> <li>⇒ Policies</li> <li>Tasks</li> <li>Tasks</li> <li>Kaspersky Lab Licenses</li> <li>Madvanced</li> </ul>	New policy	Import policy	y from file	Add/Remove	<u>columns</u>					Refresh
	Name	· · · · · · · · · · · · · · · · · · ·		Status	Application		Inhe	Kaspersky Sec	urity Center 1	1 Network×
	Kaspersky Secur	ity Center 11 Net	work Agent	A ativa	Kananda Saawita C	enter 11 Network Ameri	Net	Agent		
	Aspersky sector	unty Center 11 re	itti mi	Active	Kasperský security G	enter 11 Network Agern	NGL	Application: Created: Changed: Inherited policy:	Kaspersky Sec 11 Network A 5/21/2020 2:: 5/21/2020 2:: Not inherited Affecter Benfor success Details	urity Center gent 53:10 PM 53:31 PM d: 1 devices rcement ful: 1 devices
									Help - K	ASPERSKY

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

#### **Configuring KICS for Nodes instances**

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

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

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

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

- Import of the generic ("backbone") policy for **KICS for Nodes** from the **Generic\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp** file supplied as a part the distribution package.
- Remote installation of KICS for Nodes 2.6 onto the target hosts.
- Remote installation of **Hotfix** onto the target hosts<sup>7</sup>.
- Initial update of antivirus databases.
- Performing the **On-Demand** scanning on the target hosts.
- Execution of the Generate Rules for Application Launch Control task.
- Setting up Application Launch Control whitelisting.
- Setting up Device Control whitelisting.
- Setting up PLC Integrity Checker (if applicable).

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

#### Creation of the generic policy for KICS for Nodes

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

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



2. Using the file browser, go to the distribution package and locate the **Generic\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp** file as shown below. Click **Open**.

	· -		-	-
ganize 🔻 🛛 New fold	ler			
📙 KL_Distributives 🔦	Name	Date modified	Туре	Size
	HotFix	5/20/2021 1:46 AM	File folder	
• OneDrive	KICS4NODES	5/20/2021 1:47 AM	File folder	
	📙 KSC	5/20/2021 1:46 AM	File folder	
This PC	📙 License	5/20/2021 1:46 AM	File folder	
🧊 3D Objects	Generic_policy-KICS4NODES_2.6_PCS7_9.1.klp	5/20/2021 1:46 AM	KLP File	72 KB
🔜 Desktop	KLNagent_policy-KICS4NODES_2.6_PCS7_9.1.klp	5/20/2021 1:46 AM	KLP File	8 KB
🔮 Documents				
🕹 Downloads				
👌 Music				
Nictures				
📑 Videos				
Local Disk (C:)				
Local Disk (D:)				
blatanada 🗸				
NetWOrk *				

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

Kaspersky Security Center 11							
File Action View Help							
🗢 🤿 🔁 🗊 🤞 📋 🛪 🗉 🤉 🖬							
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> </ul>	Administration	Server WIN-	R2FGT0TNI	<u>H3K</u> > <u>Manac</u>	ged dev	r <u>ices</u> > SIMCO	
Device selections     Inassigned devices	Devices	Policies	Tasks			G	roup properties
?     Policies       Image: Tasks     Image: Tasks       Image: Tasks     Tasks       Image: Tasks	New policy	Import policy	r from file	Add/Remove c	olumns		<u>Refresh</u> ≣== ▼
	Name	*			Status	Application	Inherited
	Kaspersky Indust	trial CyberSecurit	y for Nodes 2.6	5			
	Generic - Kasp	ersky Industrial C	yberSecurity f	or Nodes 2.6		Kaspersky Industrial CyberSecurity for Nodes 2.6	Not inherited
	Kaspersky Securi	ity Center 11 Netw urity Center 11 Net	work Agent —	11	Active	Kaspersky Security Center 11 Network Agent	Inherited fro
	•			111			
						Help <b>v</b> KA	A)PER)KY
Policies: 2							

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



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

#### Settings of KICS for Nodes generic policy

This chapter highlights some important settings of the **Generic\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp** policy that deviate from the default policy configuration. In general, the following features have been modified so that their settings are different from those of a newly created **KICS for Nodes** policy:

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

K Real-time file protection ? X	K Real-time file	e protection <b>? X</b>
General Protection scope Task management	General Protection scope Task mana	gement
Objects protection mode	Protection scope	<b>-</b>
Smart mode	Protection scope	Security level
On access and modification	Cocal hard drives	Custom
On access	🕑 🖑 Removable drives	Custom
O When run		
Heuristic analyzer		
✓ Use heuristic analyzer		
· · ·		
Light Medium Deep		
Integration with other components		
Apply Trusted Zone		
Use KSN for protection		
Block access to network shared resources for the nodes that show malicious activity		
KSN will be used for protection only when the KSN Usage task runs.	Configure Add	Edit Remove
OK Cancel		OK Cancel

K Real-time	file protection settings	?	X
General Actions Performance			
Objects protection			
Ohjects     Ohjects			
Objects scanned by format	t of ovtancions spacified in anti-virus d	atabaco	
	t of extensions specified in anti-virus of	atabase	
Objects scanned by specified list	t of extensions:		
		Edit	
✓ Scan disk boot sectors and MBR			
✓ Scan alternate NTFS streams			
Performance:			_
Protect only new and modified fi	iles		
			_
Compound objects protection:			
Archives	Packed objects		
Email databases	Find entail     Embedded OLE objects		
	Se	curity level	
		curry level.	·
	OK		ancol
	UK		ancer
K Real-time	file protection settings	?	X
K Real-time	file protection settings	?	X
K Real-time	file protection settings	?	X
K Real-time	file protection settings	?	x
K Real-time	file protection settings	?	×
K Real-time	file protection settings	<b>?</b> Edit	×
	file protection settings	<b>?</b> Edit	×
K Real-time	file protection settings	Edit	X
	file protection settings	Edit	X
Real-time      General Actions Performance      Exclusions      Exclude files:      Do not detect:      Advanced settings	file protection settings	Edit	X
	file protection settings	<b>?</b> Edit Edit	X
	than (sec.): arger than (MB):	Edit           Edit           60           8	
K Real-time      General Actions Performance      Exclusions      Exclude files:      Do not detect:      Advanced settings      ✓ Stop scanning if it takes longer t      ✓ Do not scan compound objects I      ✓ Use iSwift technology	than (sec.): arger than (MB):	Edit           Edit           60         \$	
K       Real-time         General Actions       Performance         Exclusions	than (sec.): arger than (MB):	Edit       Edit       60       \$\$\screwthin\$\$       8       \$\$\screwthin\$\$\$	
K       Real-time         General Actions       Performance         Exclusions	than (sec.): arger than (MB):	Edit       Edit       60       v       8       v	
General Actions Performance   Exclusions Exclusions   Exclude files:   Do not detect:   Advanced settings   Stop scanning if it takes longer time   Do not scan compound objects I   Use iSwift technology   Use iChecker technology	than (sec.): arger than (MB):	₹	
Real-time   General Actions Performance   Exclusions Exclude files:   Do not detect: Do not detect:   Do not detect: Do not scan compound objects I   Vois iSwift technology Use iChecker technology	than (sec.): arger than (MB):	Edit Edit 60	
K       Real-time         General Actions       Performance         Exclusions       Exclude files:         Do not detect:       Do not detect:         Void       Void         Advanced settings       Stop scanning if it takes longer to         Void       Do not scan compound objects if         Void       Use iSwift technology         Void       Use iChecker technology         Information       The Trusted Zone is applied this tab, Trusted Zone exclusion	than (sec.): arger than (MB): within this task. In addition to exclusion	Edit	X
K       Real-time         General Actions       Performance         Exclusions	than (sec.): arger than (MB): within this task. In addition to exclusion sions are also taken into account.	Edit	X
General Actions Performance   Exclusions Exclusions   Exclude files:   Do not detect:   Do not detect:   Use iStop scanning if it takes longer to   O no not scan compound objects I   Use iSwift technology   Use iChecker technology   Information   The Trusted Zone is applied this tab, Trusted Zone exclusion	than (sec.): arger than (MB): within this task. In addition to exclusion sions are also taken into account.	Edit	X
Real-time     General Actions     Performance     Exclusions   Exclude files:   Do not detect:     Do not detect:     Void Do not detect:     Void Do not detect:     Void Do not detect:     Void Do not can compound objects I     Void Use iSwift technology     Void Use iSwift technology     Information     The Trusted Zone is applied   this tab, Trusted Zone exclusion	than (sec.): arger than (MB): within this task. In addition to exclusion sions are also taken into account.	Edit	X
Ceneral Actions Performance     Exclusions   Exclude files:   Do not detect:     Advanced settings   Stop scanning if it takes longer the state of the	than (sec.): arger than (MB): within this task. In addition to exclusion sions are also taken into account.	Edit	x
Real-time     General Actions     Performance     Exclusions     Exclude files:     Do not detect:     Do not detect:     Advanced settings     Yop scanning if it takes longer to     Do not scan compound objects I     Use iSwift technology     Yuse iChecker technology   Information   The Trusted Zone is applied this tab, Trusted Zone exclusion	than (sec.): arger than (MB): within this task. In addition to exclusion sions are also taken into account.	Edit	

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

K	Exploit Prevention	?	X
Γ	xploit Prevention settings Protected processes		
	Exploit prevention mode		
	○ Terminate on exploit		
	Use the mode to terminate process if it is tried to be abused. Critical system processes are terminated.	never	
	Only notify about abused process		
	Use the mode to inform about process that has been abused. The application informs you viewents.	a the	
	Preventing actions		
	Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled		
L			
	ОК	Ca	ancel

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

nile generating allowing rules	If the certificate is missing, us
Use digital certificate subject and thumbpri	nt SHA256 hash
Use SHA256 hash Generate rules for user or group of users:	
Everyone	Browse
Principle of adding: Replace ex	isting rules
The allowing rules will be exported to a file.	
Add protected device details to file name	
C:\SWInventory\SWInventory.xml	Browse

K Applications Launch Control	x
General Software Distribution Control Task management	
Schedule settings	Ь
- Task start	
Advanced           Task will be performed according to the local time on the computer.	
OK Cance	el

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

K Device Control	K Device Control ? X
General Task management	General Task management
Task mode         Statistics Only         ✓         Allow using all mass storage devices when the Device Control task is not running         Rules list         Total rules: 0.	Schedule settings   Run by schedule  Frequency: At application launch  Task start
	Advanced          Task will be performed according to the local time on the computer.
OK Cancel	OK Cancel

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

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

K			Anti-Cryptor		? X
General	Protection scope	Exclusions	Task management		
Task O S A	mode tatistic only pply this mode to re	egister share	ed folders encryption ev	rents in the Anti-Cryptor task	logs.
A A U	ctive pply this mode to ir oon detecting encry	nmediately b ption activity	plock access to the shar /.	ed folders for active user's s	ession
Heuri	stic analyzer				-
<b>v</b> U	se heuristic analyze	er			
-					
Light			Medium		Deep
				ОК	Cancel



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

K Removable Drives Scan ? X
Removable Drives Scan
Scan on connection
Scan removable drives on connection via USB
Scan removable drives if its stored data volume
Scan with security level:
Maximum protection
OK Cancel

