Exim Configuration Manager - Basic Editor

(*WHM >> Home >> Service Configuration >> Exim Configuration Manager*)

Overview

Select the *Basic Editor* tab in the *Exim Configuration Manager* interface to modify the settings for your server's Exim configuration.

Basic Editor options

Click a tab below to view options for the associated tab in the WHM interface.

> **Note:**
> The *All* tab displays the options for all of the *Exim Configuration Manager* tabs.

ACL Options Access Lists Domains and IPs Filters Mail RBLs Security Apache SpamAssassin™ Options

> **Notes:**
> - The *ACL Options* options limit who can send mail to your server. Use these options to minimize bandwidth usage, prevent spam, and block emails with a forged sender address (spoofed emails).
> - The system discards any email messages that it rejects at SMTP time.

Option	Description

Apache SpamAssassin™ reject spam score threshold	This option sets the spam score that Apache SpamAssassin™ uses to reject incoming messages. • Enter a positive or negative number, which may contain a single decimal point. **Important:** If you enter a value that contains an integer greater than or less than 0 and a decimal point, Apache SpamAssassin multiplies the value that you enter by a measure of ten. For example, if you enter a spam score threshold of 1.6, Apache SpamAssassin sets the threshold to 16. For example, if you enter a spam score threshold of `1.0`, Apache SpamAssassin sets the threshold to `10`. • Select *No reject rule by spam score* to disable this option. For more information, visit Apache SpamAssassin's documentation.
Dictionary attack protection	This option allows you to drop and rate-limit hosts with more than four failed recipients, in order to block dictionary attacks. A dictionary attack is a method whereby a malicious user attempts to guess a password with words in a dictionary.
Reject remote mail sent to the server's hostname	This option allows you to reject messages in which the recipient exists as an address of your server's primary hostname. In general, the primary hostname, a common target for spammers, should **not** receive remote mail.
Enable Apache SpamAssassin™ for secondary MX domains	This option configures Apache SpamAssassin to scan email for domains that exist in the `/etc/secondarymx` file which users send to the primary mail exchanger.

Ratelimit suspicious SMTP servers	This option allows you to rate-limit incoming SMTP connections that violate RFCs. This setting rate-limits mail servers that do not send `QUIT`, recently matched an RBL, or recently attacked the server. Real mail servers **must** follow RFC specifications. **Note:** To ensure that the system does **not** rate-lim it an SMTP connection, add the server to a whitelist. • This allows the system to deliver mail from connections that violate RFCs to your inbox. • To add a server to a whitelist, edit the *O nly-verify-recipient* setting in the *Access Lists* tab, and enter the IP address of the trusted server.
Apache SpamAssassin™: ratelimit spam score threshold	This option allows you to rate-limit hosts that send spam to your server. When you activate this option, rate limits delay email from hosts that send you spam. The system activates rate limits when it meets **both** of the following conditions: 1. A host reaches or exceeds the Apache SpamAssassin score that you enter in the text box. 2. That host exceeds the number of emails that the rate-limit formula specifies. **Notes:** • By default, the system uses the following rate-limit formula: `ratelimit = 1.2 / 1h / strict / per_conn / noupdate` • Exim averages rate limits over time.

Ratelimit incoming connections with only failed recipients	This option allows you to rate-limit incoming SMTP connections that only send email to failed recipients during five separate connection times in the past hour.
Require HELO before MAIL	This option allows you to require that incoming SMTP connections send a HELO command before they send a MAIL command. **Note:** A HELO is a command that mail servers send before an email, and that specifies the name of the sending domain. Apache SpamAssassin can perform various checks on this information (for example, it can ensure that the domain name matches the IP address that sent the message). This ensures that your server does not receive spam that reports a false domain name.
Introduce a delay into the SMTP transaction for unknown hosts and messages detected as spam.	This option configures the SMTP receiver to wait a few additional seconds for a connection when it detects spam messages. Typically, legitimate mailing systems will wait past the delay, whereas spammers do not wait past the delay. **Note:** The system excludes the following remote hosts from the delay: • Neighbor IP addresses in the same netblock • Loopback addresses • Trusted Hosts • Relay Hosts • Backup MX Hosts • Skip SMTP Checks Host • Sender Verify Bypass Hosts

