**Внешний помощник CGP-KAS**

**для**



Руководство пользователя

|  |  |
| --- | --- |
| Версия продукта : | 1.0.0 |
| Версия документации : | 1.0 |
| Дата : | 01.10.2024 |

**Содержание**

[Предисловие 3](#__RefHeading___Toc1564_3575718543)

[Требования 3](#__RefHeading___Toc1566_3575718543)

[Примечания 3](#__RefHeading___Toc1568_3575718543)

[Сокращения 3](#__RefHeading___Toc1570_3575718543)

[Установка Помощника CGP-KAS 4](#__RefHeading___Toc1572_3575718543)

[Установка из дистрибутива 4](#__RefHeading___Toc1843_3575718543)

[CommuniGate Pro 4](#__RefHeading___Toc1574_3575718543)

[Настройка внешнего помощника 4](#__RefHeading___Toc1845_3575718543)

[Настройка SMTP-правил 4](#__RefHeading___Toc1847_3575718543)

[Запуск Внешнего помощника CGP-KAS 5](#__RefHeading___Toc1576_3575718543)

[Включение Внешнего помощника 5](#__RefHeading___Toc1849_3575718543)

[Выключение Внешнего помощника 5](#__RefHeading___Toc2905_4160107288_Copy_1)

[Утилита диагностики 5](#__RefHeading___Toc1851_3575718543)

[Настройка Внешнего помощника CGP-KAS 5](#__RefHeading___Toc1578_3575718543)

[Основные настройки 5](#__RefHeading___Toc1580_3575718543)

[Настройки Anti-Spam 6](#__RefHeading___Toc1582_3575718543)

[Отладка внешнего помощника CGP-KAS 8](#__RefHeading___Toc1584_3575718543)

[Режим подробного журналирования помощника 8](#__RefHeading___Toc1586_3575718543)

[Заголовки результатов сканирования 10](#__RefHeading___Toc1588_3575718543)

[Kaspersky Anti-Spam Engine 10](#__RefHeading___Toc1590_3575718543)

[Спам не обнаружен 10](#__RefHeading___Toc1853_3575718543)

[Спам обнаружен 10](#__RefHeading___Toc1855_3575718543)

[Список статусов KAS 10](#__RefHeading___Toc1857_3575718543)

[Ошибка 10](#__RefHeading___Toc1859_3575718543)

[Расширенные настройки 11](#__RefHeading___Toc1592_3575718543)

[Kaspersky Anti-Spam Engine 11](#__RefHeading___Toc1594_3575718543)

[Настройки сетевых proxy 11](#__RefHeading___Toc1861_3575718543)

[Обновление лицензионных ключей KAS 11](#__RefHeading___Toc1596_3575718543)

[Настройки производительности 12](#__RefHeading___Toc1598_3575718543)

[Рекомендации Лаборатории Касперского по настройке KAS 12](#__RefHeading___Toc1600_3575718543)

# Предисловие

В этом документе описано, как устанавливать, настраивать и запускать Внешний помощник CGP-KAS для CommuniGate Pro, необходимый для проверки электронных писем с помощью Анти-Спама Касперского. В электронные письма будут добавлены SMTP-заголовки с результатами проверок. Это позволит автоматически фильтровать электронные письма с помощью SMTP-правил CommuniGate Pro.

## Требования

CommuniGate Pro: 6.3.39 и новее

OS: Linux amd64

## Примечания

Технологиям Kaspersky необходим доступ к Kaspersky Security Network для обновления базы данных определений антиспама. 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 хосты:

\*.kaspersky-labs.com

\*.kaspersky.com

## Сокращения

KAS: Анти-Спам Касперского

KSN: Kaspersky Security Network CGPro: CommuniGate Pro

# Установка Помощника CGP-KAS

В этом разделе описано, как устанавливать Внешний помощник CGP-KAS.

*cgpro\_home* - это путь к директории установленного CGPro.

