# How to identify a problem and collect diagnostic information in Kaspersky Industrial CyberSecurity for Nodes

On this page, you will learn how to identify and fix a problem and what diagnostic information about Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes) to collect and provide to Kaspersky Technical Support.

## Contents:


- Frequently asked questions and how to diagnose problems
- Check list before contacting Kaspersky Technical Support
- Useful links


## Frequently asked questions and how to diagnose problems

If you experience any issue with KICS for Nodes, follow the recommendations below to fix it yourself.



**KICS for Nodes installation package**

To get the KICS for Nodes installation package, submit a request to Technical Support via Kaspersky CompanyAccount. Select the "Installation/Uninstallation" request type and the "Other" request subtype.



**Popular Kaspersky Security Center for Windows requests**

If you are experiencing problems with Kaspersky Security Center for Windows (KSCW), try to find an answer or solution on this page.

There you can find an answer to almost every question about KSCW: how to install, activate or configure the application, how to fix issues that you may experience, etc.

kaspersky

### Check your Windows version

Make sure that there are no special requirements or limitations from KICS for Nodes for your version of Windows.

### Check mandatory updates and the Agent version on outdated operating systems

If you are using an outdated Windows operating system, make sure it has the updates mandatory for the installation and operation.

✓ Check for the Network Agent update for Windows and install it if necessary.

✓ Check for the KICS for Nodes for Windows update and install it if necessary.

✓ Make sure that you are using the compatible version of the Network Agent for outdated Windows operating systems.

### Install a cumulative patch

Install from CompanyAccount the latest update package with important fixes for your version of the application. This usually solves most of the problems.

### Update Windows root certificates

Update Windows root certificates for installing KICS for Nodes.

### Check the KICS for Nodes compatibility certificate for your solution

Check that your industrial solution has the KICS for Nodes compatibility certificate.
Make sure that the correct exclusion profiles are applied to your industrial solution.

**Check files that have been deemed malicious**

If the Anti-Cryptor component is triggered, check which files KICS recognizes as malicious (it may be triggered by Google browser cache).
Add to exclusions folders or files that are deemed malicious in the following cases:

- They do not contain sensitive information.
- They are easy to recover even in the case of a successful encryption attack (for example, the .exe files).
- The alerts are caused by the legitimate software.

# What to check and what information to collect before you contact Kaspersky Technical Support

If you cannot resolve the issue yourself, create a request to Kaspersky Technical Support via Kaspersky CompanyAccount.

Before contacting the Support, make sure that you complete the steps from the list below. The more details you can provide about the issue and what you have already tried and checked, the faster we can resolve your issue.

**1. Check the policy or task settings.**
All the settings must be locked, and the settings must be correct. To check, use these instructions for Kaspersky Endpoint Security. Export a policy and attach the file to your request.

**2. Check which component affects the occurrence of the error or reproduction of the problem.**
To do this, perform one or both of the diagnostic options and specify the problematic component in your request.

- Disable the components in the policy one by one. See if the problem reproduces after you disable the component.
- Remove the application, restart the operating system and install only file anti-virus. This will minimize the number of application drivers in your operating system. Then try to reproduce the problem.

  If the issue does not reoccur, install the components one by one, checking if the issue occurs after each installation.

  In most cases, you will only need to reboot the affected application, not the device itself.

**3. Collect and attach to your request the latest GSI report.**
Run the utility as an administrator and set the "Include Windows event logs" checkbox to include Windows event logs in the report.

If Net Framework 2.0 or later is not installed on the device, use the GSI utility version 5.2. In this case, you will also need to manually collect the System, Application, Kaspersky Security and Kaspersky Event Log in the .evt or .evtx format.

**4. Detections from the Anti-Cryptor and Exploit Prevention components.**

- If the Anti-Cryptor component responds to malicious encryption activity in folders with files that have to be protected:

  1. Describe in detail how the detected file was created.
  2. Enable tracing.
  3. Reproduce the issue or wait until it occurs.
  4. Save the trace files and disable tracing.

- If the Exploit Prevention component detects malicious encryption activity, collect the logs:

  1. Enable Windows Error Reporting (WER) on the problem device to collect dumps.
  2. Open the KICS policy → Real-Time File Protection → Exploit Prevention and set the "Terminate on exploit" checkbox.
  3. Close the locks and wait for the policy to apply.
  4. Enable collecting of the KICS dump and trace files.
  5. Reproduce the issue.
  6. Save the trace files and disable collecting of dump and trace files.

KICS will detect an attempt to exploit the vulnerability and terminate the process, while WER will create a dump of this process.

Attach the process dump and trace files (synchronized with the dump) to the request.

**5. Copy data from the hidden folder**
Copy the entire contents of the hidden "Reports" folder (%ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<KICS version>\Reports), create an archive and attach it to the request.

In outdated operating systems, such as Windows XP or 2003, the folder may be located at: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<KICS version>\Reports

**6. Check the optimization status of the disk I/O subsystem**
If the Disk I/O usage optimization option is enabled on a device with low available RAM, disable it.

If you are sure that you need this option for your infrastructure and cannot disable it, set the virtual disk size to 1500 MB (initial boot may require a lot of space for databases).

**7. Create a request via CompanyAccount**
Describe your issue or error in detail using these instructions, attach to your request all the data mentioned above, and submit your request to Technical Support.

# Useful links

- Kaspersky Industrial CyberSecurity for Nodes Online Help
- About diagnostic data for KICS for Linux Nodes
- How to get assistance from Technical Support
- All you need to know about licenses and their activation
- Training and KICS training program
- How to work with Kaspersky Industrial CyberSecurity for Networks and collect diagnostic information