

<http://www.tffenterprises.com/cgpsa/>

==== CGPSA - A Spam Filter for [CommuniGate® Pro](#)
Version 1.7

==== Copyright © 2002-2010 TFF Enterprises
Written by [Daniel M. Zimmerman](#)
All Rights Reserved

CGPSA works in concert with [SpamAssassin™](#) software to scan email messages distributed by a [CommuniGate® Pro](#) server. The filter works efficiently, by directly using the SpamAssassin API. It does not rely on a daemon process such as spamd or on the execution of shell scripts (as the usual process for utilizing SpamAssassin with CommuniGate servers does). It can safely be used with multiple CommuniGate Pro enqueuer threads.

CGPSA supports all features of SpamAssassin, including such functionality as the use of [Razor](#), [DCC](#), Bayesian learning, and auto-whitelists. All these features are controlled through SpamAssassin's regular configuration files. For more information on SpamAssassin features and configuration, see the SpamAssassin [documentation](#).

Downloads

The most current (release) version of CGPSA can always be downloaded from <http://www.tffenterprises.com/cgpsa/cgpsa.tgz>. The current (release) version is [1.7](#), released 9 May 2010.

There is no current testing version of CGPSA.

Documentation

This documentation consists of the following sections:

- [Overview](#)
- [System Requirements](#)
- [Installation](#)
- [Upgrading](#)
- [License and Fees](#)
- [Bugs Reports, Feature Requests and the Like](#)
- [Revision History](#)
- [Future Plans](#)
- [Legal Stuff](#)

Overview

CGPSA has two basic operating modes, “[full-featured](#)” and “[headers-only](#)”.

Full-Featured Mode

Full-featured mode uses CommuniGate Pro's PIPE functionality to resubmit messages to the server after scanning, and can also use the CommuniGate Pro CLI to determine information about message recipients and load separate CGPSA settings and SpamAssassin settings for individual CommuniGate Pro domains and individual users. In this mode, email is scanned only for the recipients on the local system for whom scanning is turned on, and email for remote systems is always left unaltered. This is good, because SpamAssassin headers added according to your local policy may interfere with the spam filtering policy of a remote system. If a particular message is destined for both local and remote users, the local users receive a scanned copy and the remote users an unaltered one. Scanned email is treated exactly as SpamAssassin would treat it; for instance, if the SpamAssassin preferences say to rewrite the subject line of spam, a scanned spam will have a rewritten subject line.

At this time, there is no user interface to configure CGPSA settings and SpamAssassin preferences for individual domains and users; however, system administrators with access to the CommuniGate Pro base directory may take advantage of these features for their own use and that of the domains they administer. Individual user SpamAssassin preferences and state files are located in a `.spamassassin` directory inside the web directory corresponding to the account (`username.macnt/account.web`), and individual user CGPSA preferences are located in a `.cgpsa.conf` file within the same directory; domain CGPSA preferences are located in a `cgpsa.domainconf` file inside the domain's Settings directory, which can, among other things, specify the location to find the domain's SpamAssassin preferences and state files.

Headers-Only Mode

Headers-only mode does not use CommuniGate Pro's CLI or PIPE functionality. Instead, it adds headers to messages directly through CommuniGate's external filter interface. This has the benefit of being more efficient than using PIPE, because it does not require resubmission and reprocessing of messages. However, it also eliminates much of the advanced functionality, such as the use of individual preference and state files, and the ability to distribute unaltered messages to remote servers.

System Requirements

CGPSA requires the following in order to run:

1. CommuniGate Pro version 4.0 or higher (4.1 or higher preferred)
2. Perl version 5.6.1 or higher
3. [SpamAssassin](#) version 3.0 or higher
4. Additional Perl modules as required by the configuration options you choose for CGPSA and SpamAssassin (described in the installation steps below and in SpamAssassin's documentation).

Installation

Installation of CGPSA takes several steps. The following step-by-step instructions should enable you to get the filter working on your system (there are special instructions for Win32 systems throughout the steps). If you can't get it working, ask for help (as described below in [Bug Reports, Feature Requests and the Like](#)).