	Warning:
	• If you use third-party sites to diagnose mail server issues, this setting may falsely detect spam messages.
	• If your external monitoring system reports failures after you update your server, configure your monitoring system to allow 45 seconds timeout for connections to port 25. For more information about how to adjust the timeout and polling settings, read your monitoring system's documentation.
	  • If that does not resolve the problem, add the IP address of your monitoring system to the *Trusted SMTP IP Addresses* section of WHM's *Exim Configuration Manager* interface *(WHM >> Home >> Service Configuration >> Exim Configuration Manager)*.
	  • If you still encounter errors on your monitoring system, disable the *Introduce a delay into the SMTP transaction for unknown hosts and messages detected as spam* setting in the *Basic Editor* section of WHM's *Exim Configuration Manager* interface *(WHM >> Home >> Service Configuration >> Exim Configuration Manager)*. However, this will likely result in an increase in spam that your server receives.

Do not delay the SMTP connections for hosts in the Greylisting "Trusted Hosts" list	This option configures the SMTP receiver to not delay any hosts that you add to the list in the *Trusted Hosts* tab in WHM's *Greylisting* interface *(WHM >> Home >> Email >> Greylisting)*.
Do not delay the SMTP connections for hosts in the Greylisting "Common Mail Providers" list	This option configures the SMTP receiver to not delay any hosts that you add to the list in the *Common Main Providers* tab in WHM's *Greylisting* interface *(WHM >> Home >> Email >> Greylisting)*.

Require remote (hostname/IP address) HELO	This option allows you to require that incoming SMTP connections send a HELO command that does not match the primary hostname or a local IP address (IPv4 or IPv6). Enable this option to block emails with a forged sender address (spoofed emails).
Require remote (domain) HELO	This option allows you to require that incoming SMTP connections send a HELO command that does not match your server's local domains. Enable this option to block emails with a forged sender address (spoofed emails).
Require RFC-compliant HELO	This option allows you to require that incoming SMTP connections send a HELO command that conforms with the Internet standards in RFC 2821 4.1.1.1. **Note:** If you enable this setting, it overrides any entries in the `/etc/alwaysrelay` and `/etc/relayhosts` files.
Allow DKIM verification for incoming messages	This option allows you to use DomainKeys Identified Mail (DKIM) verification to verify incoming messages. **Warning:** This verification process can slow your server's performance.
Reject DKIM failures	This option allows you to reject email at SMTP time if the sender fails DKIM key validation. **Note:** This option appears when you set the *Allow DKIM verification for incoming messages* option to *On*.

Maximum message recipients (soft limit)	This option allows you to determine the number of recipient addresses your server accepts in a single message. Select *No rejection based on number of recipients* to disable this option. **Note:** RFCs specify that SMTP servers **must** accept at least 100 RCPT commands for a single message.
Maximum message recipients before disconnect (hard limit)	This option allows you to determine the number of recipient addresses that your server permits in a single message before it disconnects and rate-limits a connection. Select *No disconnection based on number of recipients* to disable this option. **Note:** RFCs specify that SMTP servers **must** accept at least 100 RCPT commands for a single message.

Note:
The *Access Lists* options further limit who sends mail to your server.

Option	Description

Automatically whitelist known mobile device providers	This option allows you to add known mobile device providers to a whitelist. If you enable this option, messages from known mobile device providers bypass the mail filter. **Note:** The system stores information about mail providers in the `/etc/mailproviders/*` directory. Currently, the only cPanel-provided file in this directory is the `/etc/mailproviders/rim/ips` file, which contains IP addresses for Blackberry devices. To add other mobile device providers to the whitelist, manually add the desired IP addresses to this file.
Blacklisted SMTP IP addresses	This option allows you to edit the list of blacklisted SMTP IP addresses. The system does **not** allow these IP addresses to connect to the SMTP server, and instead drops connections with a 550 error.
Sender verification bypass IP addresses	This option allows you to edit the list of IP addresses that the system excludes from SMTP sender verification checks.
Only-verify-recipient	This option allows you to edit the list of hosts or IP addresses that the system excludes from all spam checks at SMTP connection time, except recipient verification checks. The system adds any hosts or IP addresses you enter here to the `/etc/trusted mailhosts` file.

