# CustomRulesets

## Disclaimer

**Custom or third-party rules described here are not part of the official Apache SpamAssassin distribution. They may have a different license and are not from the Apache Software Foundation.**

## Available Custom Rulesets

Listed below are several custom rulesets that are available as "drop in" .cf files. To use these rules, just place the file in /etc/mail/spamassassin (if you use spamD, be sure to restart). Before running these rules please do the following:

1. Read any extra info available with the rules, including the comments in the .cf files.
2. Check to make sure that the default scores in these rules fit your installation. You might want to modify scores.
3. Make sure to --lint the rules after loading them.
4. Test the new rulesets. Keep an eye on hits from the new rules to determine if the scoring is right for you.
5. **Never use sa-update --allowplugins option**, it allows running any code on your server (usually even with root permissions).
6. SpamAssassin **version 3.4.6 or later** is strongly recommended, previous versions have many security vulnerabilities with .cf files.

**Use at your own risk.**

Rule sets which have been removed from the SpamAssassin distribution can be found at RemovedRulesets.

---

**Status Information**
Active: Ruleset is actively updated and maintained
Inactive: Ruleset is not actively updated, should be fine to run
Defunct: Ruleset is no longer maintained, not available, or maybe have serious problems

Auto-update: Author/Maintainer has given permission to use scripts to automate the download of the ruleset
Please respect the wishes of the authors and/or the site hosts
Users of the latest version on SpamAssassin should use sa-update, not Rules Du Jour, for auto-updates. This documented elsewhere in the Wiki and rulesets such as SARE.

---

**KAM.cf**
Collection of special rules KAM has developed and uses in production. With contributions by other authors.
Created by: Kevin A. McGrail
Contact: Kevin.McGrail@McGrail.com
License Type: Apache License, Version 2.0
Status: Active
Auto-update: Yes.
Available at: https://mcgrail.com/
Note: The full ruleset can be found in the *Downloads* section and consists of 4 cf files: `KAM.cf`, `nonKAMrules.cf`, `KAM_deadweight.cf` and `KAM_heavyweight.cf`. An update channel exists too.

**Malware Patrol (previously Malware Block List)**
Malware Patrol is an automated and user contributed system for checking URLs for the presence of Viruses, Trojans, Worms, or any other software considered Malware. The list of URLs that point to Malware is available and formatted for using on SpamAssassin.
Created by: Malware Patrol
Contact: support@malwarepatrol.net
License Type: ?
Status: Active
More information: https://www.malwarepatrol.net/spamassassin-configuration-guide/
Note: Requires registering an account. **Free for non-commercial use only.**

**German Language Ruleset**
Catches german language SPAM. Please report your german SPAM with full headers
Created by: Michael Monnerie ( http://protéger.at or http://proteger.at )
Contact: spam-german@zmi.at
License Type: Artistic
Status: Active
Available at: Homepage: http://sa.zmi.at/

**Greek Language Domain Ruleset**
Catches spams written in Greek or by Greek spammers or that target the .GR domain.
Created by: Dimitris Michelinakis
License Type: Artistic
Status: Active
Auto-update: Yes - Please try to keep checks down to no more than once every 24 hours
Available at: http://www.michelinakis.gr/Dimitris/spamassassin/gr_domain.cf
More information on the site: http://www.michelinakis.gr/Dimitris/spamassassin/

**Italian Language Domain Ruleset**
Catches spams written in Italian or by Italian spammers or that target the .IT domain.
Created by: Giovanni Bechis
License Type: Artistic
Status: Active
Auto-update: Yes
Available at: https://spamassassin.snb.it

**IP Reputation**
A free public email reputation system, basically a combined whitelist and blacklist. Uses more automated data collection. Results for people contributing data are looking better than anything else available for SpamAssassin.
Contact: Darxus
License Type: Apache, data is public domain
Status: Inactive (provided DNS service not updated since 2016?)
Available at: http://www.chaosreigns.com/iprep/
Sample Results: http://www.chaosreigns.com/iprep/#results