1. Install [SpamAssassin](#) on your system. The way to do this is platform dependent - on FreeBSD, for example, you might use the FreeBSD Ports system. Also install any auxiliary programs you want SpamAssassin to use, such as Razor and DCC. [Perl](#) is a prerequisite for SpamAssassin. Instructions for installing SpamAssassin on Win32 operating systems are available [here](#). On Win32, you *must* add RES_NAMESERVERS to your system environment variables to enable DNS lookups under Perl (this is discussed in the installation instructions for SpamAssassin).
2. Verify that the path in the first line of the cgpsa script points to the Perl executable on your system. If you have Perl in a different location (such as /usr/local/bin/perl or /opt/bin/perl), change the line accordingly. On Win32, this step is not required.
3. Verify that the \$cgp_base variable (listed under "Customizable Variables" near the top of the cgpsa script) contains the correct path to your CommuniGate Pro Base Directory (hereafter referred to as "CommuniGate directory"). The default path is /var/CommuniGate on most systems. On Win32, specify the location with a drive letter, using forward slashes (not backslashes) as separators: for example, C:/CommuniGate Files/ (the default base directory on Win32).
4. Install the cgpsa script inside your CommuniGate directory, and make sure it is executable. You can create a new subdirectory for it, or just put it at the top level; it doesn't really matter where it is, but make sure you know the full path to it (/var/CommuniGate/cgpsa, if it is at the top level of a default CommuniGate directory on UNIX) - you'll need the path later.
5. Install the cgpsa.conf configuration file into the Settings subdirectory of your CommuniGate directory. Modify any of the settings you want to change - they are all well documented in the configuration file itself.
6. Install customized cgpsa.domainconf configuration files into the Settings subdirectories of all domains (e.g., /var/CommuniGate/Domains/mydomain.com/Settings) for which you want customized CGPSA settings. You can modify any settings you choose in this file, but only those that explicitly indicate that they can be overridden at the domain level will be used. Also note that domain settings will only be used if CLI usage is enabled (see the next step for details).
7. If you are running CGPSA in its full-featured mode with CLI usage enabled, you must install the [CommuniGate Pro CLI Perl Module](#), CLI.pm. A version of CLI.pm is included with the CGPSA distribution. You can copy it to any of your system's Perl @INC directories, or just place it in the directory where you've installed cgpsa. CLI.pm requires the [Digest::MD5](#) Perl module; if you do not have it installed on your system, download and install it (or use the [CPAN](#) module to install it). If you have installed other scripts on your system that require the CommuniGate Pro CLI, you may already have installed CLI.pm; you do not need to reinstall it for CGPSA, though you should ensure that it's a recent version. If you are running in headers-only mode, or in full-featured mode without the CLI, you need not install CLI.pm for CGPSA to function.
8. If you are running CGPSA in its full-featured mode with CLI usage enabled, you must create a CommuniGate Pro account with PWD access (as described in the configuration file). Use the username and password specified in your cgpsa.conf. This user must have administrative access to all the domains for which you will be using CGPSA (the easiest way to do this is to

give it access to “modify and monitor everything”; at minimum, it should have access to modify “server and module settings” and “all domains and accounts settings”). Enable a number of PWD connections greater than the number of enqueueer threads used by your server. See the configuration file for details. If you are running in headers-only mode, or in full-featured mode without the CLI, you need not create an account for PWD access.

