Tweak Settings - Mail

(*WHM >> Home >> Server Configuration >> Tweak Settings*)

Max hourly emails per domain

This setting specifies the maximum number of emails that each domain can send per hour.

This setting defaults to *Unlimited*.

> ⚠️ **Notes:**
>
> - The system **only** enforces email send limits on remote email deliveries.
> - This setting does **not** appear if you disable the *Exim* service in WHM's [Service Manager](#) interface *(WHM >> Home >> Service Configuration >> Service Manager).*
> - This setting does **not** override the following settings:
>   - *Maximum Hourly Email by Domain Relayed*
>   - *Maximum percentage of failed or deferred messages a domain may send per hour*

Number of emails a domain may send per day before the system sends a notification.

This setting specifies the number of emails per day that a domain can send before the system sends a notification.

This setting defaults to *Unlimited*.

> ⚠️ **Notes:**
>
> - In order to count each account's outbound emails, this feature uses the [TailWatch](#) script to monitor a rolling 24 hour window of hourly logfiles. When a new hour begins, the system deletes the **oldest** hour's logfile.
> - The system counts outbound mail from subdomains and addon domains **separately** from their parent domain.

⚠️

The mailbox storage format for new accounts

This setting specifies the storage format for new accounts' mailboxes.

> ⚠️ **Note:**
>
> Accounts that you restore or transfer to your server will retain their original mailbox format.

You can select the following options:

- *mdbox* — An updated format which stores multiple messages in a file and uses index files for message flags and keywords.
- *maildir* — A format which stores folders as separate directories and messages as individual files.

  > ⚠️ **Note:**
  >
  > The *maildir* format uses more inode resources than the *mdbox* format.

This setting defaults to *maildir*.

For more information about the storage formats, read Dovecot's dbox documentation and Dovecot's maildir documentation.

Initial default/catch-all forwarder destination

This setting specifies the initial forwarding destination for new accounts' default (catch-all) email addresses. The default address handles email that nonexistent users on your server's domains receive.

> ⚠️ **Notes:**
>
> - Because a domain may receive a large number of spam messages for nonexistent users, if you choose to process this mail your server may use **more** resources.
> - cPanel users can modify this forwarding destination in cPanel's *Default Address* interface (*cPanel >> Home >> Mail >> Default Address*).

You can select the following options:

- *System account (default)* — The system forwards unroutable mail to the cPanel user's main email account.

  > ⚠️ **Note:**
  >
  > If you select this option, this account collects spam.

- *Fail* — The system discards the message and sends a notification to the sender.

  > ⚠️ **Note:**
  >
  > Select this option if you receive email attacks.

- *Blackhole* — The system accepts the message, discards it, and does **not** notify the Remote SMTP server.

  > ⚠️ **Note:**
  >
  > We recommend that you **not** use this option, because it violates SMTP's RFC 5321.

Mail authentication via domain owner password

This setting specifies whether to allow the use of the website owner's password to access any email address that the owner created within the account. The *Single Sign On* system generates a temporary user to access a cPanel account and its email accounts as the account owner. This means that if you log in to any email account through the cPanel interface, you do **not** have to enter a password.

This setting defaults to *Off*.

Include mailman in disk usage calculations

This setting specifies whether cPanel's disk usage calculations include Mailman mailing lists.

This setting defaults to *On*.

Email delivery retry time

This setting specifies the number of minutes that your mail server waits before it attempts to redeliver a message after delivery failure.

This setting defaults to *15 minutes*.

> ⚠️ **Note:**
>
> This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Track email origin via X-Source email headers

This setting specifies whether to track the origin of messages that users send through your mail server. This feature adds X-Source headers to email messages.

This setting defaults to *On*.

> ⚠️ **Notes:**
>
> - This feature requires Exim version 4.34 or later.
> - This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery.

This setting specifies whether to queue outgoing messages for later delivery after a domain reaches its limit for outgoing messages per hour.

> ⚠️ **Note:**
>
> The minimum value for this setting is `100`, with a maximum value of `10,000`.

For example, with the default value of `125%`, after the domain reaches its hourly limit Exim queues any additional messages, up to 125% of the *Max hourly emails per domain* value. After the account reaches 125% of the *Max hourly emails per domain* value, any additional outgoing messages will fail.

This setting defaults to *125%*.

> ⚠️ **Note:**
>
> - To force the failure of **all** outgoing messages after the domain reaches its limit, set this option to `100`.
> - This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Monitor the number of unique recipients per hour to detect potential spammers.

This setting configures the system to monitor the number of emails to unique recipients that each individual email user sends. If this number exceeds the value of the *Number of unique recipients per hour to trigger potential spammer notification* setting, the system will send a notification.

This setting defaults to *Enabled*.

Select the action for the system to take on an email account when it detects a potential spammer

The system will automatically take this action on every email account that it detects as a potential spammer.

- *Take no action* — Do not perform any action on the email account.
- *Hold outgoing mail* — Hold all outbound messages in a queue for the email account.
- *Reject outgoing mail* — Block all outbound email for the email account.

This setting defaults to *Take no action*.

⚠️

> ⚠ **Note:**
>
> To release or delete outgoing mail held in the queue, perform the following actions in cPanel's *Email Accounts* interface (*cPanel >> Home >> Email >> Email Accounts*):
>
> 1. Click *Manage Suspension*.
> 2. Select *Allow* for the *Send* option.
> 3. If applicable, click *Delete messages from the mail queue* to remove any queued messages.
> 4. Click *Save*.

Number of unique recipients per hour to trigger potential spammer notification.

This setting specifies the number of emails sent by any email account in one hour that will cause the system to send an alert notification.

This setting defaults to *500*.