Trusted SMTP IP addresses	This option allows you to edit the list of hosts or IP addresses that the system excludes from the following checks at SMTP connection time: • Recipient verification checks • Sender checks **Note:** These senders **must** still use an RFC-compliant HELO name if the Require RFC-compliant HELO setting is enabled. • Spam checks • Relay checks. The system adds any hosts IP addresses that you enter here to the /etc/skipsmtpcheckhosts file.
Backup MX hosts	This option allows you to edit the list of hosts from which the system permits SMTP connections, regardless of rate limits. Make certain that you properly configure reverse DNS records for any hosts which you enter here.
Trusted mail users	The *Trusted mail users* option allows system administrators to designate certain users as trusted mail users. This option affects the *EXPERIMENTAL: Rewrite From: header to match actual sender* setting in the *Mail* tab. Trusted users can bypass the *EXPERIMENTAL: Rewrite From: header to match actual sender* setting. The *Trusted mail users* option allows the listed users to modify their *From:* header, and the *EXPERIMENTAL: Rewrite From: header to match actual sender* setting does **not** override these changes. Enter the trusted mail usernames or their email addresses, one per line.

Note:
The *Domains and IPs* options change the IP address from which Exim sends mail. If you disable these options (the default), Exim automatically sends mail from your server's main shared IP address. For more information, read our How to Configure the Exim Outgoing IP Address documentation.

Option	Description

Send mail from account's dedicated IP address	This option allows you to automatically send outgoing mail for users without a dedicated IP address from a reseller's main shared IP address instead of the server's main IP address. If you enable this option, the `/usr/local/cpanel/scripts/updateuserdomains` file automatically populates the `/etc/mailhelo` and `/etc/mailips` files. • This prevents the use of the *Reference /etc/mailhelo for outgoing SMTP HELO* and *Reference /etc/mailips for outgoing SMTP connections* options. • If you enable this setting, the system **will** overwrite any manual changes that you subsequently make to the `/etc/mailhelo` and `/etc/mailips` files. **Warnings:** • If you enable this setting, make **certain** that your provider's reverse DNS entries are valid. For more information about how to configure reverse DNS entries, read our How to Configure Reverse DNS for BIND in WHM documentation. • This setting **only** applies to IPv4 addresses.
Reference /etc/mailhelo for outgoing SMTP HELO	This option allows you to send a HELO command that is based on the domain name in the `/etc/mailhelo` file. For more information, read our How to Configure the Exim Outgoing IP Address documentation.
Reference /etc/mailips for outgoing SMTP connections	This option allows you to send outgoing mail from the IP address that matches the domain name in the `/etc/mailips` file. For more information, read our How to Configure the Exim Outgoing IP Address documentation.

Note:
The *Filters* options allows you to select and configure filters that can block spam and potentially dangerous attachments.

Option	Description
System Filter File	Use this option to enable or disable Exim's system filter file, which the system stores in the `/etc/cpanel_exim_system_filter` file. Select one of the following settings: • *None (default)* — Select this option to disable Exim's system filter file • */etc/cpanel_exim_system_filter* — Select this option to enable Exim's system filter file. This is the default setting. • You can also choose to specify and customize another Exim system filter file. **Warning:** Regardless of the option that you select, the Exim configuration includes all of the files in the `/usr/local/cpanel/etc/exim/sysfilter/options/` directory.

Attachments: Filter messages with dangerous attachments	Select this option to filter email messages that contain potentially dangerous attachments. ˅ Click here to view the list of extensions that the system detects by default... .ade .adp .bas .bat .chm .cmd .com .cpl .crt .eml .exe .hlp .hta .inf .ins .isp .js .jse .lnk .mdb .mde .msc .msi .msp .mst .pcd .pif .reg .scr .sct .shs .url .vbs .vbe .wsf .wsh .wsc
Apache SpamAssassin™: Global Subject Rewrite	Select this option to prefix the *Subject* header with information from the *X-Spam-Subject* header and omit the *X-Spam-Subject* header.

Apache SpamAssassin™: bounce spam score threshold	Select this option to define the spam score that Apache SpamAssassin uses to bounce incoming messages. • Enter a positive or negative number, which may contain a single decimal point. • By default, the system disables this option. For more information, read the Apache SpamAssassin documentation.
Apache SpamAssassin™: X-Spam-Subject/Subject header prefix for spam emails	Select this option to use the default *X-Spam-Subject* header prefix for spam email or to enter a custom prefix. **Note:** You can use an Exim variable as a custom prefix. For a complete list of Exim's variables, read Exim's documentation.