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

K Log Ir	nspection 📃 🗖 🗙	K Log Inspection – 🗖 🗙			
Custom rules Predefined rules Task mar	nagement	Custom rules Predefined rules Task management			
Custom rules list		Predefined rules list			
Apply custom rules for log inspection	n	Apply predefined rules for log inspection			
Rule name	Windows Event Log ID's	Select predefined rules from the list below to analyze log files basing on built-in heuristics:			
Application popup detection	26				
A service was installed in the sy	7045	Rule name			
<ul> <li>A service was installed in the sy</li> </ul>	601	There are patterns of a possible brute-force attack in the system			
<ul> <li>A scheduled task was created</li> </ul>	4698, 602	✓ There are patterns of a possible Windows Event Log abuse			
		<ul> <li>Atypical actions detected on behalf of a new service installed</li> </ul>			
		Atypical logon that uses explicit credentials detected			
		✓ There are patterns of a possible Kerberos forged PAC (MS14-068) atta			
		Atypical actions detected directed at a privileged built-in group Adminis			
		There is an atypical activity detected during a network logon session			
Add Modify	Pomovo	Advanced cettings			
Add	Remove	Auvanced settings			
L					
	OK Cancel	OK Cancel			

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

Notify users:	
By using terminal service	
By using Windows Messenger Service command	Message text

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

K	Administration Server Network lists	? X
	Interaction with Administration Server Inform Administration Server about the following data types:	
	<ul> <li>Quarantined files</li> <li>Backed up files</li> <li>Blocked hosts (Are shown in unprocessed objects on KSC side)</li> <li>Available Wi-Fi networks</li> <li>Versions of PLC projects</li> </ul>	
	ОК	Cancel

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

K Incidents	x
Select events for which the application will generate incidents on the side of Kaspersky Security Center	
PLC project does not match reference project	
Error matching PLC project to reference project	
Error getting PLC project information	
License has expired	
End User License Agreement has been violated	
Failed to update	
Application database is corrupted	
Application database is extremely out of date	
Application database is out of date	
Integrity of software modules is corrupted	
Host listed as untrusted	=
Application launch denied	
Statistics only mode: application launch denied	
Error processing application launch	
Untrusted external device detected and restricted	
Statistics only: untrusted external device detected	
Error processing device connection	
Infected or other object detected	
KSN-untrusted object found	
Probably infected object detected	
Object not disinfected	
Object not backed up	-
Dhiert not quarantined	
OK Cancel	

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

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

# Remote installation of KICS for Nodes onto target computers via KLnagent

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

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

File Action View Help					
🗢 🔿 🗡 📰 🐇 📋 🗙 🖬 🔽 🥫					
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> </ul>	Administration Server	WIN-R2FGT0T	<u>NH3K</u> > <u>Manager</u>	<u>d devices</u> > SIMCO	
Mobile Device Management     Device selections     Inassigned devices	Devices Polic	ies Tasks			
→ Policies [1] Tasks [5] Kaspersky Lab Licenses [6] Advanced	Move devices to group	New group	Perform actio	Add/Remove columns	
	No filter specified,	records total:	1 Search by text	t columns	
	Select statuses: <b>Crit</b> The records total above include selected group.	ical: 1 🗸 Warn	ning: 0 <b>OK: 0</b> vices with the specified st	tatus. These devices are in the specified gro	up and any of it
	Name	Last connecte	Network Agen R	eal-time protection Created	
	SIMCO	1 minute ago	Ves	One day ago	
				Events	
				Install application	
				Check device accessibility	
				Connect to device	
				Connect to Remote Desktop	
				Custom tools	
				All tasks	
				Refresh	
				Export list	
Groups: 0, devices: 1				Properties	



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

	Remote Installation Wizard		
3	Select installation package		
	Taspersky Security Center 11 Network Agent (11.0	.0.1131)	
	Kaspersky Security Center 11 Network Agent (11.0.0.1	1131)	
		New	Properties
			Next Cancel

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

_		and March	×
0	New Package	: Wizard	
	Select install	ation package type	
		Create installation package for a Kaspersky Lab application	
		Create installation package for specified executable file	
		Select an application from Kaspersky Lab database to create an installation package	
			Cancel

4. Give a name to the newly created installation package (KICS4NODES\_X64\_ENG, in our case). Click Next.

9	New Package Wizard	
	Defining installation package name	
	Name:	
	KICS4NODES_X64_ENG	
		Not Concel
		Livext Cancel

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

Organize 🔻 New folde	er			· · ·
Desktop	Name	Date modified	Туре	Size
Downloads	kics.kud	22.06.2018 12:47	KUD File	10 KB
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>□ Music</li> <li>□ Pictures</li> <li>□ Videos</li> <li>■ Computer</li> <li>▲ Local Disk (C:)</li> <li>□ Shared Folders (</li> </ul>				
Ele el	and the bad		Karperbul	ab application derc

Page 58 of 161



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



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



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



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

File Action View Help			
🗇 🧼 🖄 📰 🗐 🖾 🧟 🛛 🖬 😻			
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> <li>Device selections</li> </ul>	Administration Server WIN-R2FGT0TNH3	K > <u>Advanced</u> > <u>Remote installation</u> > Installation pac te deployment.	kages
↓ Unassigned devices ✓ Policies Tasks → Kaspersky Lab Licenses ▲ ↓ Advanced	Create installation package View the list of Add/Remove columns	of stand-alone packages Additional actions 🔻	Ver
Luser accounts	Kasparslav Sasurity Cantor 11 Naturaly Agent (11)	Application	11.0
<ul> <li>Application management</li> <li>Remote installation         <ul> <li>Installation packages</li> <li>Data encryption and protection</li> <li>Q Device discovery</li> <li>Deleted objects</li> <li>Repositories</li> </ul> </li> </ul>	Kaspersky Security Center 11 Network Agent (11.0)           KICS4NODES_X64_ENG	0.0.1131)       Kaspersky Security Center 11 Network Agent         Kaspersky Industrial CyberSecurity for Nodes 2.6         Install application         Create stand-alone installation package         Show the list of stand-alone packages         Group by column         Delete         Export list         Properties	11.0

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

Properties: KICS4NODES_X64_E	NG 🖂 🔍 💌 💌
Sections	Settings
General	Components to install:
Settings Key Revision history	Real-Time File Protection         On-Demand Scan         KSN Usage         Exploit Prevention         Applications Launch Control         Device Control         Wi-Fi Control         Figure Magazement
	<ul> <li>Anti-Cryptor</li> <li>PLC Project Control</li> <li>File Integrity Monitor</li> <li>Log Inspection</li> <li>Integration with Kaspersky Security Center</li> <li>Performance Counters</li> <li>SNMP protocol support</li> <li>Command Line Utility</li> <li>System Tray Icon</li> </ul>
	Destination folder:       %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\         Advanced installation settings         Scan computer for viruses before installation         Ø Enable real-time protection after installation of application         Ø Add Microsoft recommended files to exclusions list         Ø Add Kaspersky Lab recommended files to exclusions list         Configuration file
Help	OK Cancel Apply

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

Properties: KICS4NODES_X64_ENG		And in case of the local division of the	
Sections	Кеу		
General			
Settings	1E54-00076B-572BFFDC.k	ey	Browse
Key			
Revision history	Key: Application information: End date of key validity period: License type: Restriction: Service information:	1E54-00076B-572BFFDC Kaspersky Industrial CyberSecurity for 17.05.2019 Commercial. 5	or Nodes, Server Russian Edition. 5-9 Node
Help		OK	Cancel Apply

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

File Action View Help					
🗢 🔿 📶 🖾 🍳 🔽 📷					
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> <li>Device selections</li> </ul>	Administration Server WIN-R Installation package Installation packages listed below are	2FGT0TNH3K > Advar S used for remote deploym	nced > <u>Remote installation</u> : ent.	> Installation pa	ickages
☐ Unassigned devices ➢ Policies ☐ Tasks ☐ Kaspersky Lab Licenses ▲ Advanced	Create installation package	View the list of stand-alc	Additional a	actions 💌	
L User accounts	Name		Application		Vers
Application management	🧮 Kaspersky Security Center 11 Netv	vork Agent (11.0.0.1131)	Kaspersky Security Center 11 Net	work Agent	11.0
Remote installation	E KICS4NODES_X64_ENG		Kaspersky Industrial CyberSecuri	ty for Nodes 2.6	2.6.(
Installation packages		Install applicati	on		
<ul> <li>▶ ➡ Data encryption and protection</li> <li>▷ Q. Device discovery</li> <li>□ Deleted objects</li> <li>▶ ➡ Repositories</li> </ul>		Create stand-al Show the list of	lone installation package f stand-alone packages		
		Group by colur	110 <b>P</b>		
		Delete			
		Export list			
		Properties			
				·	

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



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

C Remote Installation Wizard	×
Select devices for installation	
Managed devices     SIMCO     SIMCO     KSC     Unassigned devices	Add If no relevant devices are displayed in the list, dick Add to type their names or IP addresses.
	Next Cancel

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

0	Remote Installation Wizard	
	Defining remote installation task settings	
	Force installation package download          Image: Second structure       Image: Second structure         Image: Second structure	
	Behavior for devices managed through other Administration Servers <ul> <li>Install always</li> <li>Install only on devices managed through this Administration Server</li> </ul>	
	Do not re-install application if it is already installed	
	Next	incel

G	Remote Installation Wiza	rd
	Key properties	
	Key with settings has been f	ound in the package:
	Key:	1E54-000768-5728FFDC
	Application information:	Kaspersky Industrial CyberSecurity for Nodes, Server Russian Edition. 5
	End date of key validity	17.05.2019
	License type:	Commercial.
	Restriction:	5
	Service information:	
	We do not recommend that read access is shared by def	you distribute the key using this method because the package repository ault.
	If you want to replace or de	ete the key, open the <u>package properties</u>
		Next Cancel

16. We have picked the license file before. Verify the terms once again and, if you agree, click Next.

17. In the windows that appears, apply the settings as shown below. Click Next.



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

$\bigcirc$	Remote Installation Wizard	
	Select accounts to access devices	
	No account required (Network Agent installed)	
	Account required (for installation without Network Agent)	
	Add accounts with administrator rights on the devices where the applical domain controller for installation through Active Directory.	tion is to be installed or on the
		Add
		Properties
		Next Cancel

19. In the Starting installation window just click Next.



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

0	Remote Installation Wizard	
	Starting installation	
	The deployment has successfully started.	
	Opployment task created	
	Opployment task started	
	The remote installation task has been started successfully. To view the task progress, go to the Tasks folder. Tasks folder. Click Finish to proceed to the general list of tasks.	
	F	inish

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



22. Wait until the installation task is completed<sup>8</sup>. Make sure that the task **execution statistics** are displayed as **Completed on ... devices** and the chart has turned green.



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

me	Device	Status	Description			Group
i) 5/21/2020 4:43:30 PM	Administration Server <simco></simco>	Completed	Installation compl	eted successfu	lly.	SIMCO
Administration Serve	<simco></simco>					
lime	Status D	escription		Regi	Name of virtual Administr	ation Server
	Completed In	nstallation completed succe	essfully.	5/2		
5/21/2020 4:43:30 PM	Running S	etup started.		5/2		
5/21/2020 4:43:30 PM 5/21/2020 4:38:43 PM		Copying files to the specifie	d device	5/2		
5/21/2020 4:43:30 PM 5/21/2020 4:38:43 PM 5/21/2020 4:37:24 PM	Running C			5/2		
<ul> <li>5/21/2020 4:43:30 PM</li> <li>5/21/2020 4:38:43 PM</li> <li>5/21/2020 4:37:24 PM</li> <li>5/21/2020 4:36:40 PM</li> </ul>	Running C Scheduled V	Vaiting for connection				
5/21/2020 4:43:30 PM     5/21/2020 4:38:43 PM     5/21/2020 4:37:24 PM     5/21/2020 4:36:40 PM     5/21/2020 4:36:39 PM	Running C Scheduled V Scheduled	Vaiting for connection		5/2		
5/21/2020 4:43:30 PM 5/21/2020 4:38:43 PM 5/21/2020 4:38:43 PM 5/21/2020 4:37:24 PM 5/21/2020 4:36:40 PM 5/21/2020 4:36:39 PM 5/21/2020 4:36:38 PM	Running C Scheduled V Scheduled Scheduled	Vaiting for connection		5/2 5/2		

<sup>&</sup>lt;sup>8</sup>A remote installation task may take up to 15 minutes depending on the performance of the target PC. Page **70** of **161** 

#### Remote installation of Hotfix onto target computers via KLnagent

At the time, we are writing this installation and deployment guide; the actual **Hotfix** version is **critical\_fix\_core\_12<sup>9</sup>**. However, you are likely to receive the installation package with a newer **Hotfix**. Since the **Hotfix** installation procedure remains the same regardless of the version, we recommend that you always follow the steps described below. Every **Hotfix** is cumulative as it incorporates all the previous patches and improvements. Conversely, there is no need to uninstall the previous **Hotfixes** (if already installed) before installing the newest one.