9. If you are running CGPSA in its full-featured mode with CLI usage enabled, and your CommuniGate Pro setup has IP addresses specifically assigned to domains, make sure that either you have specified “127.0.0.1” as an address associated with one of your domains or you have changed the “cgp_hostname” setting in `cgpsa.conf` to refer to a hostname or IP address on which the CommuniGate server is listening.
10. Create the “default home directory”, whose path is set in the configuration file (`cgpsa.conf`). This is where the default SpamAssassin preferences and state files will be stored - that is, those that are used in the absence of individual user preferences. If you have created customized settings for domains, and they have their own default home directory paths, create those directories as well.
11. Create a SpamAssassin configuration in the default home directory, if necessary. If the CommuniGate Pro server is the only software on your system using SpamAssassin, you can just use SpamAssassin's `local.cf` file (usually in `/etc/mail/spamassassin/`) to set up SpamAssassin's preferences. Otherwise, create a `.spamassassin` subdirectory inside the default home directory, containing a `user_prefs` file with the SpamAssassin preferences to be used by CGPSA. Repeat this step for the default home directories of any domains for which you want to use custom SpamAssassin preferences.
12. In the CommuniGate Pro web administration interface, go to the “Helper Settings” page (under “Settings/General”). In an empty “Content Filtering” section, enter a name for the filter (such as “CGPSA”). For the Program Path on UNIX, enter the full path to the filter (example: `/var/CommuniGate/cgpsa` - see step 4). For the Program Path on Win32, enter `perl` followed by the full path to the filter in quotes (example: `perl “C:\CommuniGate Files\cgpsa”`). Set the Log level to “Low Level” or “All Info” (for now). Leave “Time-out” set to “Disabled” unless you experience problems with the filter (be optimistic for the time being), and set “Auto-Restart” to a relatively small value (1 minute is reasonable). Finally, enable the filter and save your changes.
13. Examine the CommuniGate Pro log for the current day, and search for the string you entered as the filter's name in the previous step. You should see a line that reads similar to the following: “* TFF Enterprises CGPSA Filter (Version) Ready”. If you do not see this line, wait a few seconds and look again. If you still do not see it after a minute or so, something went wrong and there will likely be an error message in the log. If you can make sense of it and fix the problem, wonderful; if not, ask for help (as described below in [Bug Reports, Feature Requests and the Like](#)).
14. Go to the “Server-Wide Rules” page of the CommuniGate Pro web administration interface (“Settings/Rules”) and create a rule for CGPSA. The rule action should be “ExternalFilter CGPSA” (the name you assigned to the filter two steps ago). No rule conditions are necessary for proper operation, but greater efficiency will be attained with the following conditions: “Any Route is LOCAL*” and “Header Field is not X-TFF-CGPSA-Filter*” (or whatever you've changed the loop prevention header to). Note that omitting the first of these conditions means that mail distributed to remote servers will be scanned (which may not be a good idea - in full-featured mode with the CLI, CGPSA will automatically leave mail for remote servers alone, but in other modes, it scans every message passed to it).

If all went well, CGPSA is running and you're done. Send a test message to yourself and examine its headers to see whether it has been scanned. You may want to change the log level after running CGPSA for a while, because it does generate quite a lot of output (it's pretty interesting output, but if

you aren't writing/debugging the filter, much of it isn't too useful).

Upgrading

To upgrade from a previous version of CGPSA, perform the following steps:

1. Copy the new `cgpsa` and `CLI.pm` over the ones you currently have installed.
 2. Compare the configuration file (`cgpsa.conf`) that came with the new CGPSA to the configuration file you currently have installed. If there are any new configuration options that you want to use, add them to your installed configuration file. Alternatively, you can add your own customizations to the new configuration file and copy it over the old one. When upgrading from a pre-1.3 version to 1.3 or higher, you may also want to create domain and user settings files as described in step 6 of the installation instructions and in the included `cgpsa.conf` file.
 3. Restart CGPSA. There are two ways to do this. If you have "Auto-Restart" enabled for CGPSA in the CommuniGate Pro "Helper Settings", you can manually kill the running CGPSA process(es); this done with a command such as `killall cgpsa` (on Linux) or `pkill cgpsa` (on Solaris), or through a graphical interface such as Mac OS X's "Activity Monitor" or Windows' "Task Manager". If you cannot kill the running CGPSA processes, you can restart CGPSA using the "Helper Settings" page of the CommuniGate Pro web administration interface. In the "Content Filtering" section you made for CGPSA, uncheck the checkbox by "Use Filter", and then click "Update". Then, re-check the checkbox by "Use Filter" and click "Update" again.
 4. Examine the CommuniGate Pro log for the current day. You should see a line that reads "* TFF Enterprises CGPSA Filter (Old Version Number) Done", and slightly later a line that reads "* TFF Enterprises CGPSA Filter (New Version Number) Ready". If you don't see this, and it doesn't show up after a reasonable amount of time, restart your CommuniGate server (using the startup/shutdown script installed with CommuniGate). If CGPSA still doesn't start, ask for help (as described below in [Bug Reports, Feature Requests and the Like](#)).
-