Note:
The *Mail* options allow you to configure specific incoming mail options.

Option	Description
Log sender rates in the exim mainlog. This can be helpful for tracking problems and/or spammers.	This option allows you to log sender rates in the Exim mail log.
Sender Verification Callouts	This option allows Exim to connect to the mail exchanger for an address. This allows Exim to verify that the address exists before Exim accepts the message.
Smarthost support	This option allows you to use a smart host for outgoing messages. To configure this option, enter a valid `route_list` value in the *Smarthost support* text box.

Important:

- If you enter IPv6 addresses, you **must** enclose the IP addresses in quotes and begin the list with `</` to cause Exim to use slashes (`/`) as separators. Otherwise, Exim will interpret the colons in each IPv6 address as separators, and use each segment of the IPv6 address as a separate host.
- If you do not enter an asterisk before the IP address or addresses, the smart host will **not** function.

- To configure a smart host that uses one IP address, enter an asterisk (*) followed by an IPv4 or IPv6 address. For example:

```
* 192.168.0.1
```

```
* "</
2001:0db8:85a3:0042:1000:8
a2e:0370:7334"
```

- To configure a smart host that uses multiple IP addresses, enter an asterisk, followed by the IP addresses. For example:

```
*
192.188.0.20:192.188.0.21:
192.188.0.22
```

```
* "</
[2001:0db8:85a3:0042:1000:
8a2e:0370:7334]:1225 /
[::1]:1226 / 192.168.0.1"
```

- To configure a smart host that uses only specific domains from the hosts that you enter, replace the asterisk with the desired domain name. Separate entries for multiple domain names with a semicolon (;). For example:

```
example.com
192.188.0.20:192.188.0.21:
192.188.0.22;
exampletwo.com 192.168.0.1
```

```
example.com "</
[2001:0db8:85a3:0042:1000:
8a2e:0370:7334]:1225 /
[::1]:1226 / 192.168.0.1";
exampletwo.com "</
2001:0db8:85a3:0042:1000:8
a2e:0370:7334"
```

	For more information, read the Exim route_list documentation.
EXPERIMENTAL: Rewrite From: header to match actual sender	This option rewrites the *From* header in emails to show the original identity of the actual sender for messages sent from your server. • Email recipients can see the original *From* header as *X-From-Rewrite*, as well as the rewritten *From* header. • Use this option to determine the actual mail sender. For more information, read the EXPERIMENTAL: Rewrite From: header to match actual sender section below.
Send generic recipient failure messages	This option allows you to send the following message to senders who attempt to send an undeliverable message: `The recipient cannot be verified. Please check all recipients of this message to verify they are valid.`
Allow mail delivery if malware scanner fails	This option allows the system to deliver mail if the malware scanner if it fails. If you select *On,* in the event of a malware scanner failure, the server delivers all mail normally. **Note:** If you select *Off* and the malware scanner fails, users do **not** receive new messages until you repair the malware scanner.
Sender Verification	This option allows you to verify the origin of mail senders.

Set SMTP Sender: headers	This option allows you to set the *Sender:* header as *-f flag passed to sendmail* when a mail sender changes. **Notes:** • This setting defaults to *Off.* • If you set this option to *Off*, Microsoft® Outlook® will **not** add an *On behalf of* h eader. This may limit your ability to track abuse of the mail system.
Allow mail delivery if spam scanner fails	This option allows you to disable the spam scanner if it fails. If you select *On*, the system delivers all mail normally in the event of a spam scanner failure. **Notes:** • This setting defaults to *On.* • If you select *Off* and the spam scanner fails, users will **not** receive new messages until you repair the spam scanner.

Enable Sender Rewriting Scheme (SRS) Support:	This option rewrites sender addresses so that the email appears to come from the forwarding mail server. This allows forwarded email to pass an SPF check on the receiving server **Notes:** • This setting defaults to *Off*. • This setting uses the default configuration for SRS. If you wish to customize the SRS configuration, use the *Advanced Editor* interface. **Warning:** Sender Rewriting Scheme (SRS) will **not** fu nction correctly if the external mail server's autoresponder replies to the Sender address instead of the From address.
Query Apache server status to determine the sender of email messages sent from processes running as nobody	This option allows the mail delivery process to query the Apache server to determine the true sender of a message when the `nobody` user sends a message. • This option requires an additional connection to the server for each message that the `nobody` u ser account sends when suPHP and the mod_ruid2 module are both disabled. • This option is more secure, but it is faster to trust the *X-PHP-Script* headers. This option defaults to *On*.