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

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

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



<sup>&</sup>lt;sup>9</sup> As of the date we are revising this document, **Hotfix 12** is the most recent version. We strongly recommend that you use **Hotfix 12** and no other version, even if a subsequent version has become available.
2. In the Select installation package type window, click Create installation package for specified executable file.

New Package Wizard	×
Select installation package type	
Create installation package for a Kaspersky Lab application	
Create installation package for specified executable file	
Select an application from Kaspersky Lab database to create an installation package	I
	Cancel

In the window that appears, give the Hotfix package a name (in our case, we are about to install Hotfix 12<sup>10</sup>). Click Next.

-

		×
÷	New Package Wizard	
	Defining the installation package name	
	Name:	
	HOTFIX12_x64	]
	<u>N</u> ext Can	cel

<sup>&</sup>lt;sup>10</sup> Most likely, you have received a newer version of the **KICS for Nodes Hotfix**. Page **73** of **161** 

4. In the Selecting the distribution package for installation window, browse to the Hotfix<sup>11</sup> 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.

		×
←	New Package Wizard	
	Selecting the distribution package for installation	
	C:\Users\E5_U5ER\Desktop\KL_Distributives\HotFix\critical_fix_c Browse	
	Executable file command line (optional):	
	DISCLAIMER=1	
	Copy entire folder to the installation package	
	<u>N</u> ext C	ancel

<sup>&</sup>lt;sup>11</sup> You should mind suffixes **X64** and **X86** in the names of **Hotfix** installation files. The installation file must match the target operating system you are planning to install **Hotfix** onto.



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



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



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



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

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



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

📧 Kaspersky Industrial CyberSecuri	ty for Nodes 2.6 settings	(r	—		$\times$
Sections	General				
General	Kanavalu, Taskustvial Cultar Saura	ity for Modes 2.6			
Application settings	Kaspersky Industrial Cyberbecur	ity for Nodes 2.6			
Supplementary					
Real-Time Computer Protection	Version number:	2.6.0.767			
Logs and notifications	Installed:	4/29/2021 12:0	)8:35 PM		
Malfunction diagnosis	Current status:	Running			
Components	Last software update:	5/19/2021 8:52	2:50 PM		
License keys	Installed undates:				
Event configuration	Critical Fix Core 12;				
Advanced	Application detections				
	Application databases	E/10/2021 E/05			
	Database uate;	2/19/2021 3:00	):UU PM		
	Number of anti-virus records:	16615128			
	Last updated:	2114/2021 8:24	2:50 PM		
			_		
	Start	Stop			
Hala	I				
<u>neip</u>		ОК	Cancel	Apply	

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

File Action View Help								
🔶 🔿 📶 🦧 📋 🗙 🖬 🖉 📷								
Kaspersky Security Center 11  Administration Server WIN-R2FGT0TNH3K  Managed devices  SIMCO	Administration	Server WIN	-R2FGT0TNF	<u>+3K</u> > <u>Man</u>	aged de	<u>evices</u> > SIMCO		
Mobile Device Management     Device selections     Unassigned devices     Policier	Devices	Policies	Tasks					Group properties
Tasks Tasks Advanced User accounts	New policy	Import policy	y from file	Add/Remov	<u>a columns</u>	5		Refresh
Application management     P. Remote installation     Installation packages     Data encryption and protection	Name Kaspersky Indust	trial CyberSecuri	ity for Nodes 2.6	5	Status	Application	Generic - Kasp CyberSecurity	oersky Industrial × • for Nodes 2.6
Q Device discovery ☐ Deleted objects	Generic - Kaspe Kaspersky Securi	ersky Industrial ( ity Center 11 Ne	CyberSecurity fo twork Agent —	or Nodes 2.6	Active	Kaspersky Industrial CyberSecurity for Nodes 2.6	Application:	Kaspersky Industrial CyberSecurity for Nodes 2.6
Repositories	🖹 Kaspersky Secu	ırity Center 11 N	etwork Agent		Active	Kaspersky Security Center 11 Network Agent	Created: Changed: Inherited policy:	5/21/2020 3:23:58 PM 5/21/2020 3:29:22 PM Not inherited
	٢		m			,		Affected: 1 devices Enforcement successful: 1 devices Details
								Help - KASPERSKY
Policies: 2								

#### **Rule generation optimization for Application Launch Control**

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

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

1. Create a batch file with the following contents:

```
@echo off
set exclusion="C:\Program Files (x86)\SIEMENS\STEP7\s7hlp\*.js"
setlocal enableextensions enabledelayedexpansion
```

```
reg query
```

