АО «Система Безопасных Коммуникаций»

123458, г. Москва, Строгино, ул. Маршала Прошлякова, д. 30, офис 307, ком. 1

+7 495 789-04-56

info@communigatepro.ru

Руководство администратора Внешнего помощника CGP-KAV версии 2.0.0

В документе описано, как устанавливать, настраивать и запускать Внешний помощник CGP-KAV для CommuniGate Pro версии 2.0.0, необходимый для проверки писем с помощью Антивируса Касперского. В письма будут добавлены заголовки с результатами проверок. Это позволит автоматически фильтровать письма с помощью правил.

Сокращения

- KAV: Антивирус Касперского
- KSN: Kaspersky Security Network
- CGPro: CommuniGate Pro

Требования

CommuniGate Pro: 6.3.31 и новее

Операционная система: Linux x86_64

Лицензии

Убедитесь, что лицензии для внешнего помощника CGP-KAV добавлены в CGPro. Для этого откройте раздел интерфейса администратора CGPro `Главное → Лицензия`. Если лицензионные ключи помощника CGP-KAV добавлены, в списке будут записи, содержащие “Kaspersky AntiVirus”.

Доступ к внешней сети

Технологиям Kaspersky необходим доступ к Kaspersky Security Network для обновления базы данных вирусных сигнатур. Некоторые функции сканирования, используемые для повышения точности, могут требовать отправки данных в Kaspersky Security Network. Вам необходимо открыть сетевой доступ по протоколам HTTP и HTTPS (80-TCP, 443-TCP) на следующие адреса:

- `*.kaspersky-labs.com`
- `*.kaspersky.com`

Установка Помощника

Установка из дистрибутива

Скачайте последнюю версию архива и распакуйте его в рабочую директорию CGPro (обычно это `/var/CommuniGate`), а затем выполните скрипт установки прав, находящийся внутри директории Помощника:

```
# cd cgpro_home
# tar xf path/to/CGP-KAV-Linux-amd64_vX.Y.Z.tar.bz2
# cgpro_home/CGP-KAV/set_helper_perms.sh
```

где cgpro_home - это путь к рабочей директории CGPro.

> Обратите внимание: в случае динамического кластера необходимо устанавливать Помощник

Обновление с предыдущих версий

Остановите старую версию Помощника в интерфейсе администратора. Для этого откройте раздел `Установки → Общее → Помощники`, выберите `Выключено` для старого Помощника и нажмите `Модифицировать`. После остановки старой версии Помощника удалите его директорию с файловой системы. Установите новую версию из дистрибутива.

При обновлении Помощника с версий до 2.0.0 необходимо перенастроить новую версию Помощника.

При обновлении с версии 2.0.0 и выше перед удалением не забудьте сделать резервную копию файла конфигурации, чтобы потом заменить им файл конфигурации по умолчанию из архива, иначе Помощник нужно будет настраивать заново.

Параметры запуска

Помощника можно запустить с дополнительными параметрами запуска:

- `--help`, `-h` - Справка
- `--config`, `-c` - Путь к конфигурационному файлу

  По умолчанию Помощник ожидает, что конфигурационный файл будет находиться в его корневой директории. Именно так он работает при запуске из Сервера. При необходимости можно задать относительный или абсолютный путь к конфигурационному файлу и запустить Помощник вручную, но работать с Сервером он не будет.

  > Обратите внимание: Параметр нельзя использовать при уже запущенном экземпляре Помощника.

```
# ./CGP-KAV --config /tmp/kav.conf
```

- `--update`, `-u` - Обновление баз нежелательной почты

  Перед первым запуском доступно обновление баз данных до актуального состояния, чтобы не запускать Помощник на устаревших базах и не копить Очередь. Антивирусные базы актуальны на день выпуска Помощника.

  > Обратите внимание: Параметр нельзя использовать при уже запущенном экземпляре Помощника.

  > Обратите внимание: При обновлении антивирусных баз проверка писем невозможна. Перед первым запуском из интерфейса Администратора рекомендуется обновить антивирусные базы при низкой скорости соединения.