Disclaimer

It is possible that CGPSA contains bugs, although it has proven to be quite stable on production systems. Any bugs that might exist in CGPSA are unlikely to cause the loss of email, because CommuniGate Pro is very intelligent about how it works with external filters - when a filter fails, the message stays enqueued. However, it is *possible* that email could be lost. There is no warranty, express or implied, associated with CGPSA; we will not be liable for any lost email. Use at your own risk.

License and Fees

CGPSA is non-commercial software, even though it has similar functionality to some existing commercial products. If you find it useful, feel free to send me something for it (email cgpsa@tffenterprises.com if you need information on how to do so). I also do CGPSA installations on a flat-fee basis.

Another way to provide some support for CGPSA's development is to do your [Amazon.com](https://www.amazon.com) shopping via the link in this sentence.

CGPSA is not to be redistributed without explicit permission. Its source code may not be used in any other products, in verbatim or modified form, whether or not the product is open-source. You may of course modify the source code in any way you like for use on your own system.

Bug Reports, Feature Requests, and the Like

Suggestions for feature improvements and bug fixes are gladly accepted. There is a mailing list for discussion about this filter, cgpsa-discuss@tffenterprises.com; this mailing list is the primary channel for support, discussion of feature requests and bug fixes, etc. It's a standard CGP mailing list: you can join it by emailing cgpsa-discuss-on@tffenterprises.com. I expect it to be pretty low traffic; if you don't want to join the list, though, send any questions, comments, rants, etc. to cgpsa@tffenterprises.com.

When sending a bug report, be sure to include any relevant information from the CommuniGate Pro log and the `cgpsa.err` log (located in the same directory as your `cgpsa.conf` file).

Revision History

1.7 - 9 May 2010

Major Changes

- CGPSA now requires SpamAssassin 3.0 or higher (and is compatible with SpamAssassin 3.3).
- Added options to set a score ("`temp_blacklist_score`") and duration ("`temp_blacklist_duration`") for temporary blacklisting, using the temporary blacklisting facilities of CommuniGate Pro releases that support it (thanks to Duane Hill for initial code).
- Added the ability to turn on spamd-style logging ("`spamd_style_log`") (thanks to Duane Hill for initial code).
- Added a setting for the maximum message length to scan ("`max_scan_length`"), instead of the previous 128K hard-coded limit (thanks to Duane Hill for initial code).
- Added a setting for the maximum length of a response to return to CommuniGate Pro ("`cgp_max_response_length`") (thanks to Duane Hill for initial code).
- Added header reduction and header inclusion settings ("`header_to_reduce`", "`headers_to_include`") to handle long sets of headers in an orderly fashion (thanks to Duane Hill for initial code).
- Added additional support for SQL-based user preferences.

Minor Changes

- Improved compatibility with SPF checking (thanks to Duane Hill for initial code).
- Extended the "`sa_debug`" parameter to enable the specification of specific SpamAssassin log facilities (such as "`check`") (thanks to Duane Hill for initial code).

Bug Fixes

- Fixed a long-standing bug where user-level SpamAssassin preferences would not be properly read and incorporated into the SpamAssassin preference set being used.

Known Issues

- Same as for Version 1.5 (all carried forward from Version 1.1)

1.5 - 23 August 2006

Major Changes

- Added support for SQL-based user preferences and auto-whitelists with new configuration options "sql_user_prefs" and "sql_auto_whitelist" (thanks to Stephane Claude and Duane Hill for spurring me to action on SQL support).
- Added support for scanning messages addressed to mailing lists with new configuration option "list_scan".
- CGPSA now strips "Envelope-To" headers from messages when scanning in full-featured mode, to prevent header-based relay trickery.