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.6\Environment" >nul
if %errorlevel% equ 1 goto OUTNOW
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.6\Environment" /f /v
ALCRuleGenExclusions /t REG_MULTI_SZ /d %exclusion%
:OUTNOW
exit
```

2. Save the file as AddGenerateExclusions.bat.



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



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





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

÷	New Package Wizard	×
	Selecting the distribution package for installation	
	::\Users\ES_USER\Desktop\AddGenerateExclusions.bat Browse	
	Executable file command line (optional):	
	Copy entire folder to the installation package	
	Next Ca	ancel

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



7. Let us suppose, we have Simatic Manager installed on the ES\_WIN10 engineering workstation. As was mentioned before, we need to run AddGenerateExclusions.bat to optimize rule generation on that workstation. So, we should go to the ES\_WIN node, right-click on it and choose Install application from the context menu.





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

	N			
	Remote Installation Wizar			
S	elect installation package			
	74000			_
	AddGenerateExclusions			^
	<		>	~
	AddGenerateExclusions			
		N <u>e</u> w	Properties	
			<u>N</u> ext Ca	ncel

9. Preserve the default settings and click Next.





10. Proceed with the default settings as shown below.





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



#### Initial update of antivirus databases

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

• By letting the **KSC** server retrieve updates from the Kaspersky Lab update sources available on the Internet and by performing databases propagation to **KICS for Nodes** devices directly from the **KSC** repository. This requires that your **KSC** server should be connected to the Internet.

• By letting **KICS for Nodes** devices retrieve updates directly from the Kaspersky Lab update sources available on the Internet. This scheme does not utilize **KSC** but it requires that every **KICS for Nodes** device be able to access the Internet.

• By manual retrieval of updates from the Internet using **Kaspersky Update Utility**. It enables you to store the updates on some intermediary file server (located in DMZ, for example). Once the updates are available on the secure file server, you can tell **KICS for Nodes** devices to retrieve updates from that file server.

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

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

🧼 End User License Agreement and Privacy Policy — 🗆 🗙
End User License Agreement and Privacy Policy
Kaspersky Update Utility 3.0 MR2 END USER LICENSE AGREEMENT;  AND
Products and Services PRIVACY POLICY
KASPERSKY LAB END USER LICENSE AGREEMENT ("LICENSE AGREEMENT")
IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.
CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY THAT YOU AS THE ORGANIZATION FOR
WHICH THE SOFTWARE IS DOWNLOADED OR ACQUIRED HAVE
☐ I confirm that I have fully read, understand, and accept the terms of the End User License Agreement
☐ I confirm that I have fully read, understand, and accept the terms of the Privacy Policy
Decline Accept



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



7. The following window should appear.

Kaspersky Update Utility	
Kaspersky Update Utility	KASPERSKY
Applications with updates downloading:	Applications
Start manually Last update date: Next update: Start manually	Schedule View download report
Start About the program Check for new version	Settings Exit

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

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



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

🎯 Kaspersky Update Utility	- 🗆 X
Kaspersky Update Utility	KASPERSKY
Applications with updates downloading:	Applications
Kaspersky Industrial CyberSecurity for Nodes 2.6.0.785	
Start manually	Schedule
Last update date: 22.05.2020 at 14:29	View download report
Download certdb.dat.klz	13 %
Stop	Settings
About the program Check for new version	Exit

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

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

Administration Server WIN-LPJARCQOGPK	Administra	tion Server WIN-LPJARCO	QOGPK > Man	aged devices > SI	мсо				
<ul> <li>☐ Managed devices</li> <li>☐ SIMCO</li> <li>☐ Mobile Device Management</li> <li>☐ Device selections</li> </ul>	Group	o tasks							
Unassigned devices	Devices	Policie: Task							
7/ Policies	_								
Tasks	Create a ta	sk Import task from file	Add/Remove	e columns					
🖹 Kaspersky Lab Licenses									
Advanced									
Over accounts     Application management	Inherited tas	ks: hide   show							
▲ 모 Remote installation	1	*	1	La succession	N_	-	-	0	
Installation packages	Name		Application	l ask type	Status	Runn	Com	Com	Com
Data encryption and protection									
Q Network poll				1					
Repositories		Create +	Task						
		All tasks 🕨							
		View +							
		Group by column							
		Refresh							
		Export list							

13. In the Select the task type window, select Kaspersky Industrial CyberSecurity for Nodes 2.6-

>Database Update and press Next >.

Kabyersky industrial cycle becauty for nodes and         Activation of Application         Application Integrity Control         Baseline File Integrity Monitor         Copying Updates         Database Update         On-Demand Scan         Rule Generator for Applications Launch Control         Rule Generator for Device Control         Software Modules Update         Kaspersky Endpoint Security for Windows (11.2.0)         Add key         Change application components         Integrity check         Inventory         Manage Authentication Agent accounts         Update         Update         Update         Wipe data         Xespersky Security Center 11 Administration Server         Advanced         Fix vulnerabilities         Install application remotely         Install application remotely	- 🗖	Kaspersky Industrial CyberSecurity for Nodes 2,6
<ul> <li>Activities of Application</li> <li>Application Integrity Control</li> <li>Baseline File Integrity Monitor</li> <li>Copying Updates</li> <li>Distabase Update</li> <li>On-Demand Scan</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Applications Launch Control</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Wire data</li> <li>Wire data</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install application remotely</li> </ul>		Activation of Application
<ul> <li>Application antegray control</li> <li>Baseline File Integrativy Monitor</li> <li>Copying Updates</li> <li>Database Update</li> <li>On-Demand Scan</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Rix vulnerabilities</li> <li>Install application remotely</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Application Integrity Control
<ul> <li>Oddates</li> <li>On-Demand Scan</li> <li>On-Demand Scan</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Values Control</li> <li>Software Modules Update</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Avanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install application remotely</li> </ul>		Application Integrity Control
<ul> <li>Corporation</li> <li>Dotabase Update</li> <li>On-Demand Scan</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wire data</li> <li>Xaspersky Security Center 11 Administration Server</li> <li>Avanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Copying Lindates
<ul> <li>On-Demand Scan</li> <li>On-Demand Scan</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Software Modules Update</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Wire scan</li> <li>Wire data</li> <li>Softwared</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Database Lindate
<ul> <li>Alback of Database Update</li> <li>Rollback of Database Update</li> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Wire scan</li> <li>Wire data</li> <li>Xaspersky Security Center 11 Administration Server</li> <li>Avanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Dr-Demand Scan
<ul> <li>Rule Generator for Applications Launch Control</li> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Rotevine</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Rollback of Database Update
<ul> <li>Rule Generator for Device Control</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Rule Generator for Applications Launch Control
<ul> <li>Software Modules Update</li> <li>Software Modules Update</li> <li>Kaspersky Endpoint Security for Windows (11.2.0)</li> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Update</li> <li>Wirus scan</li> <li>Wre data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>In vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Rule Generator for Device Control
Image: State of Control		Software Modules Update
<ul> <li>Add key</li> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>	. 🗖	Kaspersky Endpoint Security for Windows (11.2.0)
<ul> <li>Change application components</li> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>✓ Kaspersky Security Center 11 Administration Server</li> <li>✓ Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Add key
<ul> <li>Integrity check</li> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Change application components
<ul> <li>Inventory</li> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Waspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		📋 Integrity check
<ul> <li>Manage Authentication Agent accounts</li> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Wipe data</li> <li>Z Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Inventory
<ul> <li>Update</li> <li>Update rollback</li> <li>Virus scan</li> <li>Wipe data</li> <li>Virus Scanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Manage Authentication Agent accounts
Update rollback  Virus scan  Kaspersky Security Center 11 Administration Server  Kaspersky Security Security Center 11 Administration Server  Kaspersky Security Security Center 11 Administration Server  Kaspersky Security Secu		Update
<ul> <li>Virus scan</li> <li>Wipe data</li> <li>Kaspersky Security Center 11 Administration Server</li> <li>Advanced</li> <li>Fix vulnerabilities</li> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		📋 Update rollback
Wipe data  Kaspersky Security Center 11 Administration Server  Kaspersky Security Center 11 Administration Server  Kaspersky Content of the server of the s		Virus scan
<ul> <li>☑ Kaspersky Security Center 11 Administration Server</li> <li>☑ Advanced</li> <li>iii Fix vulnerabilities</li> <li>iii Install application remotely</li> <li>iii Install Windows Update updates</li> </ul>	_	📋 Wipe data
	8 🔽	Kaspersky Security Center 11 Administration Server
Fix vulnerabilities  Fix vulnerabilities  Install application remotely  Install Windows Update updates	+	Advanced
<ul> <li>Install application remotely</li> <li>Install Windows Update updates</li> </ul>		Fix vulnerabilities
Install Windows Update updates		Install application remotely
		Install Windows Update updates



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

·	New Task Wizard	
5	Settings	
	5	
	Task creation method	
	New	
	$\bigcirc$ Import task created with Kaspersky Industrial CyberSecurity for Nodes	
	Configuration file:	
		Browse

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

New task wizard	
Update source	
Update source	
C Kaspersky Security Center Administration Server	
Kaspersky Lab update servers     Curters	
Custom HTTP or FTP servers, or network rolders	
Use Kaspersky Lab update servers if specified (Cu	istom HTTP or FTP servers, or network fold
	Connection settings
Disk I/O usage optimization	
Lower the load on the disk I/O	
RAM used for optimization 512	
	Ivext Can

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

Undata an u	K Llodate servers	? <b>X</b>
Opdate sour		
Kaspers	VKsc\c\$VLUpdates\Updates	Add
<u>Custom</u>		Remove
V Use Kas		Edit
		uttings
		Move up
Disk I/O usa		Move down
📃 Lower th	8	
RAM used f (MB):		
	OK	Cancel

17.Simply click Next in the Schedule window.

Schedule setting:	) hule	
Frequency:	After Administration Server has retrieved updates	Ŧ
	[	Advanced
Task will be	e performed according to the local time on the computer.	
Task will be	e performed according to the local time on the computer.	
A Task will be	e performed according to the local time on the computer.	

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

🚱 📕 New task wizard		
Selecting an account to ru	in the task	
Specify a user account ur	ider which you run the task.	
Automatically generated a	account	
Specify an account		
Account:	Administrator	
Password:	•••••	
Confirm password:	•••••	
		Next Cancel

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

K New task wizard	×
Define the task name	
Name: Database Update	
Next	Cancel
	Name:   Define the task name     Name:     Database Update

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



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

Administration Server KSC	Administration	Server KSC >	Managed devices > SIMCO					
Managed devices	🐨 Group ta	asks						
Device selections	Devices	Policies	Tasks					
<ul> <li>Tasks</li> <li>Advanced</li> <li>User accounts</li> <li>Application management</li> </ul>	Create a task	Import task	from file Add/Remove columns					
▲ 모 Remote installation Installation packages	Inherited tasks:	hide   show						
Q Network poll	Name	^	Application	Task type	Status	Runn	Detabase Us date	
Repositories	Rule Generator f	for Applications La	unch Control				Database Opdate	
	SIMCO - Rule	Generator for Ap	Kaspersky Industrial CyberSecurit	Rule Generator for Applications L	Completed	0	Task type:	Database Update
	On-Demand Sca	an					Application:	Kaspersky Industrial CyberSecurity for Nodes
	On-Demand S	ican	Kaspersky Industrial CyberSecurit	On-Demand Scan		0		
	Database Update	e					Running: 18%	
	Database Upda	ate	Kaspersky Industrial CyberSecurit	Database Update	Running (18%	1		
								Execution statistics on devices Running on 1 devices View results
								Stop
							Configure task     Export task to file     Delete task	

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





Kaspersky Industrial CyberSecuri	ty for Nodes 2.6 settings				
Sections	General				