Trust X-PHP-Script headers to determine the sender of email messages sent from processes running as nobody	This option allows Exim to trust messages that the nobody user sends with *X-PHP-Script* headers. This option also enables the mail server to determine the true sender. This provides a faster delivery process than a query to the Apache server to determine the sender. **Note:** Advanced users may forge this header. If your users may misuse this function, disable this option and send a query to the Apache server to determine the sender of nobody messages.
Hosts to which to advertise the SMTP DSN option	This option allows you to specify a list of hostnames to which to advertise SMTP Delivery Status Notification (DSN) support. Enter a list of hostnames to which to advertise the SMTP DSN extension in the text box, or an asterisk (*) to advertise to all of the hosts on the Internet. This option defaults to *Disabled for all hosts*. **Note:** For more information about SMTP DSN support, read ietf.org's RFC 3461 documentation.

Hosts to which to advertise the SMTPUTF8 SMTP option	This option allows you to specify a list of hostnames to which to advertise SMTP support for international email addresses that contain UTF-8 characters. Enter a list of hostnames to which to advertise the SMTP UTF-8 support in the text box, or an asterisk (*) to advertise to all of the hosts on the Internet. This option defaults to *Disabled for all hosts*. **Note:** For more information about SMTPUTF8 support, read ietf.org's RFC 6531 document ation.

EXPERIMENTAL: Rewrite From: header to match actual sender

This option rewrites the *From* header in emails to show the original identity of the actual sender for messages sent from your server. Email recipients can see the original *From* header as the *X-From-Rewrite* header as well as the rewritten *From* header. This option is useful to determine the actual mail sender.

Note:
This option does **not** affect mail that you receive from a remote host. The system only rewrites the *From* header for mail that it sends from the local machine because it is not possible to determine or validate the actual mail sender from remote machines.

System administrators can choose the following settings for this option:

Setting	Description	Conditions

remote	This setting uses SMTP to rewrite the *From* header in outgoing emails to match the actual sender.	• If a local user sends mail to a user on a remote host, this setting rewrites the *From* hea der. • If a local user receives mail from a user on a remote host, this setting does **not** rewrite the *From* header because it is not possible to determine the authenticated sender. • If a local user sends mail to another local user on the same server, this setting does **not** rewrite the *From* header because this is not a remote delivery. • If a local user receives mail from another local user on the same server, this setting does **not** rewrite the *From* header.
all	This setting rewrites the *From* he ader in all outgoing emails to match the actual sender.	• If a local user sends mail to a user on a remote host, this setting rewrites the *From* hea der. • If a local user receives mail from a user on a remote host, this setting does **not** rewrite the *From* header because it is not possible to determine the authenticated sender. • If a local user sends mail to another local user on the same server, this setting rewrites the *From* header because this option includes local deliveries. • If a local user receives mail from another local user on the same server, this setting rewrites the *From* header because the sender already rewrote the *From* header.

disable	This setting does **not** rewrite the *From* header in any email. **Note:** This is the default setting.	Not applicable.

In order to conduct an attack or send unsolicited email, a malicious user can alter the *From* header in an email to confuse the recipient. For example, a user may authenticate as `user@example.com` and send a message with the *From* header set to `account@forged.example.com`. When you enable this option, Exim rewrites the *From* header to show the authenticated sender (`user@example.com`).

To avoid a potential problem, system administrators can enable this option to ensure that the *From* header for mail sent from their servers always matches one of the following methods:

Method	Example
The actual sender.	If you authenticate as `user@example.com`, the *From* header will **always** display `user@example.com`.
An email address to which the sender has access.	If you authenticate as the `username` user, set the *From* header to any email account that the `username` user controls.
An email address that has been forwarded to the actual sender.	If `user@example.com` is an email address on your server and it forwards mail to `account@domain.org`, then `account@domain.org` may set the *From* header to either address.

Note:
The *RBLs* options allow you to configure your mail server to check incoming mail against the available Real-time Blackhole Lists (RBLs). Your server blocks the incoming messages if the IP address or hostname matches an RBL entry.

