

Как выявить проблему и собрать диагностическую информацию по Kaspersky Industrial CyberSecurity forNodes

На этой странице вы найдете информацию о том, как выявить и исправить проблему, а также какую диагностическую информацию по Kaspersky Industrial CyberSecurity for Nodes (далее KICS for Nodes) собрать и предоставить технической поддержке «Лаборатории Касперского».

Содержание:

- Частые вопросы и самодиагностика проблем
- Проверка перед обращением и информация для технической поддержки
- Полезные ссылки

Частые вопросы и самодиагностика проблем

Если при работе с KICS for Nodes возникла проблема, вы можете использовать рекомендации ниже, чтобы решить ее самостоятельно.



Дистрибутив KICS for Nodes

Чтобы получить дистрибутив KICS for Nodes, создайте обращение в техническую поддержку через [Kaspersky CompanyAccount](#) с типом запроса «Установка/Удаление» и подтипом — «Другое».



Популярные запросы по Kaspersky Security Center для Windows

Если сложность возникла в работе Kaspersky Security Center для Windows (далее KSCW), попробуйте найти ответ или решение на [этой странице](#).

Здесь есть ответ на практически любой вопрос по KSCW: как установить, активировать или настроить приложение, как решить проблемы, которые могут возникнуть при работе, и многое другое.



Проверьте версию ОС Windows

Убедитесь, что для вашей версии ОС Windows нет специальных [требований и ограничений](#) со стороны KICS for Nodes.



Проверьте обязательные обновления и версию агента на устаревших ОС

Если вы используете устаревшие ОС Windows, убедитесь, что на них установлены обязательные обновления для установки и работы.

✓ Проверьте и при необходимости установите [обновление Агента администрирования для Windows](#).

✓ Проверьте и при необходимости установите [обновление для KICS for Nodes для Windows](#).

✓ Убедитесь, что вы используете [совместимую версию](#) Агента администрирования для устаревших ОС Windows.



Установите кумулятивное исправление

Установите из CompanyAccount [пакет последних обновлений](#) с важными исправлениями для вашей версии приложения. Обычно это помогает решить большую часть проблем.



Обновите корневые сертификаты ОС Windows

Обновите [корневые сертификаты](#) ОС Windows для установки KICS for Nodes.



Проверьте сертификат совместимости KICS for Nodes с вашим решением

Проверьте, что у вашего промышленного решения есть [сертификат совместимости](#) KICS for Nodes.

Убедитесь, что применены нужные [профили исключений](#) для вашей промышленной программы.



Проверьте файлы, действия над которыми расценены как вредоносные

Если сработал компонент «Защита от шифрования», проверьте, действия над какими именно файлами KICS расценил как вредоносные (сработка может произойти на кеш браузера Google).

Исключите в настройках компонента папки или файлы, на которые идет срабатывание, если:

- Они не содержат в себе чувствительной информации.
- Их легко восстановить, даже в случае реальной успешной атаки шифровальщика (например, .exe-файлы).
- Известно, что сработки вызваны работой вашего легального ПО.

Что проверить перед обращением и какую информацию собрать для технической поддержки «Лаборатории Касперского»

Если решить проблему самостоятельно не получилось, создайте запрос в техническую поддержку «Лаборатории Касперского» через [Kaspersky CompanyAccount](#).

Перед обращением в поддержку, пожалуйста, убедитесь, что вы выполнили все шаги из списка ниже. Чем более подробно вы опишете проблему и чем более детально укажете, что уже попробовали сделать и проверить самостоятельно, тем быстрее мы сможем решить ваш вопрос.

1. Проверьте настройки политики или задачи.

Все замки должны быть закрыты, а настройки корректны. Для проверки вы можете использовать [инструкцию](#) для приложения Kaspersky Endpoint Security. [Экспортируйте политику](#) и приложите файл к запросу.

2. Проверьте, какой компонент влияет на появление ошибки или воспроизведение проблемы.

Для этого выполните один или оба варианта диагностики и укажите в запросе проблемный компонент.

- Последовательно отключайте компоненты в политике и проверяйте, воспроизводится ли проблема после каждого отключения.
- Удалите приложение, перезагрузите ОС и установите только файловый антивирус. Так вы минимизируете количество драйверов приложения в вашей ОС. После этого попробуйте воспроизвести проблему.

Если проблема не повторится, поочередно устанавливайте компоненты и проверяйте появление проблемы после каждой установки.

В большинстве случаев нужно перезагружать только проблемное приложение, перезагрузка самого устройства после установки не требуется.

3. Соберите и приложите к запросу отчет **последней версии утилиты GSI**.

Запускайте утилиту от имени администратора и обязательно устанавливайте флажок Include Windows event logs, чтобы в отчет попали журналы событий Windows.

Если на устройстве не установлен Net Framework 2.0 или выше, используйте утилиту GSI версии 5.2. Также в этом случае потребуются **вручную собрать** в формате .evt или .evtx журналы System, Application, Kaspersky Security и Kaspersky Event Log.

4. Обнаружения от компонентов «Защита от шифрования» и «Защита от эксплойтов».

- Если компонент «Защита от шифрования» отреагировал на вредоносную активность шифрования в папках, файлы в которых необходимо защищать:
 1. Подробно опишите, как именно создается файл, на который происходит детект.
 2. Включите **запись трассировки**.
 3. Воспроизведите или дождитесь воспроизведения проблемы.
 4. Сохраните файлы и выключите запись трассировки.
- Если детектирует компонент «Защита от эксплойтов», соберите логи:
 1. **Включите Windows Error Reporting (WER)** на проблемном устройстве на запись дампов.
 2. Откройте политику KICS → раздел «Постоянная защита файлов» → раздел «Защита от эксплойтов» и установите флажок «Завершать скомпрометированные процессы в политике».
 3. Закройте замки и дождитесь, когда политика применится.
 4. **Включите запись файлов дампов и трассировки KICS**.
 5. Воспроизведите проблему.
 6. Сохраните файлы и выключите запись дампов и трассировки.

KICS обнаружит попытку эксплуатации уязвимости и завершит процесс, а WER создаст дамп этого процесса.

Приложите к запросу дампы процесса и файлы трассировки (синхронные с дампом).

5. Скопируйте данные из скрытой папки

Скопируйте все содержимое скрытой папки Reports (%ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<версия KICS>\Reports), создайте архив и приложите его к запросу.

В старых ОС, например Windows XP или 2003, папка может находиться по адресу:

C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<версия KICS>\Reports

6. Проверьте статус оптимизации дисковой подсистемы

Если опция [ОПТИМИЗАЦИИ ДИСКОВОЙ ПОДСИСТЕМЫ](#) включена на устройстве с малым объемом доступной оперативной памяти, отключите ее.

Если вы уверены, что для вашей инфраструктуры опция нужна и выключать ее нельзя, установите размер виртуального диска в 1500 МБ (при первоначальной загрузке может потребоваться много места для баз).

7. Создайте обращение через Company Account

Опишите подробно и по [инструкции](#) проблему или ошибку, соберите все данные из предыдущих пунктов, приложите к запросу и отправьте его в техническую поддержку «Лаборатории Касперского».

Полезные ссылки

- [Онлайн-справка по Kaspersky Industrial CyberSecurity for Nodes](#)
- [О диагностических данных для KICS for Linux Nodes](#)
- [Как получить помощь технической поддержки](#)
- [Все о сертификации, лицензиях и активации](#)
- [Обучение и учебная программа по KICS](#)
- [Руководство по работе и самодиагностике Kaspersky Industrial CyberSecurity for Networks](#)