General	Macaurola a Taduebial Cudar Shouebia Far Modae, 7, 5				
Application settings	vaspersky industrial cybersecurity for nodes zio				
Supplementary					
Real-Time Computer Protection	Version number:	2.6.0.785			
Logs and notifications	Installed:	5/21/2020 4:39:12 PM			
Malfunction diagnosis	Current status:	Running			
Components	Last software update:	5/22/2020 3:22:58 PM			
Keys	Installed updates:				
Event configuration	ent configuration Critical fix core 9;				
Advanced	And the database				
	Application databases				
	Database date:	5/22/2020 9:37:00 AM			
	Number of anti-virus records:	14826120			
	Last updated:	5/22/2020 3:22:58 PM			
	Start	Chan			
Help	Juix	OK Cancel Anniv			

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

#### **Performing On-Demand Scanning on target hosts**

Once we the antivirus databases are up to date, it is highly recommended to configure and start the **On-Demand scan** task on the **SIMCO** host. This essential step aims to ensure that the target host will be free of any malicious software and that no malicious executables will later appear on the **Application Launch Control** white list. Apparently, the **On-Demand scan** requires some additional processing resources and may slightly deteriorate computer performance. That is why we recommend that you start this task only in the manual mode in order to be able to supervise its execution.

Please perform the following steps to configure the scanner:

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

Administration Server WIN-LPJARCQOGPK   Managed devices   SIMCO  Mobile Device Management	Administration	<u>Server WIN-LF</u> Isks	PJARCQO	GPK > Mana	ged devices > SIMCO
Device selections     Inassigned devices	Devices	Policies	Tasks		
<ul> <li>Policies</li> <li>Tasks</li> <li>Kaspersky Lab Licenses</li> <li>Advanced</li> <li>User accounts</li> <li>Application management</li> </ul>	Create a task	Import task fr	rom file	Add/Remove	<u>columns</u>
	Inherited tasks:	hide   show			
▲ 모 Remote installation	Name	^	1	Application	Task type
Data encryption and protection	Database Update				
<ul> <li>Q Network poll</li> <li>Repositories</li> </ul>	📋 Database Upda	ate		Kaspersky Ind	Database Update
		Create		▶ Task	
		All tasks		•	
		View Group by column		*	
		Refresh Export list			

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





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

			x
G	New Task Wizard		
	Settings		
	settings		
	Task creation method		
	New		
	$\bigcirc$ Import task created with Kaspersky Industrial CyberSecurity for Nodes		
	Configuration file:		
		Browse	
		Next Cance	-
			_

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



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

curity level	
Security level	
Maximum performance	•
Plaxman performance	
	Settings
scans, excluding certain hie types from the sca security level is set, the application: - Scans files by format - Scans new and modified files only - Scans disk boot sectors and MBR - Scans alternate NTFS streams - Scans only new self-extracting archives - Scans only new packed files - Scans only new embedded OLE files	an scope. If the Maximum Performance

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

neral	Actions	Performance					
Scan	objects						
0	bjects to s	scan:					
C	All objec	ts					
0	Objects :	scanned by forma	t				
C	) Objects	scanned according	to list of ext	ensions specif	ied in anti-	virus dati	abase
B	Objecto	ccanned by cnecif	Iad lict of avt	encione:			
0	Objects	scanned by specin	ieu list of ext	ensions:		10	Tarren
-	L						Edit
V Su	ubfolders						
SI SI	ubfiles						
So So	an disk bo	pot sectors and Mi	BR				
▼ Sc	an alterni	ate NTFS streams					
Perfo	rmance:						
So So	an only n	ew and modified fi	les				
Scan	of compo	und objects:					
V 4	archives	5	~	All packed ob	jects		
V 1	I SFX ard	hives		All plain email			
	l email da	itabases	~	All embedded	OLE object	ts	
						Security	level

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

Image: Construction of the second	Scan scope	Security level
Image: System memory     Custom       Image: Startup objects     Custom	Local rate drives     Systemroot% ( <subfiles>     %systemroot% (<subfiles>     %systemroot% (system32) (<subfiles>     %systemroot% (system34) (<subfiles) (<subfiles)="" (<subfiles<="" td=""><td>Custom</td></subfiles)></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles></subfiles>	Custom
Startup objects Custom	System memory	Custom
	Startup objects	Custom

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

				×
🔶 New task v	vizard			
Ontinus				
Options				
-Heuristic analy:	zer			
Use heuris	tic analyzer			
		Y		1.1
Light		Medium		Deep
- Integration wit	h other components			
	ted Zone			
Perform ta	sk in background mode			
Consider ta	ask as critical areas scan			
Use KSN fo	r scanning			
			Next	Cancel



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 v	
Task will be performed according to the local time on the computer.	Advanced
	Next Cancel

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

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

New task wizard		
Selecting an account to run the	task	
Specify a user account under whic	h you run the task.	
Automatically generated account	:	
○ Specify an account		
Account:		
Password:	•••••	
Confirm password:	•••••	
		Next Cancel



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

📀 New t	task wizard	X
Define th	he task name	
Name:		
On-Dema	and Scan	]
	Next Can	<del>Act</del> iv

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

۲	New task wizard		X
	Finish creating the task		
	Click the Finish button to create "On-Demand Scan" and complete the Wizard.		
	Run task after Wizard finishes		
		Finish	Cancel div

Page 102 of 161

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

Administration Server WIN-LPJARCQOGPK	Administration Server WIN-LPJARCQ	OGPK > Mana	ged devices > SIMCO					
A 🖵 Managed devices	0.0.1.1							
SIMCO	Group tasks							
Mobile Device Management								
Device selections	Devices Policies Tasks							
Unassigned devices								
7 Policies		-						
Tasks	Create a task Import task from file	Add/Remove	columns					
Kaspersky Lab Licenses								
Advanced								
L User accounts	The standard of Fide 1 stress							
Application management	Innerited tasks: hide   snow							
A 모 Remote installation	Name	Application	Task type	Status	Runn	Com	Com	Com
Installation packages	Database Update							
Data encryption and protection	Database Undate	Kaspershy Ind	Database Undate		0	0	0	0
Paparitariar		Ruspersky man	butubuse opuate		Č.	Č.		Ŭ
	On-Demand Scan				5210			
	On-Demand Scan	Kaspersky Ind	On-Demand Scan		0	0	0	0
				Start				
				Stop				
				Pause				
				Resume				
				Results				
				All tasks		•		
				Group by co	lumn	+		
				Cut				
				Conv				
				Delate				
				Delete				
				Export list				
				Properties				

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

#### **Execution of the Generate Rules for Application Launch Control task**

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

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

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

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

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

Administration Server WIN-R2FGT0TNH3K	<u>Administratio</u>	on Server \	WIN-R2FGT0TN	<u> NH3K &gt; Managed</u>	devices > SIMCO
Managed devices     If SIMCO     Mahile Device Measurement		tasks			
In Mobile Device Management     If Mobile Device Management     If Device selections     If Unassigned devices	Devices	Policie	s Tasks		
<ul> <li>⇒ Policies</li> <li>☐ Tasks</li> <li>➡ Kaspersky Lab Licenses</li> <li>▲ Advanced</li> <li>▲ User accounts</li> <li>▶ ➡ Application management</li> </ul>	New task	Import ta	sk from file	Add/Remove columns	
▲ 모 Remote installation	Name		Application	Task type	Status
<ul> <li>A lata encryption and protection</li> <li>Q Device discovery</li> <li>□ Deleted objects</li> <li>▷ Repositories</li> </ul>	Database Upda Database Up On-Demand So On-Demand	ate date can Scan	Kaspersky Ind Kaspersky Ind	Database Update On-Demand Scan	Completed
		Create	•	Task	
		All tasks	•		
		View Group by	r column 🕨		
		Refresh Export lis	t		

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





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

	New Task Wizard	
	attings	
-	settings	
	Task creation method	
	New	
	Import task created with Kaspersky Industrial CyberSecurity for Nodes	
	Configuration file:	
		Browse

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

refix for rule names: S Allowing rules usage sco	IMCO ppe				
Create allowing rule	s based on running appl or applications from the f	ications folders:			
Scan scope C:\	EXE F		MSI	Scr	Add
5. In the following window, specify appropriate settings as shown in the example below. In our case, we have previously created the SWInventory folder on the C:\ drive of our SIMCO station. It is where the automatically generated rule list will be stored to as soon as the task finishes. In practice, you can specify any existing folder on a target host. Always select Use digital certificate and check Use digital certificate subject and thumbprint. Also, remember checking Add allowing rules to the list of Application Launch Control list. This option facilitates module configuration so that we will not need to deal with an XML-file import (although this file will still be created). Click Next.

While generating allowing rules		If the certificate is a	nissing user
Ose digital certificate		If the certificate is f	nissing, use:
Use digital certificate subject	t and thumbprint	SHA256 hash	•
OUse SHA256 hash			
Generate rules for user or group of	fusers:		
Everyone			Browse
Add allowing rules to the list of	Applications Launch C	ontrol rules	
Principle of adding	g: Merge with existin	ig rules	•
Principle of adding The allowing rules will be exported Add computer details to file i	g: Merge with existin to a file.	ig rules	•



6. In the Schedule window, simply click Next.

New task wizard	
Schedule	
Schedule settings	
Run by schedule	
Frequency: Hourly	T
Task start settings	
Every: 1 🚔 hour(s)	
Start time: 5:19 PM	
Start date: Friday , May 22, 2020 -	
	Advanced
<ul> <li>Task will be performed according to the local time on t</li> </ul>	he computer
	ne computer.
	Next Cancel

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

New task wizard		×
Selecting an account to run the	e task	
Specify a user account under whi	ch you run the task.	
Automatically generated account	t	
Specify an account		
Account:		
Password:	•••••	
Confirm password:	•••••	
		Next Cancel

Page 109 of 161

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

0	New task wizard	
	Define the task name	
	Name:	
	SIMCO - Rule Generator for Applications Launch Control	
	~	
		Next Cancel

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



Page 110 of 161

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

<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> <li>Device selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Kaspersky Lab Licenses</li> <li>Advanced</li> <li>User accounts</li> </ul>	Administration Server	WIN-R2FGT0TN	NH3K > Managed devices > SIMCO			Course and the
	Devices     Policies     Tasks       New task     Import task from file     Add/Remove columns					Refresh
<ul> <li>▲ 모 Remote installation</li> </ul>	Name	Application	Task type	Status		<b>^</b>
Installation packages     Data encryption and protection     Q Device discovery	Database Update	Kaspersky Ind	Database Update	Completed	SIMCO - Rule Generator for Applications Launch Control	Generator for ×
Repositories	On-Demand Scan On-Demand Scan Rule Generator for Applicat	and Scan Kaspersky Ind On-Demand Scan ator for Applications Launch Control		Application:		Applications Launch Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	SIMCO - Rule Generato	Kaspersky Ind	Rule Generator for Applications Launch Co	Running (6% completed)	Running: 6%	
						_
	٠ [			,		Execution statistics on devices Running on 1 devices View results
						Help - KASPERSKY
Tasks: 3						

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

#### Setting up Application Launch Control whitelisting

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

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

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

File Action View Help								
🗢 🏟   🚈 📰 🖌 📋   🗙 🖾 🛛 🖬								
<ul> <li>Kaspersky Security Center 11</li> <li>Administration Server WIN-R2FGT0TNH3K</li> <li>Managed devices</li> <li>SIMCO</li> <li>Mobile Device Management</li> <li>Device selections</li> <li>Unassigned devices</li> <li>Policies</li> <li>Tasks</li> <li>Kaspersky Lab Licenses</li> <li>Advanced</li> <li>User accounts</li> <li>Application management</li> </ul>	Administration Policies Devices	n Server WIN- Policies	R2FGT0TNH Tasks	<u>ł3K</u> > <u>Mana</u>	aged o	<u>levices</u> > SIMCO		
	New policy Inherited policies	Import policy	r from file	Add/Remove	<u>e colum</u>	<u>ns</u>		
▲ 모 Remote installation • Installation packages	Name	×			Status	Application		
Data encryption and protection	Kaspersky Industrial CyberSecurity for Nodes 2.6							
Q Device discovery	📔 Generic - Kasp	persky Industrial C	yberSecurity fo	or Nodes 2.6	Active	Kaspersky Industrial CyberSecu	rity for No	des 2
묘 Deleted objects ▷ 점 Repositories	Kaspersky Secur	rity Center 11 Net urity Center 11 N	work Agent —			Active policy Compare policy to another policy Export All tasks Group by column Cut Copy Delete Export list	•	ent
	•					Properties		

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

Properties: Generic - Kaspersky Industr	ial CyberSecurity for Nodes 2.6	
Sections	General	
Properties: Generic - Kaspersky Industr Sections General Event configuration Application settings Supplementary Real-Time Computer Protection Local activity control System inspection Logs and notifications Revision history	Application: Target administration group: Created: Modified: Policy status @ Active policy @ Inactive policy @ Inactive policy	Inity for Nodes 2.6 Kaspersky Industrial CyberSecurity for Nodes 2.6 Managed devices\SIMCO 5/21/2020 3:23:58 PM 5/21/2020 3:29:22 PM
	Settings inheritance	
Help		OK Cancel Apply