**Polish Language Ruleset 2**
Catches Polish language spam - invitations to receive more spam.
Created by: <lemat at lemat.priv.pl> & pl.internet.mordplik users,
License Type: Public Domain
Status: Inactive (last update 5/2019 at time of checking 4/2021)
Available at: http://lemat.priv.pl/pliki/sa_body_test_pl.cf
Auto-update: no

**MIME Validation Ruleset**
This is a tiny set of rules, designed to find MIME errors commonly encountered in mails sent by the bulk mailers used by spammers.
Created by: Byteplant GmbH
Contact: nstsupport@byteplant.com
License Type: GPL
Status: Inactive (last update 2013 at time of checking 4/2021)
Available at: http://antispam.byteplant.com/download/mime_validate.cf

## Defunct Custom Rulesets

Custom Rulesets which are no longer updated or available via any listed main source or mirror. Retained for now but moved out of the Available section.

Checked 4/2021.

**sought.cf**
**FORMERLY** an automatically-generated ruleset which seeks good rules directly from the SpamAssassin spamtraps.
Created by: Justin Mason
Contact: jm@jmason.org
License Type: same as SpamAssassin
Status: Defunct
Auto-update: No
More information: SoughtRules

**Polish Language Ruleset**
Catches Polish language spam; moved from the Spamassassin distribution after SA 3.1.8.
Created by: <radek at alter dot pl>, contributions by <adek at ines dot wonlok dot com dot pl>
Contact: <radek at alter dot pl>
License Type: Apache Software License 2.0
Status: Defunct
Available at: BodyTestsPl
Sample Results: None yet.

**antidrug.cf**
antidrug.cf is a set of rules designed to catch those pesky "pill spams".
Created by: Matt Kettler
Contact: mkettler_sa@verizon.net
License Type: Artistic/GPL dual
Status: Defunct
Auto-update: Yes, subject to change if Verizon later objects to the practice. Note: at this time the ruleset is not actively being updated.
Available at: http://mysite.verizon.net/mkettler_sa/antidrug.cf
Mirror: N/A
Note: Matt Kettler says "It may not be appropriate for a medical or pharmaceutical environment. If in doubt, adjust the scores of all the rules to 0.01 and see if they fire off on your daily nonspam."
Note: SA 3.0.0 documentation indicates that much of this rule set has been incorporated into that version. This file is unnecessary with SA 3.0.0 or higher and may downgrade any improvements contributed directly to the standard ruleset. ONLY use antidrug if you are stuck on SA 2.6x for some reason.
Sample Results: MasscheckAntidrug (rev 0.65 04/28/2004)

**backhair.cf**
backhair is a set of rules designed to catch those ugly, unsightly HTML tags.
Created by: Jennifer Wheeler
Contact: TBD
License Type: TBD
Status: Defunct
Auto-update: **No**
Available at: http://www.emtinc.net/includes/backhair.cf
Mirror: rulesemporium.com
More information on Jennifer's rules: http://www.emtinc.net/spamhammers.htm
**NOTE: Early versions of Rules Du Jour included this set in its default config. This set is now considered "stable" and is no longer actively updated. Please do not use auto-update scripts**
Note: This is a fairly aggressive ruleset that can hit on UUencoded attachments...
Note: SA 3.0.0 documentation indicates that much of this rule set has been incorporated into that version. This file is unnecessary with SA 3.0.0. Sample Results: MasscheckBackhair (Version 1.5 2004-01-21)

**chickenpox.cf**
chickenpox is a set of rules designed to catch spam like "l.ooks f|or th.is kind of garb+age"
Created by: Jennifer Wheeler
Contact: TBD
License Type: TBD
Status: Defunct
Auto-update: **No**
Available at: http://www.emtinc.net/includes/chickenpox.cf
Mirror: rulesemporium.com
**NOTE: Early versions of Rules Du Jour included this set in its default config. This set is now considered "stable" and is no longer actively updated. Please do not use auto-update scripts**
More information on Jennifer's rules: http://www.emtinc.net/spamhammers.htm
Sample Results: MasscheckChickenpox (Version 1.15 2004-02-06)
Chickenpox rules are BROKEN for non-English text, they treat all accented characters as non-letters!