Minor Changes

- Moved CGPSA-generated headers to the top of the header block, so as to be friendlier to DomainKeys.

Bug Fixes

- Fixed a bug where, on newer versions of CommuniGate Pro, the combination of DMA spam filing and account detail (that is, an address of the form "foo+bar@email.com") caused spam to bounce rather than to be filed in the spam mailbox.
- Implemented a fix for broken domain directory paths on systems where the CLI does not return a reasonable value for (or does not support) GetDomainLocation.
- Fixed a bug where preferences for the root domain were improperly cached if the CLI was not in use.

Known Issues

- Same as for Version 1.4.

1.4 - 2 January 2005

Major Changes

- Added compatibility with SpamAssassin 3.x releases.
- Added support for CommuniGate Pro 4.2's domain foldering feature.

Minor Changes

- Removed support for loading domain configuration files named "cgpsa.conf"; all domain configuration files must now be named "cgpsa.domainconf".
- Updated the version of CLI.pm included in the CGPSA distribution.
- Changed log level assignment throughout CGPSA to make the range of log levels more useful. A log level of 4 is sufficient for "spam"/"non-spam" reports to make it into the CommuniGate Pro log; a log level of 7 is sufficient to provide all but the most detailed debugging log information.

The default log level, which used to be 9, has been changed to 8.

Known Issues

- Same as for Version 1.3.

1.3.5 - 2 December 2004

Bug Fixes

- Fixed an issue where above-threshold spam would always be discarded, regardless of configuration settings.

1.3.4 - 5 August 2004

Changes

- Added the ability to create a CGPSA domain configuration file for the CommuniGate Pro main domain.
- Changed the filename for domain configuration files from “cgpsa.conf” to “cgpsa.domainconf”. Files named “cgpsa.conf” continue to work in this release, but will not work in version 1.4.

1.3.3 - 19 June 2004

Bug Fixes

- Fixed an issue where user SpamAssassin preferences would not be loaded if there were no corresponding user CGPSA preferences.

1.3.2 - 24 April 2004

Changes

- Updated code and documentation to properly reflect that this version of CGPSA is incompatible with SpamAssassin 3.x releases.

1.3.1 - 10 April 2004

Changes

- Added configuration options “allow_domain_cgpsa_conf” and “allow_user_cgpsa_conf” to disable the use of domain-level and user-level CGPSA configuration files, respectively. This should improve performance (negligibly) and decrease the amount of log output (substantially) on systems where preference inheritance is not being used. By default, both domain- and user-level CGPSA configuration files are allowed.

Bug Fixes

- Fixed an issue where auto-whitelist databases at the server or domain levels would not be used, but auto-whitelist databases at the user level would be. All auto-whitelist databases should now work.
- Modified and fixed many logging statements to remove some redundancy and unnecessary output from the logs.
- Fixed the logging output to properly reflect the score and threshold of spam discarded by

CGPSA's auto-discard functionality.

1.3 - 28 March 2004

Major Changes

- Added domain- and user-level CGPSA preferences, domain-level SpamAssassin preferences, and preference inheritance. When a particular user's mail is scanned, the CGPSA and SpamAssassin preferences for that user are determined as follows: the default CGPSA and SpamAssassin preferences are used as a base; next, any domain-level CGPSA and SpamAssassin preferences for the user's domain are used to override the defaults; finally, any user-level CGPSA and SpamAssassin preferences are used to override the domain-level preferences. It is possible to turn off user-level preference overrides, or CGPSA itself, on a per-domain basis; there are also fine-grained controls over what can be overridden in user preferences (for example, you might allow a user to have their own SpamAssassin preferences but not to use auto-whitelisting).
- Added the ability to use direct mailbox addressing to place detected spam directly into users' spam mailboxes without the need for user-level rules; the spam mailbox names can be chosen on a server-wide, domain-wide, or individual user basis. CGPSA checks to be sure that direct mailbox addressing is enabled on the server before attempting to use it.
- Added two new configuration settings, "auto_discard" and "discard_threshold", that together add functionality to automatically discard spam messages that score above a specified threshold. This threshold, and the auto-discard setting, can be changed at the root, domain, and user levels.
- CGPSA now requires SpamAssassin 2.6 or higher.