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



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

K Applications Launch Control	? 🗙
General Software Distribution Control Task management	
Task mode	
Statistics Only	•
Repeat action taken for the first file launch on all the subsequent launches for this f	ile
Deny the command interpreters launch with no command to execute	
CRules managing	
Rules list Total	rules: 24
Rules combination: Add policy rules to the local rules	
The application merges a policy-defined rules list with the local rules lists defin computer. You can configure local rules lists via the Rule Generator for Applica Launch Control tasks.	ed on each ations
Rules usage scope	
Apply rules to executable files	
Monitor loading of DLL modules	
Apply rules to scripts and MSI packages	
KSN Usage	
Deny applications untrusted by KSN	
Allow applications trusted by KSN	
Users and / or user groups allowed to run applications trusted by KSN:	
Everyone; NT AUTHORITY\SYSTEM	Edit
ОК	Cancel

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

K Applications Launch Control
General Software Distribution Control Task management
Schedule settings
Frequency: At application launch
Task start
Advanced
OK Cancel

7. Once you have reverted to Local activity control, close all locks (a), press Apply and OK to exit editing the SIMCO\_POLICY policy properties.



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

#### Setting up Device Control whitelisting

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

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

Administration Server KSC	Administration Serve	er KSC (KSC\Administra	tor)		
Managed devices					
	Monitoring 5	Statistics Reports	Events		
Device selections		Construction of the second			
L <sub>x</sub> ! Unassigned devices					
Policies	Selection events	Recent events * *			
Tasks	Selection events	Instally existing ~			
A dvanced	Sector Contractor and Street				
L User accounts	Run selection	Selection prope	rties Create a selection	Import/Export 🔻	
A D Application managemer		2			
<ul> <li>Application categorie</li> </ul>	Add Remove columns				
Applications registry	HUNDREINVE LUMINIS				
Executable files					
<ul> <li>Software vulnerabiliti</li> </ul>	Ime	Device	Event	Description	Group
. Software undater	20.02.2018 18:34:58	SIMCO	Statistics Only: untrusted mass storage detected	{"Vendor": "VID_090C", "Product": "PID_1000", "SerialNum"	SIMCO
- Kaspassin I ah lissass	0 20.02.2018 18:32:29	SIMCO	Running		SIMCO
Raspersky Lab license	20.02.2018 18:33:22	SIMCO	Modified		SIMCO
A H Remote installation	0 20.02.2018 18:33:21	SIMCO	Modified		SIMCO
Installation packages	0 20.02.2018 18:33:22	Administration Server <k< td=""><td>Audit (changes to the object's status)</td><td>Group task "Managed devices/SIMCO/SIMCO - Rule Gen</td><td>Managed devices</td></k<>	Audit (changes to the object's status)	Group task "Managed devices/SIMCO/SIMCO - Rule Gen	Managed devices
A Q Network poll	20.02.2018 18:33:21	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Group task "Managed devices/SIMCO/SIMCO - Rule Gen</td><td>Managed devices</td></k<>	Audit (objects modification)	Group task "Managed devices/SIMCO/SIMCO - Rule Gen	Managed devices
b • Domains	0 20.02.2018 18:33:22	SIMCO	Scheduled		SIMCO
<ul> <li>Active Directory</li> </ul>	3 20.02.2018 18:33:21	SIMCO	Scheduled		SIMCO
<ul> <li>IP subnets</li> </ul>	0 20.02.2018 18:26:42	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Policy "SIMCO_POLICY" has been modified by user "KSC\</td><td>Managed devices</td></k<>	Audit (objects modification)	Policy "SIMCO_POLICY" has been modified by user "KSC\	Managed devices
<ul> <li>MyPCS7</li> </ul>	1 20.02.2018 18:02:11	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Policy "SIMCO_POLICY" added by user "KSC\Administrator"</td><td>Managed devices</td></k<>	Audit (objects modification)	Policy "SIMCO_POLICY" added by user "KSC\Administrator"	Managed devices
Repositories	0 20.02.2018 17:44:58	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Policy "Kaspersky Security Center 10 Network Agent" ad</td><td>Managed devices</td></k<>	Audit (objects modification)	Policy "Kaspersky Security Center 10 Network Agent" ad	Managed devices
Contract Contract Contract Net N	0 20.02.2018 17:43:35	Administration Server <k< td=""><td>Device status is Critical</td><td>Status of device 'SIMCO' changed to Critical: Windows u</td><td>Managed devices</td></k<>	Device status is Critical	Status of device 'SIMCO' changed to Critical: Windows u	Managed devices
	120.02.2018 17:34:49	SIMCO	Real-time protection security level has changed		SIMCO
	3 20.02.2018 17:35:44	SIMCO	Completed	Remote installation has been successfully completed on t	SIMCO
	0 20 02 2018 17-34-38	SIMCO	Rupping	Setup started	SIMCO

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

Time	Device	Event	Description		Group
A 20.02.2018 18:34:58	SIMCO	Statistics Only: untrusted mass storage detected	2000 aversion	", "Product": "PID_1000", "SerialNum"	SIMCO
0 20.02.2018 18:32:29	SIMCO	Running	Device Properties		SIMCO
1 20.02.2018 18:33:22	SIMCO	Modified	Go to device		SIMCO
1 20.02.2018 18:33:21	SIMCO	Modified	Go to group		SIMCO
0 20.02.2018 18:33:22	Administration Server <k< td=""><td>Audit (changes to the object's status)</td><td>-</td><td>devices/SIMCO/SIMCO - Rule Gen</td><td>Managed devices</td></k<>	Audit (changes to the object's status)	-	devices/SIMCO/SIMCO - Rule Gen	Managed devices
1 20.02.2018 18:33:21	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Export</td><td>devices/SIMCO/SIMCO - Rule Gen</td><td>Managed devices</td></k<>	Audit (objects modification)	Export	devices/SIMCO/SIMCO - Rule Gen	Managed devices
120.02.2018 18:33:22	SIMCO	Scheduled	Delete		SIMCO
0 20.02.2018 18:33:21	SIMCO	Scheduled	Delete		SIMCO
0 20.02.2018 18:26:42	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Delete All</td><td>" has been modified by user "KSC\</td><td>Managed devices</td></k<>	Audit (objects modification)	Delete All	" has been modified by user "KSC\	Managed devices
1 20.02.2018 18:02:11	Administration Server <k< td=""><td>Audit (objects modification)</td><td>View</td><td>" added by user "KSC\Administrator"</td><td>Managed devices</td></k<>	Audit (objects modification)	View	" added by user "KSC\Administrator"	Managed devices
17:44:58 20.02.2018	Administration Server <k< td=""><td>Audit (objects modification)</td><td>VIEW</td><td>rity Center 10 Network Agent" ad</td><td>Managed devices</td></k<>	Audit (objects modification)	VIEW	rity Center 10 Network Agent" ad	Managed devices
0.02.2018 17:43:35	Administration Server <k< td=""><td>Device status is Critical</td><td>Refresh</td><td>O' changed to Critical: Windows u</td><td>Managed devices</td></k<>	Device status is Critical	Refresh	O' changed to Critical: Windows u	Managed devices
0 20.02.2018 17:34:49	SIMCO	Real-time protection security level has changed	B		SIMCO
17:35:44 20.02.2018	SIMCO	Completed	Properties	s been successfully completed on t	SIMCO
0 20.02.2018 17:34:38	SIMCO	Running	Setup started.		SIMCO
120.02.2018 17:35:26	Administration Server <k< td=""><td>Audit (changes to the object's status)</td><td>Task for specific device</td><td>es "Deploy KICS4NODES_HotFix8"</td><td>Managed devices</td></k<>	Audit (changes to the object's status)	Task for specific device	es "Deploy KICS4NODES_HotFix8"	Managed devices
120.02.2018 17:35:26	Administration Server <k< td=""><td>Audit (objects modification)</td><td>Task for specific device</td><td>es "Deploy KICS4NODES_HotFix8"</td><td>Managed devices</td></k<>	Audit (objects modification)	Task for specific device	es "Deploy KICS4NODES_HotFix8"	Managed devices
0 20.02.2018 17:35:26	SIMCO	Running	Copying files to the sp	pecified device	SIMCO
17:35:26	SIMCO	Scheduled	Waiting for connection	n	SIMCO
120.02.2018 17:35:26	SIMCO	Scheduled		200	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.

Events Export Wizard	
xport file	
Select file:	
C:\Users\Administrator\Desktop\BlockedUSB.bt Browse	
Next Canc	el

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

G Events Export Wizard	×
Export format	
Export as tab-delimited text	
Export as tab-delimited Unicode text	
	Next Cancel

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



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

#### Rules list...

Properties: SIMCO_POLICY	
Sections	Local activity control
General Event configuration Application settings Supplementary Real-time computer protection Local activity control Network activity control System inspection Logs and notifications Revision history	Applications Launch Control <ul> <li>Configure applications launch control.</li> <li>Set the list of rules for applications launch control.</li> </ul> Device Control <ul> <li>Configure device control.</li> <li>Set the list of rules for device control.</li> </ul> Wi-Fi Control <ul> <li>Configure Wi-Fi control.</li> <li>Set the list of rules for Wi-Fi control.</li> </ul> <ul> <li>Configure Wi-Fi control.</li> <li>Set the list of rules for Wi-Fi control.</li> </ul> <ul> <li>Configure Wi-Fi control.</li> <li>Set the list of rules for Wi-Fi control.</li> </ul>
<u>Help</u>	OK Cancel Apply

K Device Control	? 🔀
General Task management	
Task mode	
Statistics Only	-
Allow using all mass storage devices when the Device C not running	Control task is
Rules list Total rules: 0.	
ОК	Cancel

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

📕 Device Con	ntrol rules			
Search: Type	e to search the rules			
Add Total rules: 0 Appl M	Remove selected         Generate rules based on connected devices         Generate rules based on system data         Import rules from XML file         Import data of blocked devices from Kaspersky Security Center report		Export to a svice instance path Merge with existing rules Add to existing rules Replace existing rules	Gener.
•	III.	_		Þ
🕜 Help			Save	ncel

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

Search:	Control rules Type to search the ru Delete selected tal: 1.	iles				Export to a file
Appl	Manufacturer (	Controller type	Serial number	Des	Device instance path	Generation met
Yes	VID_090C	PID_1000	FC160923000253ZBK6XF		USB\VID_090C&PID_1000\FC160923000253ZBK6XF	Added manually
🕐 Help						Save Cancel

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

📕 Device Control
General Task management
Task mode
Active
Allow using all mass storage devices when the Device Control task is not running
Rules list Total rules: 1.
OK Cancel

Page 120 of 161

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.

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

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

#### **Setting up File Operations Monitor**

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

You may benefit from the preconfigured **KICS for Nodes** security policy contained in **Generic\_policy-KICS4NODES\_2.6\_PCS7\_9.1.klp**. The default security policy already specifies some most common **WinCC** project locations available for file integrity monitoring. The file monitoring is set up so that false notifications would hardly ever bother you unless you start downloading an OS project using **Simatic Manager**.

Nevertheless, some fine tuning is still necessary.

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

Properties: SIMCO - Kaspersky Industrial CyberSecurity for Nodes 2.6					
Sections	System inspection				
General Event configuration Application settings Supplementary	File Operations Monitor Set areas to intercept file operations in it. Settings				
Real-Time Computer Protection Local activity control Network activity control	Log Inspection - Set custom rules list for Windows Event Log inspection Configure predefined rules settings for Windows Event Log inspection.				
System inspection Logs and notifications Revision history					

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

K File Operations Monitor	and an other states	8 X						
File operations monitoring settings	Task management							
Monitor interruption								
V Log information about file op	$\blacksquare$ Log information about file operations that appear during the monitoring interruption period							
Apply this setting if yo been taken place on a Operations Monitor ta:	Apply this setting if you want the application to consider all the file operations that have been taken place on a media during the period when the media has been out of the File Operations Monitor task view.							
The application is to lo reappearance.	g information about file	e operation detected after the media						
USN log Block attempts to compromis	e the USN log							
Monitoring scope	Monitoring scope							
Area to monitor	Trusted users	File operations						
C:\Program Files (x86)\		COMPRESSION_CHANGE,						
D:\Projects\		COMPRESSION_CHANGE,						
Add Modify		Remove						
		OK Cancel						

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

K File operation	is monitoring rule	X
Monitor file oper-	ations for the scope:	
D:\Projects\*		Browse
Set rule triggerin	g criteria for a scope specified:	
Trusted users	File operation markers Exclusions	
Trusted users	and/or groups of users:	
Users		
Add	J	Remove
	ОК	Cancel
		Cancor

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

K File operations monitoring rule
Monitor file operations for the scope:
D:\Projectsi * Browse
Set rule triggering criteria for a scope specified:
Trusted users File operation markers Exclusions
Cxclude the following folders from control
Exclusion
d:\projects,*\*.cfg
d:\projects <mark>,</mark> *\*.ldf
d:\projects <mark>,</mark> *\*.mcp 🗏
d:\projects <mark>,</mark> *\*.wnf
d:\projects <mark>,</mark> *\*.liccount
d:\projects <mark>,</mark> *\*.lck
d:\projects <mark>,*</mark> \*.mdf
d:\projects <mark>,*</mark> \*.\$\$\$
d:\projects <mark>,</mark> *\*.err
d:\projects <mark>,</mark> *\opc\alarmevent\ccaeprovider.ini
d:\projects <mark>,</mark> *\meld\ccalarmfilterstorage.xml
d:\projects <mark>,*</mark> \imtagfiles\schema.ini
d:\projects <mark>,</mark> *\opc\dataaccess\sopcsrvr.ini
d:\projects,*\*.tst
Add Modify Remove
OK Cancel

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

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

#### Setting up PLC Integrity Checker

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

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