### Установка из дистрибутива

Скачайте последнюю версию пакета для вашей системы по адресу: <https://www.communigatepro.ru/pub/plugins/Kaspersky/>

# cd *cgpro\_home*

# sudo tar xf *path/to/CGP-KAS*-Linux-amd64\_vX.Y.Z.tar.bz2

# sudo chown -R root:mail *cgpro\_home*/CGP-KAS

## CommuniGate Pro

Чтобы внешний помощник CGP-KAS обрабатывал почту, необходимо объявить этот новый помощник и создать SMTP-правило для вызова помощника на основе почтового потока.

### **Настройка внешнего помощника**

Чтобы добавить внешнего помощника CGP-KAS, в интерфейсе администрирования CGPro перейдите в

Установки → Общее → Помощники

Создайте новый помощник в разделе Фильтрация данных:

|  |  |  |
| --- | --- | --- |
| **Выключено** | AntiSpam |  |
| **Уровень журнала** | Все | **Путь к Программе** | CGP-KAS/CGP-KAS |
| **Тайм-аут** | 2мин | **Авторестарт** | 15сек |

### **Настройка SMTP-правил**

В данном примере показано, как сканировать все письма, направляемые через модуль LOCAL, который будет доставлять письма в почтовые ящики пользователей. Такие настройки означают, что любое письмо, отправленное даже от вас самих на ваш собственный почтовый ящик, будет направлено во Внешний помощник CGP-KAS.

Перейдите в раздел Установки → Почта → Правила

Добавьте новое правило с названием AntiSpam и нажмите Изменить

Добавьте в правило следующие параметры :

**Данные Операция Параметр**

Любой Маршрут равно LOCAL(\*

 –--

**Действие Параметр**

Внешний Фильтр AntiSpam

---

**Лицензии**

Убедитесь, что лицензии для внешнего помощника CGP-KAS добавлены в CGPro. Для этого откройте раздел интерфейса администратора CGPro Главное → Лицензия

Если лицензионные ключи помощника CGP-KAS добавлены, в списке будет запись, содержащая “Kaspersky AntiSpam”.

## **Запуск Внешнего помощника CGP-KAS**

### **Включение Внешнего помощника**

В интерфейсе администрирования CGPro перейдите в раздел Установки → Общее → Помощники и измените для Фильтра данных AntiSpam значение Выключено на Включено, после чего нажмите на кнопку Модифицировать.

### **Выключение Внешнего помощника**

В интерфейсе администрирования CGPro перейдите в раздел Настройки → Общее → Помощники и измените для Фильтра данных AntiSpam со значения Включено на Выключено. Обратите внимание, что движку KAS нужно порядка 15-30 секунд на корректное завершение работы.

### **Утилита диагностики**

Теперь можно убедиться, что движок KAS работает в вашей системе так, как ожидается, с помощью утилиты диагностики. Это не является обязательным перед запуском помощника. Она может быть использована в случае проблем с запуском внешнего помощника через CGPro. Пожалуйста, обратитесь к разделу Отладка внешнего помощника CGP-KAS для получения более подробной информации.

# cd *cgpro\_home/CGP-KAS*

# sudo ./diagnose

В случае успеха утилита диагностики выведет сообщение

INFO[0000] kas is OK.

Дополнительно в строке вывода можно будет увидеть версию сборки помощника, которая может потребоваться при обращении в службу поддержки.

# Настройка Внешнего помощника CGP-KAS

Этот раздел описывает параметры конфигурирования, которые находятся в

*cgpro\_home*/CGP-KAS/kas.conf

Конфигурационный файл регистрозависимый.

## Основные настройки

Основные настройки определены в блоке **[main]**.

Необходимо указать помощнику путь к инсталляции CGPro :

**cgpro\_home = /var/CommuniGate**

Помощник поддерживает два режима работы с CGPro для получения лицензий:

- по HTTP(S). Требуется указать логин и пароль администратора (по умолчанию, postmaster);

- через протокол помощника. В этом случае указывать логин и пароль администратора не нужно.