Minor Changes

- If "direct_mailbox_rewrite" is enabled, CGPSA now checks to be sure that account detailing is enabled on the server before rewriting addresses.
- Log level assignment has been changed throughout CGPSA to make the range of log levels more useful. A log level of 5 is sufficient for "spam"/"non-spam" reports to make it into the CommuniGate Pro log; a log level of 8 is sufficient to provide all but the most detailed debugging log information.

Known Issues

- Same as for Version 1.2.

1.2.8 - 12 February 2004

Bug Fixes

- Fixed a problem where CLI initialization would not complete successfully if the CLI.pm perl module was installed in certain locations.

1.2.7 - 31 December 2003

Bug Fixes

- Fixed documentation of "direct_mailbox_rewrite" to indicate that the rewrite happens before the decision to scan mail rather than after (and that therefore, if "direct_mailbox_rewrite" is on, "direct_mailbox_scan" is superfluous).
- Fixed direct mailbox address processing. Previously, the "direct_mailbox_rewrite" option would

have caused mail to bounce, because instead of rewriting the address "mailbox#account@domain" as "account+mailbox@domain", it would rewrite it as "mailbox+account@domain".

- Fixed a problem where a log entry did not get properly pluralized when necessary.

1.2.6 - 26 December 2003

Bug Fixes

- Fixed a problem that could cause SpamAssassin state information (such as Bayes databases) to be written to the wrong place in the filesystem.

1.2.5 - 13 December 2003

Changes

- Added the ability to specify a path ("helper_path") to helper applications, such as DCC and Pyzor, that can be used by SpamAssassin. Previously, these applications could not be used with CGPSA.
- Documented a previously-existing undocumented configuration option ("helper_state_dir") that allows CGPSA to use a different directory for the state of helper applications, such as Razor, DCC and Pyzor, than the default home directory, when user preferences are not being used.

Bug Fixes

- Added newlines to some of the debugging output lines that were added in 1.2.4, to improve readability.

1.2.4 - 3 December 2003

Changes

- Added logic to ensure that CGPSA never tries to pass CommuniGate additional headers longer than 4096 characters in headers-only mode.
- Added a configuration option to turn on SpamAssassin's internal debugging (it is off by default).

Bug Fixes

- Fixed the reading of numeric settings (such as "max_requests" and "debug_level") from the configuration file.
- Fixed a bug where a data structure that tracked child processes could potentially grow without bound. This is likely what caused CPU and memory usage explosions in previous versions of CGPSA.

1.2.3 - 14 November 2003

Bug Fixes

- Removed an unintentional dependency on Time::HiRes that was introduced in version 1.2.2 (and caused CGPSA to crash).

1.2.2 - 14 November 2003

Changes

- Added configuration options for specifying the install prefix, system rules directory, and custom rules directory for SpamAssassin. This should allow CGPSA to work properly, without hackery such as duplicating entire directory trees, on systems such as Win32 where current versions of SpamAssassin do not seem to correctly compile paths into SpamAssassin.pm.
- Added code to use Time::HiRes, if present, to give more accurate timing for SpamAssassin processing.
- Perl 5.6.1 is now required to use CGPSA. This prevents various bugs in Perl 5.6.0 from affecting CGPSA's text processing.

Bug Fixes

- Fixed an issue where pathnames with spaces could not be used in the cgpsa.conf file (this was especially problematic for Windows users).