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

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

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

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

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

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

Administration Server KSC	Administratio	on Server	KSC > Managed de	vices >	ES		
Managed devices							
CLIENT10	Managed devices						
CLIENT7							
ES ES	Devices	Polici	as Tasks				
ES_Virt	Devices	1 Onci	taana				
> 🖵 IS							
D OSRC	Add devices	New	Perform a	ction T	Add/Ramous colum	195	
C OSSB	Add dentes	iven	group	cuon -	Augrice colum	1112	
🖵 РН							
SIMCO	No filter s	necified	records total: 1				
VEB	r No miter s	pecifieu,	records total. 1				
Device selections	C.1				ow. 0		
Unassigned devices	Select statuses		ai: 1 🔽 warning:	0 0	UK: U		
7 Policies	The above numbe	rs include the	number of devices with the	e specified	status, which are in the s	ected group and in a	ny of its nested subgroup
Tasks	The list below only	y includes dev	ices from the selected grou	p.			
Advanced	Name		Type of operating syste		Windows dom	Agent installed	Agent running
User accounts			Type of operating syste	-	Windows domain	Agent instance	Agenciuming
Application management	ES ES	Protectio	n		WORKGROUP	V Yes	V Yes
Application categories	Funnte						
<ul> <li>Applications registry</li> </ul>		Lycins					
Executable files		Install ap	plication				
<ul> <li>Software vulnerabilities</li> </ul>		Check de	vice accessibility				
<ul> <li>Software updates</li> </ul>							
Kaspersky Lab licenses		Connect	to Remote Desktop				
▲ 모 Remote installation		Custom	ools				
Installation packages				10000			
Q Network poll		All Tasks		•			
Domains							
Active Directory		Cut					
IP subnets		Delete					
MvPcs		0.6.1					
New su222bnet		Kerresh					
A E Repositories		Export lis	t				
Kaspersky Lab software	0	Properti					
· Quarantine		roperti	6				
Backup							
Unprocessed files							

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

Properties: ES	
Sections	Tasks
General	
Protection	✓ Tasks created for the device:
Applications	
Tasks	Device Control
Events	
Tags	File Operations Monitor Kaspersky Industrial CyberSecurity for Nodes 2.6
System Info	
General system info	KSW Usage Kaspersky Industrial CyberSecurity for Nodes 2.6
Incidents	
Sessions	Kaspersky Industrial CyberSecurity for Nodes 2.6 Running
Applications registry	On-Demand Scan
Executable files	Let Aspersky Industrial CyberSecurity for Nodes 2.6
Hardware registry	PLC Project Integrity Check Kaspersky Industrial CyberSequrity for Nodes 2.6
Software vulnerabilities	
Available updates	FLC Project Investigation Kaspersky Industrial CyberSecurity for Nodes 2.6
Active policy profiles	C Quarantine Scan
Distribution points	Kaspersky Industrial CyberSecurity for Nodes 2.6
	Real-Time File Protection Kaspersky Industrial CyberSecurity for Nodes 2.6 Running
	Rollback of Application Database Update Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Applications Launch Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Device Control
	Results Add Properties
Help	OK Cancel Apply

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

Properties: PLC Project Investigation								
Sections	PLC configurations							
General	List of PLC configura	List of PLC configurations: Total rules: 0						
PLC configurations	DLC huma	Description	Connection actions	DLC Desistery ID				
Account	PLC type	Description	Connection settings	PLC Registry ID				
Notification								
	•			4				
			PLC Desisters	Edit Descent				
	LINK to PLC Regis	ary I Add from	1 PLC Registry	Edit				
<u>Help</u>			OK Can	cel Apply				

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

🔜 PLC Registry	management				- • •				
PLC Registry allo application solution	PLC Registry allows you to centrally manage all PLCs inside a protected perimeter. It is available for a shared use by the Kaspersky Industrial CyberSecurity application solutions.								
Filter:	Filter: Total configurations: 0.								
Only show PL	C that can be prote	ected by Kaspersky Ind	dustrial CyberSecurity for Nodes						
Import	Export			Add Modify	Remove				
Name 🗡	Model	Publisher	Description	Connection settings	PLC Regist				

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

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

	PLC se	ettings (added lo	cally)	-	<b>Negli</b>	The Parallel			
l r	Genera	l Settings							
	Name:			MyPLC	:				
	PLC typ	pe:		Siemer	is Simati	: S7-400H			•
	Descrip	otion:		57-410	ЭН				
	Wait fo	or connection:		10	* *	seconds			
ſ	Connec	tion settings							
	Port:			102	* *		🗌 Read data (	olocks	
	🗖 Api	ply password							
	Specify	y IP - address, rac	k slot and p	press Ad	d buttor	n			
	IP :	192.168.1.1		Rack:	0	<ul> <li>T</li> </ul>	Slot: 3	×	Add
	IP - a	address	Rack			Slot			Remove
	_								
								ОК	Cancel

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

PLC settings (added	locally)	-	-	rie name				X
General Settings								
Name:		MyPL	c					
PLC type:		Sieme	ns Simati	c 57-400H				-
Description:		S7-41	.0H					
Wait for connection:		10	×	seconds				
Connection settings								
Port:		102	· · · · · · · · · · · · · · · · · · ·		📃 Read data l	<u>b</u> locks		
Apply password								
Specify IP - address, ra	ack slot and p	ress A	dd buttor	ı				
IP: 192.168.1.2		Rack:	1		Slot: 3	×	Add	
IP - address	Rack			Slot			Remove	
192.168.1.1	0			3				
						_		
						_		
						ОК	Can	cel

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

E F	PLC Registry management						
PLC Registry allows you to centrally manage all PLCs inside a protected perimeter. It is available for a shared use by the Kaspersky Industrial CyberSecurity for Nodes application solutions.							
Filt	er:			Total configurations: 1.			
	Only show PLC t	hat can be protected	by Kaspersky Indust	rial CyberSecurity for Nodes			
Import Export Modify Remov							
N	ame 🔼	Model	Publisher	Description	Connection settings	PLC Regist	
	yPLC	Simatic S7-400H	Siemens	57-410H	IP address: 192.168.1.1; port: 102;	202101251	
•				III		•	
					Add to task list	Close	



9.	Click OK	in the parent	window to	finalize the	e task p	arametrization
----	----------	---------------	-----------	--------------	----------	----------------

Properties: PLC Project Investigation							
Sections	PLC configurations						
General	List of PLC configurat	ions:		Total rules: 1.			
PLC configurations	PLC type	Description	Connection settings	PLC Registry ID			
Account	Siemens Simatic	57-410H	IP-adress: 192.168.1.2; port: 102; r	201905231206			
Notification							
	•			•			
	Link to PLC Registr	Y Add from	PLC Registry Edit.	. Remove			
Help			OK Cancel	Apply			

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

Sections	Tasks
General	
Protection	Tasks created for the device:
Applications	
Tasks	KSN Usage Kaspersky Industrial CyberSecurity for Nodes 2.6
Events	
Tags	Kaspersky Industrial CyberSecurity for Nodes 2.6
System Info	Channing Con-Demand Scan
General system info	Kaspersky Industrial CyberSecurity for Nodes 2.6
Incidents	PLC Project Integrity Check
Sessions	Kaspersky Industrial CyberSecurity for Nodes 2.6
Applications registry	PLC Project Investigation
Executable files	Completed
Hardware registry	Quarantine Scan Kaspersky Industrial CyberSecurity for Nodes 2.6
Software vulnerabilities	Real-Time File Protection
Available updates	Kaspersky Industrial CyberSecurity for Nodes 2.6 Running
Active policy profiles	Rollback of Application Database Update
Distribution points	Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Applications Launch Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Device Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	Scan at Operating System Startup Kaspersky Industrial CyberSecurity for Nodes 2.6
	SIMCO - Rule Generator for Applications Launch Control
	Results Add Properties

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

Time	Status	-
13.04.2018 18:39:01	Information about PLC project received	
13.04.2018 18:22:58	Error receiving PLC project information	
05.04.2018 16:03:21	Information about PLC project received	=
05.04.2018 15:55:52	Information about PLC project received	
05.04.2018 15:49:33	Information about PLC project received	
05.04.2018 15:38:32	Information about PLC project received	
05.04.2018 15:04:45	Information about PLC project received	
05.04.2018 14:57:46	Information about PLC project received	
05.04.2018 14:52:54	Information about PLC project received	
05.04.2018 14:46:03	Information about PLC project received	
05.04.2018 14:38:52	Information about PLC project received	-
<		- F

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

Properties: PLC Project Integrity Check			
Sections	Settings		
General	Check projects integrity for	PLC configurations:	
Settings	PLC type	Connection settings	Peference DLC project rece
Schedule	PEC type	connection settings	Reference PLC project rece
Account			
Notification			
		Add	Edit Remove
Help		ОК	Cancel Apply

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

Data for PLC project integrity check	s	2	and interest	? ×
Check PLC project integrity with an inte	rval: s.			
Configurations for PLC type selected:	Siemens Simatic	S7-400H	•	
Connection settings		Description		
IP address: 192.168.1.1; port: 102; rad	tk: 0; slot: 3; read	CPU model : 6ES7 4	10-5HX08-0AB0 ; Firmware ve	ersion :
Project version to consider as reference f Reference PLC project receipt date	for PLC configuration	selected: ash	Description	
22.01.2021 15:43:27	8cbeae4b400968a5	1585b10ac158e	410-5H	
			Add	Cancel

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

Properties: PLC Project Integrity Check			
Sections	Settings		
General	Check projects integrity for PLC	configurations:	
Settings	PLC type	Connection settings	Reference PLC project rece
Schedule	Siemens SIMATIC S7-400	IP-address: 192.168.1.2; p	05.03.2018 16:57:32
Account			
Notification			
		Add	Edit Kemove
Help		ОК	Cancel Apply

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

Properties: PLC Project Integrity Check	
Sections	Schedule
General	Schedule settings
Settings	Run by schedule
Schedule	Frequency: At application launch
Account	
Notification	Task start settings
	Advanced
	Task will be performed according to the local time on the computer
	A resk will be performed according to the local time on the computer.
<u>нер</u>	OK Cancel Apply

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

Sections	Tasks
General	
Protection	✓ Tasks created for the device:
Applications	
Tasks	KSN Usage Kaspersky Industrial CyberSecurity for Nodes 2.6
Events	
Tags	Kaspersky Industrial CyberSecurity for Nodes 2.6
System Info	Pon-Demand Scan
General system info	Kaspersky Industrial CyberSecurity for Nodes 2.6
Incidents	PLC Project Integrity Check
Sessions	Kaspersky Industrial CyberSecurity for Nodes 2.6
Applications registry	PLC Project Investigation
Executable files	
Hardware registry	Quarantine Scan Kaspersky Industrial CyberSecurity for Nodes 2.6
Software vulnerabilities	Real-Time File Protection
Available updates	Kaspersky Industrial CyberSecurity for Nodes 2.6 Running
Active policy profiles	Rollback of Application Database Update
Distribution points	Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Applications Launch Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	Rule Generator for Device Control Kaspersky Industrial CyberSecurity for Nodes 2.6
	Scan at Operating System Startup Kaspersky Industrial CyberSecurity for Nodes 2.6
	SIMCO - Rule Generator for Applications Launch Control
	Results Add Properties

Tasks Sections General Protection Tasks created for the device: Applications KSN Usage Kaspersky Industrial CyberSecurity for Nodes 2.6 Tasks Events Log Inspection Kaspersky Industrial CyberSecurity for Nodes 2.6 Running Tags System Info On-Demand Scan Kaspersky Industrial CyberSecurity for Nodes 2.6 L General system info PLC Project Integrity Check Kaspersky Industrial CyberSecurity for Nodes 2.6 Incidents 7 Sessions Running Applications registry PLC Project Investigation Kaspersky Industrial CyberSecurity for Nodes 2.6 Executable files Quarantine Scan ≣ Hardware registry Kaspersky Industrial CyberSecurity for Nodes 2.6 Software vulnerabilities Real-Time File Protection Kaspera. Running Kaspersky Industrial CyberSecurity for Nodes 2.6 Available updates Active policy profiles Rollback of Application Database Update Kaspersky Industrial CyberSecurity for Nodes 2.6 Distribution points Rule Generator for Applications Launch Control Kaspersky Industrial CyberSecurity for Nodes 2.6 Rule Generator for Device Control I Kaspersky Industrial CyberSecurity for Nodes 2.6 Scan at Operating System Startup Kaspersky Industrial CyberSecurity for Nodes 2.6 SIMCO - Rule Generator for Applications Launch Control Toductrial CuborCo rity for Nod Results Add... Properties

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

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

#### to the Events tab.

Administration Server KSC	Administration Serve	r KSC (KSC\Administrat	tor)		
Managed devices					
CLIENT10	Manitarian	Denote Denote	Evente		
CLIENT7	ivionitoring 5	taustics Reports	Events		
🖵 ES					
ES_Virt	Coloritore average	Tefermational even	to =		
D IS	Selection events	Informational even	<u>us</u> ▼ ™		
▷ □ OSRC					
OSSB	Selection properties	Create a selection	Import/Export 🔻		
🖵 РН					
SIMCO	Add/Remove columns				
WEB	<u>Haaji temove colamio</u>				
Device selections	Time	Device	Event	Description	Grou
Unassigned devices		50	DLC project watches reference project	Controller type: Sigmone SIMATIC 57 400 DLC conference	EC
Policies	05.04.2018 16.22.11	ES	PLC project matches reference project	Controller type: Siemens SIMATIC 57-400. PLC configura	EC
Tasks	05.04.2018 16:20:29	ES	PLC project matches reference project	Controller type: Siemens SIMATIC 57-400. PLC configura	ES
Advanced	05.04.2018 16:19:24	ES	PLC project matches reference project	Controller type: Siemens SIMATIC S7-400, PLC configura	ES
User accounts	05.04.2018 16:18:24	ES	PLC project matches reference project	Controller type: Siemens SIMATIC S7-400, PLC configura	ES
Application management	05.04.2018 16:17:23	ES	PLC project matches reference project	Controller type: Siemens SIMATIC S7-400. PLC configura	ES