За режим работы отвечает параметр **cgpro\_httpa\_scheme**. Если требуется режим работы по HTTP(S), то этот параметр необходимо раскомментировать. По умолчанию установлен режим работы через протокол помощника.

 Политика отказов позволяет определить, как будет действовать Внешний помощник в случае сбоев при вызове движка KAS. Если политика фильтрации определена как отклонение сообщения, любая ошибка сканирования заставит Внешнего помощника отложить сообщение в очереди CGPro. Любая другая ошибка, кроме ключевого слова reject, будет указывать помощнику на то, что письмо должно быть доставлено (политика pass). В этом случае к письму добавляется заголовок ошибки (X-KAS-Error). Параметр политики отказа :

**failure\_policy = reject|pass**

 **Прим.** в случае возникновения фатальных ошибок при взаимодействии с движком (падение SDK) помощник возвращает Failure

Рабочие потоки позволяют настроить количество потоков, обрабатывающих очередь сообщений движком KAS.

**worker\_threads = 4**

Следующая настройка позволяет отсрочить запуск Внешнего помощника, чтобы убедиться, что CGPro доступен для получения лицензий:

**delay\_start = 0**

## Настройки Anti-Spam

Настройки антиспама задаются в разделе **[antispam]**.

Вы можете задать период времени в секундах, по истечении которого внешний помощник будет проверять наличие обновлений службы KAS. Для достижения максимальной точности при использовании этой технологии защиты от спама рекомендуется проверять обновления с интервалом от 1 до 5 минут. Значение по умолчанию - 1 мин:

**UpdateInterval = 1min**

Вы можете добавить собственные заголовки результатов в электронные письма после того, как они были успешно просканированы KAS:

**KAS\_Header\_Status = X-KAS-Status KAS\_Header\_Level = X-Junk-Score KAS\_Header\_Method = X-KAS-Method**

Смотрите подробности в разделе Заголовки результатов сканирования.

Вы можете задать таймаут сканирования (ScanningTimeout) в секундах, по истечении которого сканирование будет прервано и выдаст ошибку таймаута. В зависимости от политики отказа (reject или pass) в основном разделе конфигурации, письмо будет выпущено с заголовком ошибки или отложено для другой попытки. Значение по умолчанию для сканирования сообщений составляет 2 секунды:

**ScanningTimeout = 2sec**

Вы можете включить/отключить функции KAS, используемые для оценки электронной почты в соответствии с антиспамовыми детекторами:

**UseHeuristic = 1** // Проверка текстов сообщений с помощью лингвистического анализа

**UseDMARC = 1** // Использовать метод обнаружения спама DMARC

**UseLists = 1** // Использовать списки SURBL и DNSBL

**UseAntiPhishing = 1** // Использовать антифишинговое обнаружение спама

**UseGrahicalAnalysys = 1** // Использовать технологию обнаружения спама с графическим распознаванием (GSG)

**UseObsceneFiltration = 1 //** Анализировать сообщения на предмет нецензурной лексики. Такие сообщения помечаются специальным служебным заголовком

**# Следующие опции позволяют передавать данные в Kaspersky Security Network UseDNSHeuristic = 0** // Использовать обнаружение спама на основе DNS

**UseCloud = 0** // Обнаружение спама на основе облачных технологий (UDS, SURBL, URL Reputation)

 **UseEASUS = 0** // Использование Enforced Anti-Spam Updates Service (EASUS)

**UseReputationFiltering = 0** // Use Reputation Filtering spam detection

## Отладка внешнего помощника CGP-KAS

Для того чтобы внешний помощник мог вести полные журналы, необходимо активировать запись полных журналов в модуле сбора сообщений:

Почта → Очередь → Установка в очередь → Уровень журнала : Всё

Настройки для отладки находятся под заголовком **[debug]**.