1.2.1 - 2 October 2003

Bug Fixes

- Fixed an issue where we inserted a duplicate X-Spam-Checker-Version header under SpamAssassin 2.6 in headers-only mode.
- Fixed an issue where we sometimes, while trying to get rid of SpamAssassin headers from other servers, ended up duplicating our own SpamAssassin headers.

1.2 - 17 September 2003

Changes

- Perl 5.6.0 or higher is now required to run CGPSA (this was unintentionally the case before, but CGPSA will die with a much more intuitive message now)
- SpamAssassin 2.5 or higher is now required to run CGPSA.
- The "max_requests" configuration option, which causes CGPSA to kill itself after processing a certain number of requests (to help combat memory leaks on systems where "parallel_requests" can't be used), has been added.
- Spurious X-Spam-* headers (that is, those added by SpamAssassin running on other servers) are now removed from messages when running in full-featured mode.
- Headers-only mode has been made compatible with SpamAssassin 2.60 series releases.
- "\e" has replaced "\n" as the line separator in headers constructed by CGPSA.

Known Issues

- Same as for Version 1.1.

1.1 - 27 July 2003

Changes

- Parallel requests mode is now turned on by default on non-Windows platforms.
- Modified the processing of message headers to preserve more information about the Envelope-To addresses.
- Added the ability to specify a list of destination domains that should always have their mail scanned, with the "scan_domains" setting. This makes it possible to use CGP as a relay/gateway server (to filter and process email for other domains).
- Added date/time stamp to the standard error output generated by CGPSA. Output generated by

other Perl code (such as SpamAssassin) is not date/time stamped.

- Changed CGPSA's output functions to wrap lines to a reasonable number of characters (around 150), to work around the CommuniGate log line length limit.
- Added signal handling: if the main CGPSA process receives a HUP, it reloads all of its own and SpamAssassin's preferences before processing the next CLI command it receives.
- Partially worked around the behavior whereby, when `parallel_requests` is off and `use_user_prefs` is on, users' SpamAssassin preferences get "stacked" on top of each other. Now, the SpamAssassin preferences in the default home directory are loaded before each set of user preferences, so they are "stacked" on top of the user prefs; this means that, if the default preferences file contains explicit settings for every parameter changed in a user preference file, SpamAssassin will return to these defaults between users.
- Worked around SpamAssassin's problem with extremely large messages, by only scanning the first 250K of each message.
- Changed the location of the per-user configurations used by CGPSA (old configurations will automatically be moved to the new location).

Known Issues

- If CGPSA has to truncate a message in order to scan it, that message will almost definitely trigger the SpamAssassin rule "MIME_MISSING_BOUNDARY". This probably won't cause non-spam messages to cross the spam threshold, but it is a possibility.
- When CGPSA catches a HUP signal and reloads its preferences, it leaks some memory (as a result of the old SpamAssassin, or parts thereof, not going away). This cannot be fixed with the current version of SpamAssassin; work is underway on a patch to SpamAssassin to enable a fix.
- Entries in the CGP log that are line-wrapped have "\t" as their leading character when CGPSA is used with Perl earlier than 5.8. This is a result of limitations in the older Text::Wrap code.

1.0.8 - 18 June 2003

Bug Fixes

- Fixed an issue with the generation of random filenames that could have, on certain systems, resulted in message loss when using parallel requests.

1.0.7 - 17 June 2003

Changes

- Added the ability to use per-user preferences in either the old location (the user's account directory) or the new location (the user's "account.web" directory). This is primarily so that users of the 1.1 betas can have a stable version to revert to without manually moving preferences back and forth.

Bug Fixes

- Fixed a bug where mail for "all@" and "alldomains@" addresses could have been delivered when it shouldn't have been. Mail to "all@" and "alldomains@" addresses is now scanned in ADDHEADER mode, to preserve CGP's security model for such mail.

1.0.6 - 5 May 2003

Changes

- Added an option (turned on by default) to redirect SpamAssassin's error output to a file rather than to standard error. This solves a problem that would cause the filter to hang on certain operating systems (including Mac OS X).
- Added information to log output about the paths to the SpamAssassin settings files being used; the path to the default settings file is output at filter startup time, and the paths to user settings files are output when those files are used.

