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.

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-limit 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 *Only-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.

Additional documentation

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