RBL servers store lists of spam-heavy IP addresses and hostnames so that you can easily block them. The WHM interface accesses two RBLs: bl.spamcop.net and zen.spamhaus.org.

Option	Description
Manage Custom RBLs	Click *Manage* to view and manage your server's RBLs. A new interface will appear. The *Current RBLs* table lists the following information for each RBL:

Column	Description
Origin	The source of the RBL. • *Custom* indicates that you added the RBL. • *System* indicates cPanel-included RBLs.
RBL name	The RBL's name.
DNS list	The RBL's DNS list.
Info URL	The RBL information URL.
Action	For custom RBLs, click *Delete* to remove the RBL. **Note:** You **cannot** delete cPanel-included RBLs.

To add an RBL, enter the appropriate information in the text boxes and click *Add*.

Notes:

- Make certain that you choose an RBL name that allows you to remember the DNS list for this RBL.
- After you add custom RBLs, each custom RBL will appear at the bottom of the *RBLs* options tab. Select *On* to enable a custom RBL.
- Custom RBLs default to *Off*.

RBL: bl.spamcop.net	This option allows you to reject mail at SMTP-time if the sender's host is in the bl.spamcop.net RBL. For more information, visit the bl.spamcop.net website.
RBL: zen.spamhaus.org	This option allows you to reject mail at SMTP-time if the sender's host is in the zen.spamhaus.org RBL. For more information, visit the zen.spamhaus.org w ebsite.
Exempt servers in the same netblock as this one from RBL checks	This option allows you to disable RBL checks of mail from servers in the same IANA netblock.
Exempt servers in the Greylisting "Common Mail Providers" list from RBL checks	This option allows you to disable RBL checks of mail from an IP address block that you include in the *Common Mail Providers* list in WHM's *Configure Greylisting* interface *(WHM >> Home >> Email >> Configure Greylisting)*. This option defaults to enabled.
Exempt servers in the Greylisting "Trusted Hosts" list from RBL checks	This option allows you to disable RBL checks of mail from IP address blocks that you include in the *Trusted Hosts* list in WHM's *Configure Greylisting* in terface *(WHM >> Home >> Email >> Configure Greylisting)* .
Whitelist: IP addresses that should not be checked against RBLs	This option allows you to choose a list of IP addresses to whitelist. Exim does **not** RBL-check these addresses. **Note:** Enter one IP address per line in the text box.

Note:
The *Security* options allow you to configure security settings for your mail server.

Option	Description

Allow weak SSL/TLS ciphers	This option allows you to use weak SSL/TLS encryption ciphers. **Warning:** As of cPanel & WHM version 68, we only support Transport Layer Security (TLS) protocol version 1.2. • We will only support applications that use TLSv1.2. • We **strongly** recommend that you enable TLSv1.2 on your server. **Important:** Weak SSL/TLS encryption ciphers violate PCI compliance. For more information about PCI compliance, read the PCI Compliance Guide.
Require clients to connect with SSL or issue the STARTTLS command before they are allowed to authenticate with the server	This option allows you to specify whether clients must connect with SSL or issue the STARTTLS command before they authenticate.
Scan messages for malware from authenticated senders (exiscan)	This option configures the ClamAVconnector plugin to scan all outbound messages for malware. The system rejects any mail that tests positive for malware. To view this option, you **must** install ClamAV on your server.
Scan outgoing messages for malware	This option configures the ClamAVconnector plugin to scan mail from non-whitelisted domains for malware. The system rejects any mail from non-whitelisted domains that tests positive for malware. To view this option, you **must** install ClamAV on your server.

Options for OpenSSL	This option configures SSL and TLS protocols in OpenSSL that Exim will use to securely communicate with client software. Either select the default options or enter a space-separated list in the text box of the protocols that you wish to disallow. For more information about OpenSSL's protocol options, read OpenSSLs Client documentation.
SSL/TLS Cipher Suite List	This option allows you to configure the cipher suites in OpenSSL that Exim uses to securely communicate with client software. For more information about cipher suites available to OpenSSL, read OpenSSL's Ciphers documentation.

Note:
The *Apache SpamAssassin™ Options* options allow you to configure Apache SpamAssassin to suit your server's needs.