Bug Fixes

- Fixed a race condition where CGPSA would check for the ability to connect to the CLI before the CommuniGate server was ready to accept connections to the PWD port.
- Fixed the entry for "default_home_dir" in the configuration file to accurately reflect its default value.

1.0.5 - 14 April 2003

Changes

- Added some extra debugging output in various places, including printing of the preferences file location and the SpamAssassin version at startup.
- Added support for the new "Route Mail" CLI command option (for CommuniGate 4.1b3 and higher; compatibility is auto-detected).

Bug Fixes

- Fixed a problem where mail to the "all@" and "alldomains" addresses would be bounced because of routing errors.
- Fixed a problem where CGPSA would use root's home directory to store SpamAssassin state files in certain configurations.
- Fixed a problem where the "cgp_hostname" setting was not being read from the configuration file.

1.0.4 - 2 April 2003

Changes

- Added the "use_c_locale" configuration option, to force the C locale to be used by Perl when running SpamAssassin (which has some known problems with certain locales). The default is to use the C locale.
- Added more logic to the headers-only mode, so that we now produce the same headers as SpamAssassin would if it were rewriting the message itself.
- Changed the text of the loop prevention header to read either "Scanned" or "Scan Failed", as appropriate (rather than "Attempted").
- Fixed a problem that occurred with SpamAssassin's "report_safe" option turned on, where an email identified as spam would be processed in an infinite loop.
- Added the "direct_mailbox_rewrite" and "direct_mailbox_scan" configuration options, and removed the "direct_mailbox_passthrough" configuration option. This allow for more flexibility when determining the scanning policy for direct mailbox addresses. The default settings are to not rewrite direct mailbox addresses, and to not scan mail for direct mailbox addresses.

1.0.3 - 30 March 2003

Changes

- Added the “parallel_requests” setting, which defaults to “false”. This addresses problems on Win32, and potentially on other platforms as well, with the mechanism currently used to process multiple emails in parallel.
- Changed the default settings for “use_user_prefs”, “require_user_prefs”, and “use_user_state” to “no”.
- Removed OS name and Perl version from X-TFF-CGPSA-Version header.
- Added clarification in the configuration file that the default home directory setting should not be quoted.

Bug Fixes

- Fixed a problem where the “headers_only” setting was not read properly.
- Fixed a problem where, if there was no default SpamAssassin preferences file and user preferences were not being used, no mail would be scanned.

1.0.2 - 27 March 2003

Bug Fixes

- Fixed a problem where the CGP CLI module wouldn't load properly if it wasn't found as “CGP/CLI.pm”.
- Fixed a problem where, under certain circumstances, Perl's Taint Mode (security infrastructure) prevented CGPSA from removing some temporary files used in SpamAssassin initialization.
- Fixed a non sequitur in the documentation.

1.0.1 - 27 March 2003

Changes

- Added the “install CGP::CLI” step to the installation instructions.
- Added runtime check for CGP::CLI module, so that it need not be installed if CGPSA is running with “use_cli” set to false (or in headers-only mode). The module can be installed as CGP/CLI . pm or just CLI . pm.

1.0 - 23 March 2003

Initial Release Version

Future Plans

A hypothetical future version of CGPSA will have a user interface to support individual auto-whitelists, Bayes databases, and SpamAssassin preferences for CommuniGate users. This hypothetical version of CGPSA will also be refactored to be somewhat more object-oriented and modular (because 2700-line Perl scripts are not the easiest things in the world to maintain).

Legal Stuff

CommuniGate is a registered trademark of Stalker Software, Inc.

[valid-xhtml11](#) Last modified by [Daniel M. Zimmerman](#) on 9 May 2010

From:

<https://wiki.kanaalweg.sasteren.nl/> - **Sasteren-Wiki**

Permanent link:

<https://wiki.kanaalweg.sasteren.nl/beheer/archimil/cgpsa>

Last update: **2026/06/01 10:55**