**evilnumbers.cf**
evilnumbers is a collection of phone numbers, PO boxes and street addresses harvested from spam.
Created by: Matt Yackley
Contact: sare@yackley.org
License Type: Artistic
Status: Defunct
Auto-update: Yes - Please try to keep checks down to no more then once every 24 hours
Available at: http://www.rulesemporium.com/rules/evilnumbers.cf
Extras: Localized language packs available at the link below.
Mirror: yackley.org
More information on Matt Yackley's rules: http://www.yackley.org/sa-rules
Sample Results: MasscheckEvilNumbers (Version: 1.12k 03/31/2004)

**tripwire.cf**
tripwire searches for 3 characters that shouldn't be together.
Created by: Fred Tarasevicius
Contact: tech2@i-is.com
License Type: TBD
Status: Defunct
Auto-update: TBD
Available at: http://www.rulesemporium.com/rules/99_FVGT_Tripwire.cf
Note: These rules are based on the English language, due to the number of rules that can be triggered, problem have been reported by exim users that it can cause the header to go over the byte limit of the exim header limits, also MS Outlook can have problems with rules that look for "message headers" due to a unknown size limit in the amount of headers it will search.
Sample Results: MasscheckTripwire (Version 1.17)

**French Rules**
Catches spams written in French.
Created by: Maxime Ritter
Contact: mritter@alussinan.org
License Type: Public Domain
Status: Defunct
Auto-update: **On the mirror (updates of the mirror are automatic)**
Available at: http://maxime.ritter.eu.org/Spam/french_rules.cf
GPG-signature: Yes
Mirror: http://airmex.nerim.net/rule-get/french_rules.cf
More information on my site : (in French only at the moment) : http://maxime.ritter.eu.org/article.php3?id_article=11
Sample Results: None yet.

**Romanian Rules**
Catches spams written in Romanian or by Romanian spammers.
Created by: INTERSOL SRL
License Type: Public Domain
Status: Defunct
Auto-update: **On the mirror (updates of the mirror are automatic)**
Available at: http://www.intersol.ro/blacklist_ro.cf
More information on our site : (in Romanian only at the moment) : http://www.intersol.ro/anti-spam

**Airmax.cf**
Misc rules I use. Use them if you find them usefull.
Created by: Maxime Ritter
Contact: mritter@alussinan.org
License Type: Public Domain
Status: Defunct
Auto-update: **On the mirror (auto-updated)**
Available at: http://maxime.ritter.eu.org/Spam/airmax.cf
GPG-signature: Yes
Mirror: http://airmex.nerim.net/rule-get/airmax.cf
More information on my site : (in French only at the moment) : http://maxime.ritter.eu.org/article.php3?id_article=11
Sample Results: None yet.

**Chinese Rules**
Rules to catch spams written in Chinese.
Created by: Quang-Anh Tran, at CCERT Anti-Spam Team
Contact: chenguangying@tsinghua.org.cn
License Type: Apache License
Status: Defunct
Available at: http://www.ccert.edu.cn/spam/sa/Chinese_rules.cf (last updated 2006-10-01)
More information (in Chinese): http://www.ccert.edu.cn/spam/sa/Chinese_rules.htm
Note : Rules and scores are said to be updated once a week by using spams reported to the anti-spam service of CCERT in the last 3 months.
Sample Results: MasscheckChineserules

**GEE Whiz Chinese Ruleset**
We developed a set of SpamAssassin rules which apply to Simplified Chinese, based on GB2312. They include head rules, phrase rules.
Created by: Zhong(Adam) Wang at Submersion Corporation
Contact: adamwang@submersion.com
License Type: GPL
Status: Defunct
Available at: (no longer available)
More detail: (no longer available)
Note : Rules are masschecked by CCERT.
Sample Results: MasscheckGeeWhizChineseRuleset

I cleaned up part of GEE Whiz Chinese Ruleset which take forever to run mass-check and run perceptron to rescore the Ruleset Available at: http://mcli.homelinux.org:8080/apache2-default/spam
Contact: mchun.li@gmail.com