- `--version`, `-v` - Версия Помощника

Настройка Помощника в интерфейсе администратора CommuniGate Pro

Чтобы добавить внешнего помощника CGP-KAV, в интерфейсе администрирования CGPro перейдите в раздел `Установки → Общее → Помощники`. Создайте и включите новый Помощник в разделе `Фильтрация данных`, заполните параметры помощника (пример):

Параметр	**Значение**
Имя	AntiVirus
Уровень журнала	Все
Путь к Программе	CGP-KAV/CGP-KAV
Тайм-аут	2 мин
Авторестарт	15 сек

Путь к Программе указывается относительно рабочей директории CGPro.

Настройка правил

Создайте правило для сканирования всех писем, передаваемых через модуль LOCAL, доставляющий письма в почтовые ящики пользователей. Такие настройки означают, что любое письмо будет направлено во Внешний помощник CGP-KAV.

Перейдите в раздел Автоматические Правила. Необязательно настраивать глобальные правила на весь сервер, при необходимости, можно задать Правила для конкретного домена и т.д.

Добавьте новое правило с названием `AntiVirus` и нажмите `Изменить`. Установите в правиле следующие параметры:

Данные	**Операция**	**Параметр**
Любой Маршрут	равно	LOCAL(*

Действие	**Параметр**
Внешний Фильтр	`AntiVirus`

Включение/Выключение Внешнего помощника

В интерфейсе администрирования CGPro перейдите в раздел `Установки → Общее → Помощники` и измените для Фильтра данных `AntiVirus` значение с `Выключено` на `Включено`. Выключить помощника можно обратным образом.

Настройка Внешнего помощника CGP-KAV

Этот раздел описывает параметры конфигурирования, которые находятся в `cgpro_home/CGP-KAV/kav.conf`

```
Обратите внимание: Помощник уже настроен по умолчанию, для версий с 6.3.39
нет необходимости настраивать какие-либо параметры. Ознакомьтесь с настройками
и меняйте их по необходимости.

Для версий ниже 6.3.39 настройка обязательна, необходимо указать параметры
license_endpoint, license_user и license_pwd.
```

Конфигурационный файл чувствителен к регистру. При внесении изменений перезапуск Помощника не требуется.

- Основные настройки (блок `[main]`):
    - `license_endpoint` - адрес интерфейса администратора CGPro

      Адрес необходим для получения данных о лицензиях на Помощника. Это необязательный параметр и его необходимо устанавливать только в случае

использования CGPro версии ниже 6.3.39. Указывайте адрес в формате `http(s)://ip:port/`

- `license_user` - имя пользователя для авторизации в интерфейсе администратора

  Имя пользователя необходимо для получения данных о лицензиях на Помощника. Это необязательный параметр и его необходимо устанавливать только в случае использования CGPro версии ниже 6.3.39.

- `license_pwd` - пароль пользователя для авторизации в интерфейсе администратора

  Пароль пользователя необходим для получения данных о лицензиях на Помощника. Это необязательный параметр и его необходимо устанавливать только в случае использования CGPro версии ниже 6.3.39.

- `license_delay` - Задержка перед получением лицензии: По умолчанию 1 секунда

  Этот необязательный параметр задаёт задержку перед получением лицензии на Помощника, давая возможность серверу инициализировать все свои параметры при запуске.

- `status_header` - заголовок с результатом сканирования. По умолчанию `X-KAV-Status`

- `extended_header` - заголовок с расширенной информацией о результатах сканирования. Здесь будет список вирусов, обнаруженных при сканировании. По умолчанию `X-KAV-Extended`

- `error_header` - заголовок с сообщением об ошибке сканирования. По умолчанию `X-KAV-Error`

- `failure_policy` - политика отказов

  В зависимости от этой настройки Помощник будет по-разному реагировать на ошибки, возникшие при сканировании. Доступные значения: `pass`, `reject`, `error`. По умолчанию `pass`.

  В случае `pass` Помощник будет возвращать заголовок `error_header`. В случае `reject` и `error` Помощник вернёт результат `REJECTED` или `ERROR` соответственно.

  Подробнее о строках с ответами Помощника описано в документации по Внешним Фильтрам Сообщений.