<ul> <li>Application categories</li> </ul>	05.04.2018 16:16:24	ES	PLC project matches reference project	Controller type: Siemens SIMATIC S7-400. PLC configura	ES
Applications registry	05 04 2010 16:15:24	50	DLC and a state of a second second second	Carballas haras Cimeras CIMATIC CZ 400, DLC and a	50

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

🖬 🗐 Administration Server KSC 👘	Administration	Server KSC > Advance	ed > Repositories > Ha	rdware
<ul> <li>Managed devices</li> <li>Administration Servers</li> </ul>	🐨 Hardwai	re		
CLIENT10	The list displays in	formation about hardware ar	nd devices of the organizatio	on. You can edit data from
D CLIENT7			in devices of the organizatio	
🖌 🖵 ES				
Administration Servers	Add device	View hardware report	Additional actions 🔻	
⊳ 🗖 I2			Configure criteria for e	enterprise devices
▶ 🖵 KSC	No filter spe	cified. records total: 22	2 Configure custom data	a fields
			Open PLC Registry	
A La OSSB El Administration Servers	Add/Remove column	2		
▷ □ PH				
	Name	<u>^</u>	Description	Туре
▷				
Device selections				
🖵 Unassigned devices				
Policies				
Tasks				
Advanced				
Hiser accounts				
Application management				
A 🖵 Remote installation				
<ul> <li>Deploy device images</li> </ul>				
<ul> <li>Installation packages</li> </ul>				
Q Network poll				
▷ • Domains				
Active Directory				
Pranges				
Hardware				
<ul> <li>Kaspersky Lab softwari</li> </ul>				
Quarantine				
• Backup				
<ul> <li>Unprocessed files</li> </ul>				

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

#### **Enabling optional password protection**

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

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

Properties: SIMCO_POLICY			K Security settings	? 🗙
Sections	Application settings		Security	
Sections General Event configuration Application settings Supplementary Real-time computer protection Local activity control Network activity control System inspection Logs and notifications Revision history	Application settings         Scalability and interface         Image: Scalability and i	Settings	Security Reliability settings Perform task recovery Recover on-demand scan tasks no more than (times): Actions when switching to UPS backup power Do not start scheduled scan tasks Stop current scan tasks Stop current scan tasks Password protection Password protection Password: Confirm password:	
Help	OK Car	icel Apply	ОК	Cancel

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

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

#### Installing optional KICS for Nodes management console

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

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

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

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

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



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



3. Name this new installation package as KICS4NODES\_CONSOLE\_X64. Click Next.



4. In the **Selecting the distribution package for installation** window, browse to the **kicstools\_x64.msi** <sup>12</sup>file (supplied as a part of the **KICS for Nodes 2.6** distribution package) and select it. Specify the command line options as shown below. Click **Next**. Then click **Finish** in the finalization window.

New Package Wizard      Selecting the distribution package for installation
Selecting the distribution package for installation
Selecting the distribution package for instantion
\Desktop\KL_Distributives\KICS4NODES\client\kicstools_x64.msi Browse
Executable file command line (optional):
/i PRIVACYPOLICY=1 EULA=1 /qn
Copy entire folder to the installation package
Center 11
Next Cancel

<sup>&</sup>lt;sup>12</sup> In case of a 32-bit operating system of a target node **kicstools\_x86.msi** should be selected Page **143** of **161**
5. Select the just created installation package, right-click it and in the context menu select **Install application** as shown below.



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



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

0	Remote Installation Wizard	
	Remote Installation Wizard         Select devices for installation         Image devices         Image devices	Add         If no relevant devices are displayed in the list, dick Add to type their names or IP addresses.
		Next Cancel

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

		<u> </u>
0	Remote Installation Wizard	
	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 <ul> <li>Install always</li> <li>Install only on devices managed through this Administration Server</li> </ul>	
	Do not re-install application if it is already installed	
	Assign package installation in Active Directory group policies	
	Next	ancel

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

		×
$\bigcirc$	Remote Installation Wizard	
	Selecting an operating system restart option	
	Select the action that will be performed if the application installation prompts you to restart the operating system.	
	O not restart the device     O	
	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).	
	Madify	
	Force dosure of applications in blocked sessions	
	Next	Cancel

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

0	Remote Installation Wizard
	Select accounts to access devices
	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.
	Add
	Properties
	Next Cancel

11. In the **Starting installation** windows that follows, click **Next** and finally **Finish**. Actually, we have created the task that will launch **kicstools\_x64.msi** on a target host.

12. Now you are automatically redirected to the **Administration Server->Tasks** node and you can see the just created **Deploy KICS4NODES\_CONSOLE\_X64** task running. Wait for its completion.

The Action New Help										
🕨 🔿 📶 🔏 🖬 🙆 🖬 🖬	1									
Kaspersky Security Center 11 Administration Server WIN-R2FGT(	Administration Server WIN-R2FGT0T	NH3K > Tasks								
Managed devices	⊙ Tasks									
Mobile Device Management     Device selections     Inassigned devices     Policies	New task Import task from file									Bef
Tasks	Add Damage of some									811
Advanced	Name	Application	Task type	Status	Runn	Com	Com	Com	D. L. MCCM	
Application management     Remote installation	Database Update	Kaspersky Ind	Database Update	Completed	0	1	0	0	Task type:	Install application remotely
Installation packages     Data encryption and protec	Install application remotely	Kasperchy Ser	Install application remo	Completed	0	1	0	0	Application:	Kaspersky Security Center 11 Administration Server
Q Device discovery Deleted objects	Deploy KICS4NODES_CONSOLE_X64	Kaspersky Sec	Install application remo	Running (11%	1	0	0	0	Group:	Tasks for specific devices
A El Repositories	Deploy KICS4NODES_X64_ENG	Kaspersky Sec	Install application remo	Completed	0	1	0	0	Running: 11%	
Kaspersky Lab software     Triggering of rules in Sn	On-Demand Scan	Kaspersky Ind	On-Demand Scan		0	0	0	0		
Quarantine     Backup	Rule Generator for Applications Launch Cont	for Applications Launch Control	Copying files to the specified device							
Active threats	SIMCO - Rule Generator for Applications	Kaspersky Ind	Rule Generator for Appli	Completed	0	1	0	0		Execution statistics on devices Running on 1 devices View results
	1									

Application management ▲ 모 Remote installation

Installation packages

Kaspersky Lab software

Triggering of rules in Sn

Data encryption and protec

Q Device discovery Deleted objects

> · Quarantine Backup Active threats

#### Uninstalling KICS for Nodes and KLnagent

We hope that you will not encounter a situation inducing you to do this. However, if it is necessary you can perform software removal without even having to shut down your control system runtime.

Please perform the following compulsory steps to get the protection software removed from your computer (we are still referring to our SIMCO host as an example):

Application

Task type

🗐 SIMCO - Rule Generato... Kaspersky Ind... Rule Generator for Applications Launch Co... Completed

Kaspersky Ind... Database Update

Kaspersky Ind... On-Demand Scan

Status

Completed

File Action View Help (= -) 🖄 📰 🐇 🗎 🗙 🖬 🖸 Kaspersky Security Center 11 Administration Server WIN-R2FGT0TNH3K > Managed devices > SIMCO Administration Server WIN-R2FGT( Managed devices Group tasks SIMCO Mobile Device Management Device selections Devices Policies Tasks Unassigned devices Policies 📋 Tasks Import task from file Add/Remove columns 📳 Kaspersky Lab Licenses Advanced User accounts

Rule Generator for Applications Launch Control

Inherited tasks: hide | show

Database Update

On-Demand Scan -

📋 On-Demand Scan

Name

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

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



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

	Database Update	
	On-Demand Scan	
	Rollback of Database Opdate     Rollback of Database Opdate	
	Software Modules Lindate	·
	Kaspersky Endpoint Security for Windows (11.2.0)	
	Change application components	
	Integrity check	
	Inventory	
	Manage Authentication Agent accounts	
	Update	
	Update rollback	
	Virus scan	
	Wipe data	
	— Kaspersky Security Center 11 Administration Server	
	Advanced	
	Find vulnerabilities and required updates	
	Start or stop application	
	Send message to user	
	Change Administration Server	
	Manage devices	
	Update verification	
	Download updates to the repositories of distribution points	
	Distribute installation package	
	Uninstall application remotely	
	Fix vulnerabilities	
	Install application remotely	
	Install Windows Update updates	l

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



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

$\bigcirc$	New Task Wizard	
	Settings	
	Application to be removed:	-
	Kasperský Industrial Cyber Security for Tyddes 2.6	•

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

G	New Task Wizard		
	Uninstall utility settings		
	Force uninstall utility upload Using Network Agent Using Microsoft Windows resources by means of Administration Se Using operating system resources through distribution points	erver	
	Verify operating system version before uploading           Use uninstall password		
	Password is not set	Modify	
		Next	ancol

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

Θ	New task wizard	
	Selecting operating system restart option	
	Select the action that should be performed when a restart is required after removal.	
	O not restart device	
	◎ Restart device	
	Prompt user for action	
	Uninstallation completed. Your operating system must be restarted to finish the uninstallation.	*
	Repeat prompt every (min):	A V
	☑ Restart after (min):	×
	Force dosing the applications in blocked sessions	
	Next	ancel

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

		<u> </u>
$\bigcirc$	New task wizard	
	Selecting an account to run the task	
	No account required (Network Agent installed)	
	<ul> <li>Account required (for installation without Network Agent)</li> </ul>	
	List of user accounts to be used to run the task. Accounts will be selected in the order listed.	
		×
	Add Properties	
	Next	Cancel

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

~			(	
G	New task wizard			
	Configure task scheduling s	ettings		
	Scheduled start:	Manually		•
	Run missed tasks			
	Define task launch delay automatic	cally		
	Randomize the task start with inte	rval (min):	1	×
			Next Car	ncel

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

<b>(</b>	New task wizard	x
	Define the task name	
	Name:	
	Uninstall application remotely - KICS	
	Next	ancel

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

0	New task wizard	
	Finish creating the task	
	Click the Finish button to create "Uninstall application remotely - KICS" and complete the Wizard.	
	Run task after Wizard finishes	
	Finish	Cancel

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.

Kaspersky Security Center 11							
Administration Server WIN-R2FGT(	Administration Server WIN-R2FGT0TNH3K > Managed devices > SIMCO						
Managed devices							
D SIMCO	⊳ 및 SIMCO						
Mobile Device Management							
Device selections	Devices Policies Task	· s				Group propert	
Le Unassigned devices							
Policies							
Tasks	New task Import task from file	Add/Remove col	lumps			Refre	
Kaspersky Lab Licenses							
Advanced							
L User accounts							
Application management	Inherited tasks: hide   show						
	News	Amplication	Task time	Chattan			
<ul> <li>Installation packages</li> </ul>	Name	Application	Task type	Status	KICS - Uninstal	application remotely	
Data encryption and protec	Database Update					,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Q Device discovery	Database Update	Kaspersky Ind	Database Update	Completed	Task type:	Uninstall application remotely	
Deleted objects	On-Demand Scan				Application:	Kaspersky Security Center 11	
Repositories	On-Demand Scan	Kaspersky Ind	On-Demand Scan			Administration Server	
<ul> <li>Kaspersky Lab software</li> </ul>		Ruspersky mann	on benand bean				
<ul> <li>Triggering of rules in Sn</li> </ul>	Rule Generator for Applications Launch Co	ntrol			Running: 38%		
Quarantine	SIMCO - Rule Generator for Applicatio	Kaspersky Ind	Rule Generator for Applications Launch Co	Completed			
<ul> <li>Backup</li> </ul>	Uninstall application remotely				-		
<ul> <li>Active threats</li> </ul>	KICS - Uninstall application remotely	Kaspersky Sec	Uninstall application remotely	Running (38% completed)	Pupping upingtal scrip	te	
						Execution statistics on	
						devices	
						Rupping on 1	
						devices	
						View results	
		<u> </u>					

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

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

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

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

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

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

The corresponding **FSTEK** certificates and compatibility statements can be downloaded from the following weblocation: <u>https://support.kaspersky.ru/common/certificates/14567</u>

#### Recommendations

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

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

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



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