- Apache SpamAssassin is a spam detection and blocking program which examines the content of an email message and assigns it an overall score. Apache SpamAssassin bases this score on the number of spam-related traits that Apache SpamAssassin finds in the message. If the message's score exceeds a predefined limit, SpamAssassin discards it as spam. For more information, visit the Apache SpamAssassin documentation.
- Any changes that you make to Apache SpamAssassin's configuration may require you to run `/usr/bin/sa-compile` before they take effect:

Option	Description
Apache SpamAssassin™: Forced Global ON	This option allows you to turn on Apache SpamAssassin for all accounts on the server without an option for the users to disable it.
Apache SpamAssassin™: message size threshold to scan	This option allows you to set the maximum size, in Kilobytes, for messages that Apache SpamAssassin scans. It is generally inefficient to scan large messages because spam messages are typically small (4 KB or smaller).

Scan outgoing messages for spam and reject based on Apache SpamAssassin™ internal spam_score setting	This option allows Apache SpamAssassin to scan and reject messages to non-local domains with a higher spam score than Apache SpamAssassin's internal `spam_score` setting of `5`. The system disables this option by default. To enable this option, select *On*. **Note:** This setting does **not** affect outbound forwarded mail. Forwarders use the *Do not forward mail to external recipients if it matches the Apache SpamAssassin™ internal spam_score setting* setting.
Scan outgoing messages for spam and reject based on defined Apache SpamAssassin™ score	This option allows you to set the `spam_score` thre shold that Apache SpamAssassin uses to determine when it rejects messages to non-local domains. The system disables this option by default. To enable this option, select the empty text box and enter the number for Apache SpamAssassin to use as a minimum spam score. You **must** enter a number between `0.1` and `99.9`, which can use up to two decimal places. **Note:** This setting does **not** affect outbound forwarded mail. Forwarders use the *Do not forward mail to external recipients based on the defined Apache SpamAssassin™ score* setting.
Do not forward mail to external recipients if it matches the Apache SpamAssassin™ internal spam_score setting	This option allows Apache SpamAssassin to scan and reject messages in the forwarder queue with a higher spam score than Apache SpamAssassin's internal `spam_score` setting of `5`. The system disables this option by default.

Do not forward mail to external recipients based on the defined Apache SpamAssassin™ score	This option allows you to set the `spam_score` thre shold that Apache SpamAssassin uses to determine whether it rejects messages that users forward to non-local domains. The system disables this option by default. To enable this option, select the empty text box and enter the minimum spam score for Apache SpamAssassin to use for forwarded mail. You **must** enter a number between `0.1` and `99.9` , which can use up to two decimal places.
Enable BAYES_POISON_DEFENSE Apache SpamAssassin™ ruleset	This option increases the scoring thresholds that the Bayes Poison Defense module needs to learn SPAM and HAM (not spam). This helps SpamAssassin to better protect the system against spammers who use Bayes poisoning. For more information about Bayes poisoning, read the Wikipedia article.
Enable Passive OS Fingerprinting for Apache SpamAssassin™	This option allows Apache SpamAssassin to use Passive OS Fingerprinting. **Note:** You **must** enable the *Passive OS Fingerprinting* option in WHM's *Service Manager* interface (*WHM >> Home >> Service Configuration >> Service Manager*) for this option to function.
Enable KAM Apache SpamAssassin™ ruleset	This option allows Apache SpamAssassin to use the Kevin A. McGrail's KAM ruleset, with significant contributions from Joe Quinn. For more information about the KAM ruleset, read the module's website.
Enable the Apache SpamAssassin™ ruleset that cPanel uses on cpanel.net	This option allows Apache SpamAssassin to use the ruleset that cPanel, Inc. uses on the `cpanel.net` servers.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Exim Configuration Manager - Basic Editor
- Mail FAQ
- Mail Delivery Reports
- Exim Configuration Manager
- Mail Queue Manager

- Mail FAQ

- Exim Configuration Manager - Basic Editor
- Mail FAQ
- Mail Delivery Reports
- Exim Configuration Manager
- CVE-2017-1000369 Exim - Stack Clash

- WHM API 1 Functions - validate_exim_configuration_syntax
- WHM API 1 Sections - Mail
- WHM API 1 Functions - get_mailbox_status
- WHM API 1 Functions - exim_configuration_check
- WHM API 1 Functions - validate_current_installed_exim_config