- Настройки антивируса (блок `[av]`).
    - `update_period` - период времени, задающий частоту обновления антивирусных баз. По умолчанию 6 часов (6h)
    - `heuristic_level` - уровень эвристики, используемый при проверке писем. Возможные значения:
        - `fast` - минимальный уровень эвристики, но самая высокая скорость проверки
        - `balanced` - средний уровень эвристики, баланс между скоростью проверки и глубиной эвристического анализа
        - `deep` - максимальный уровень эвристики, время проверки может увеличиться, но результат проверки будет максимально точным
    - `log_level` - включение журналирования KAV SDK. Доступные значения: от 0 до 10, где 0 - выключено, а 10 - максимальный уровень журналирования. Не рекомендуется включать этот параметр без запроса от технической поддержки, так как файлы журнала могут быть очень большими
    - `bases_path` - путь к базе данных вирусов KAV SDK. По умолчанию директория Помощника bases
    - `license_path` - путь к файлу лицензии KAV SDK. По умолчанию директория Помощника license
    - `scan_timeout` - ограничение времени сканирования одного письма. По умолчанию 30 сек (30s)
    - `threads_count` - количество потоков сканирования. По умолчанию половина доступных ядер CPU
- Настройки журналирования (блок `[debug]`).
    - `log_level` - уровень журналирования. Доступные значения `Trace`, `Debug`, `Info`, `Warn`, `Error`, `Fatal`, где `Trace` - это максимально подробное журналирование, а `Fatal` - только сообщения о критических ошибках, приводящих к неработоспособности помощника. По умолчанию `Info`

> Для того, чтобы внешний помощник мог вести полные журналы, необходимо активировать запись полных журналов - `Установки → Почта → Очередь → Установка в Очередь → Уровень Журнала`

Заголовки результатов сканирования

В письма, прошедшие проверку в Помощнике, по результатам сканирования добавляется один или два заголовка. В примерах указаны заголовки по умолчанию, но их можно изменить в файле конфигурации.

- Угроз не обнаружено - добавляется один заголовок `X-KAV-Status`

```
X-KAV-Status: CLEAN
```

- Обнаружена угроза - добавляются заголовки `X-KAV-Status` и `X-KAV-Extended`

```
X-KAV-Status: DETECT
X-KAV-Extended: список идентификаторов вирусов
```

- Ошибка при сканировании - добавляется заголовок `X-KAV-Error`

```
X-KAV-Error: Something went wrong
```

Обновление лицензионных ключей KAV

Периодически внутренние ключи Kaspersky SDK нуждаются в обновлении. В этом случае АО «СБК» предоставит вам ключи и инструкции по их обновлению.

Решение проблем

Ошибки при запуске помощника

`CGP-KAV/CGP-KAV: error while loading shared libraries: libkave8.so.4: cannot open shared object file: No such file or directory`

Если появилась такая ошибка, убедитесь, что все файлы и директории Помощника принадлежат пользователю и группе root, а исполняемый файл `CGP-KAV` имеет права `2755`.

При необходимости запустите скрипт установки прав от имени root:

```
# path/to/CGP-KAV/set_helper_perms.sh
```

Скрипт автоматически выставит владельца и группу root:root и назначит корректные права для исполняемого файла.

Ошибки при инициализации

```
 * FATAL: Kaspersky Anti-Virus SDK initialization failed. Init SDK error:
KAV_E_LICENSE_EXPIRED_OR_MISSING
```

При получении такой ошибки проверьте путь к файлу лицензии KAV в параметре файла конфигурации `[av]/license_path`. По умолчанию файл лицензии ищется в корневой директории Помощника и имеет расширение `.key`. Если лицензия KAV устарела или отсутствует, необходимо запросить новую у технической поддержки.

```
 * FATAL: Kaspersky Anti-Virus SDK initialization failed. Init SDK error:
KAV_E_INVALID_BASES
```

Такая ошибка означает, что KAV не может загрузить базы сигнатур вирусов. Проверьте права на директорию с базами, а также наличие директории. Путь к директории с базами указывается в параметре файла конфигурации `[av]/bases_path` и по умолчанию базы находятся в директории `bases`. Если директория на месте и у неё выставлены правильные права, удалите директорию с базами и восстановите её из полученного архива с Помощником.