**Hebrew rules**
Status: Defunct
Available at: The Hebrew SpamAssassin rules project

**bogus-virus-warnings.cf**
bogus-virus-warnings tries to pick out 'collateral spam' caused by viruses.
Created by: Tim Jackson with contributions from others
Contact: TBD
License Type: TBD
Status: Defunct - deprecated by VBounce plugin
Auto-update: No
Available at: http://www.timj.co.uk/linux/bogus-virus-warnings.cf
More information on Tim's rules: http://www.timj.co.uk/linux/sa.php
Note: Main aim is to catch warnings generated by virus scanners along the lines of "you sent us virus", which are sent to the (usually faked) 'senders' of virus-infected e-mails. Contains many "black-and-white" very-high-scoring rules.
Sample Results: MasscheckBogusVirus (version 1.69 2004-03-04)

**sa-blacklist**
sa-blacklist is a large set of blacklist entries of domains and IP addresses.
Note: **IT IS STRONGLY RECOMMENDED YOU DO NOT USE THIS RULESET, SEE OutOfMemoryProblems**
Created by: William Stearns
Contact: wstearns@pobox.com
License Type: GPL
Status: Defunct
Auto-update: Yes - Please try to keep checks down to no more then once every 4 hours
Auto-update: Preferred method **rsync** via rsync.sa-blacklist.stearns.org::wstearns/sa-blacklist/
Available at: http://www.sa-blacklist.stearns.org/sa-blacklist/sa-blacklist.current
Available at: ftp://ftp.sa-blacklist.stearns.org/pub/wstearns/sa-blacklist/sa-blacklist.current
Mirror: ftp.bascom.com
More information on Bill's rules: http://www.sa-blacklist.stearns.org/sa-blacklist/README
Note: **IT IS STRONGLY RECOMMENDED YOU DO NOT USE THIS RULESET, SEE OutOfMemoryProblems**
Note: These are blacklist entries and will tag emails on their own! This link is not a .cf file, you will need to save it with a .cf extension.

**sa-blacklist-uri.cf**
sa-blacklist-uri is a large set of URIs
Note: **IT IS STRONGLY RECOMMENDED YOU DO NOT USE THIS RULESET, SEE OutOfMemoryProblems**
Created by: William Stearns
Contact: wstearns@pobox.com
License Type: GPL
Status: Defunct
Auto-update: Yes - Please try to keep checks down to no more then once every 4 hours
Auto-update: Preferred method **rsync** via rsync.sa-blacklist.stearns.org::wstearns/sa-blacklist/
Available at: http://www.sa-blacklist.stearns.org/sa-blacklist/sa-blacklist.current.uri.cf
Available at: ftp://ftp.sa-blacklist.stearns.org/pub/wstearns/sa-blacklist/sa-blacklist.current.uri.cf
More information on Bill's rules: http://www.sa-blacklist.stearns.org/sa-blacklist/README
Mirror: ftp.bascom.com
Note: The idea behind this list is similar to bigevil, but are pulled together from different spam. These rules are "flat" ie, one entry per rule, which uses more memory than combining multiple entries into one rule. This should not be an issue if you have lots of memory or a lighter mail load.
Note: **IT IS STRONGLY RECOMMENDED YOU DO NOT USE THIS RULESET, SEE OutOfMemoryProblems**
Sample Results: MasscheckBlacklist (2004030403)

**sa-random.cf**
sa-random searches for spamware mistakes like: %RANDOM_WORD
Created by: William Stearns
Contact: wstearns@pobox.com
License Type: GPL
Status: Defunct
Auto-update: Yes - Please try to keep checks down to no more then once every 4 hours
Auto-update: Preferred method **rsync** via rsync.sa-blacklist.stearns.org::wstearns/sa-blacklist/
Available at: http://www.sa-blacklist.stearns.org/sa-blacklist/random.current.cf
Available at: ftp://ftp.sa-blacklist.stearns.org/pub/wstearns/sa-blacklist/random.current.cf
Mirror: ftp.bascom.com
More information on Bill's rules: http://www.sa-blacklist.stearns.org/sa-blacklist/README
Sample Results: MasscheckRandom (release: 2004030501)