## Режим подробного журналирования помощника

Чтобы отладить внутренние функции внешнего помощника, вы можете активировать режим verbose для различных модулей в секции **[debug]** конфигурационного файла kas.conf:

**DebugExternal = 0** // выводит информацию об ограничениях лицензии (значения 0,1)

**DebugFilterDaemon = 0** // выводит информацию о взаимодейтсвии с KAS (значения 0,1)

**DebugThreading = 0**  // отчёты о работе потоков (значения 0,1)

**DebugConfig = 0** // выводит актуальные конфиги помощника (значения 0,1)

**DebugCGateInput = 0** // выводит запросы, приходящие от CGPro (значения 0,1)

# Заголовки результатов сканирования

В этом разделе представлен обзор заголовков, добавляемых в письма, проверяемые внешним помощником Kas.

## Kaspersky Anti-Spam Engine

### Спам не обнаружен

**X-KAS-Status : KAS\_STATUS\_NOT\_SPAM**

**X-Junk-Score : []** // рейтинг по шкале от 0 до 100, каждый X означает 10. В этом примере - 0.

**X-KAS-Method: none**

### Спам обнаружен

**X-KAS-Status : KAS\_STATUS\_SPAM**

**X-Junk-Score : [XXX]** // рейтинг по шкале от 0 до 100, каждый X означает 10. В этом примере - 3.

**X-KAS-Method: *<method id>*** // метод, используемый для оценки письма

### Список статусов KAS

Список статусов, которые KAS Engine может присвоить письму, приведен ниже:

**KAS\_STATUS\_NOT\_SPAM KAS\_STATUS\_ERROR KAS\_STATUS\_SPAM KAS\_STATUS\_PROBABLE KAS\_STATUS\_AUTO\_RESPONDER**

**KAS\_STATUS\_BLACKLISTED KAS\_STATUS\_TRUSTED\_SOURCE KAS\_STATUS\_MASS\_MAIL KAS\_STATUS\_QUARANTINED**

### Ошибка

**X-KAS-Error : <message>** добавляется к письму при возникновении ошибки.

# Расширенные настройки

Расширенные настройки позволяют настроить сетевой прокси-доступ для сервиса KAS и получить доступ к тонкой настройке движка KAS.

Файл конфигурации KAS лежит по пути

*cgpro\_home*/CGP-KAS/KAS/etc/kassdk\_http\_server.cfg

Опции, вынесенные в kas.conf в раздел [antispam], управляются помощником и будут перезаписаны при старте помощника в случае расхождения со значениями в файле kassdk\_http\_server.cfg. Остальные опции настраиваются непосредственно в kassdk\_http\_server.cfg.

## Kaspersky Anti-Spam Engine

Файл, который необходимо отредактировать, чтобы получить доступ к конфигурации движка KAS:

*cgpro\_home*/CGP-KAS/KAS/etc/kassdk\_http\_server.cfg.template

### Настройки сетевых proxy

Отредактируйте файл конфигурации KAS и измените этот раздел в соответствии с параметрами вашего сетевого прокси-сервера:

**<ProxySettings>**

**<Host></Host>**

**<Port></Port>**

**<User></User>**

**<Pass></Pass>**

**<AuthType>NTLM|BASIC|AUTO</AuthType>**

**</ProxySettings>**

## Обновление лицензионных ключей KAS

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

# Настройки производительности

## Рекомендации Лаборатории Касперского по настройке KAS

Для повышения производительности движка KAS рекомендуется установить значения ThreadsCount и ScannersCount равными количеству логических ядер в системе. Производительность снизится, если вы добавите больше потоков или сканеров, чем доступно логических ядер. В случае, если оба параметра имеют разные значения, KAS Engine будет использовать минимальное из них.

Теоретически количество **worker\_threads** должно соответствовать количеству потоков обработчиков почты CGPro, определенному в:

Почта → Очередь → Установка в очередь → Обработчики

Теоретическое количество писем в секунду, которое может обработать CGP-KAS, составляет worker\_threads+5. Время, необходимое для проверки писем KAV/KAS, может уменьшить этот теоретический предел.