> ⚠ **Notes:**
>
> - This setting does **not** count emails sent by Mailman towards its limit.
> - This setting affects the *Select the action for the system to take on an email account when it detects a potential spammer* option.

Count mailman deliveries towards a domain's Max hourly emails.

This setting allows you to specify whether to count messages to Mailman mailing lists against an account's *Max hourly emails per domain* limit.

This setting's value defaults to *Off*.

> ⚠ **Notes:**
>
> - Set this value to *Off* to accomodate users with large Mailman mailing lists.
> - If you enable this setting, you may encounter issues with mailing list subscribers who do not receive messages.

Maximum percentage of failed or deferred messages a domain may send per hour

This setting allows you to specify a maximum percentage of failed or deferred messages that your domain may send per hour. Your server temporarily blocks outgoing mail from a domain if **both** of the following conditions are true:

- The percentage of failed or deferred messages, out of the total number of sent messages, is **equal to or greater than** the specified percentage.
- The domain has sent **at least** the number of failed or deferred messages that the *Number of failed or deferred messages a domain may send before protections can be triggered* setting specifies.

The system examines all outgoing and local mail over the previous hour to determine whether these conditions are true. If **only one** of these conditions is true, the system does **not** block outgoing mail.

For more information, read our Mail Limiting Features documentation.

This setting defaults to *Unlimited*.

> ⚠ **Notes:**
>
> - This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.
> - The system uses this setting in conjunction with the *Number of failed or deferred messages a domain may send before protections can be triggered* setting. Your server does **not** temporarily block outgoing mail from a domain until the domain meets **both** settings' requirements.

Number of failed or deferred messages a domain may send before protections can be triggered

This setting specifies a number of failed or deferred messages that a domain can send before the system blocks outgoing mail. Your server temporarily blocks outgoing mail from a domain if **both** of the following conditions are true:

- The domain sends **at least** this number of failed or deferred messages.
- The percentage of failed or deferred messages (out of the total number of sent messages) is **equal to or greater than** the percentage that the *Number of failed or deferred messages a domain may send before protections can be triggered* setting specifies.

The system examines all outgoing and local mail over the previous hour to determine whether these conditions are true. If **only one** of these conditions is true, the system does **not** block outgoing mail.

For more information, read our Mail Limiting Features documentation.

This setting defaults to *5.*

> ⚠ **Notes:**
>
> - This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.
> - The system uses this setting in conjunction with the *Maximum percentage of failed or deferred messages a domain may send per hour* setting. Your server does **not** temporarily block outgoing mail from a domain until the domain meets **both** settings' requirements.

Restrict outgoing SMTP to root, exim, and mailman (FKA SMTP Tweak)

This setting redirects outgoing SMTP connections to the local mail server and allows only the `root`, `exim`, and `mailman` users to make direction connections.

> ⚠ **Note:**
>
> When you **enable** this setting, scripts and email users **must** use the `sendmail` binary to send mail and **cannot** use direct socket access.

This setting defaults to *On.*

Prevent "nobody" from sending mail

This setting denies the `nobody` user the ability to send mail to a remote address.

The setting defaults to *On.*

> ⚠ **Note:**
>
> PHP and CGI scripts generally run as the `nobody` user. To use a PHP or CGI script to send mail, enable the `suEXEC` or `mod_php` modules in your Apache configuration.

Allow users to relay mail if they use an IP address through which someone has validated an IMAP or POP3 login within the last hour (Pop-before-SMTP)

This setting allows users who authenticated against the POP3 or IMAP service in the last 30 minutes to send emails through SMTP again without the need to reauthenticate.

This setting defaults to *Off.*

> ⊘ **Warning:**
>
> An open email relay on an IP address poses a **security risk**. We recommend that you do **not** enable this option because it can compromise you users' privacy and **strongly** recommend that you use SMTP authentication.

> ⚠ **Notes:**
>
> - This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.
> - This setting does **not** appear if you disable the *RecentAuthedMailIpTracker* setting in WHM's *Service Manager* interface (*WHM >> Home >> Service Configuration >> Service Manager*).

Add X-PopBeforeSMTP header for mail sent via POP-before-SMTP

This setting requires the mail server to append a list to the `X-PopBeforeSMTP` headers of all of that user's outgoing messages. This list contains all of the email addresses that a user checks with POP before SMTP. POP before SMTP is an email protocol that allows users to check email from different IP addresses without the need to log in repeatedly.

This setting defaults to *Off.*

⊘

> ⊘ **Warning:**
>
> We recommend that you do **not** enable this option because it can compromise you users' privacy.

> ⚠ **Notes:**
>
> - This setting requires Exim 4.34 or later.
> - This setting does **not** appear if you disable the *Exim* service in WHM's [Service Manager](#) interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Enable BoxTrapper spam trap

This setting allows you to enable BoxTrapper, a spam prevention system that uses blacklists, whitelists, and ignore lists, and an automated response-verification system.

This setting defaults to *On*.

> ⚠ **Note:**
>
> This setting does **not** appear if you disable the *Exim* service in WHM's [Service Manager](#) interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Enable Email Archiving support

This setting enables email archiving support. Email archiving maintains a copy of each email that your server sends or receives. The server immediately archives an email when it receives the message. This action takes place before the system applies any filters to the message, which means that the system archives both spam and non-spam messages.

This setting defaults to *Off*.

> ⚠ **Notes:**
>
> - If you enable this setting, the amount of disk space that mail uses will **double**.
> - This setting does **not** appear if you disable the *Exim* service in WHM's [Service Manager](#) interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Enable Horde Webmail

This setting enables the Horde webmail client. Webmail allows cPanel users to access their email accounts with an Internet connection and a web browser.

This setting defaults to *On*.

Enable Mailman mailing lists

> ⊘ **Important:**
>
> The system does not start the Mailman service until the server hosts at least one mailing list.

This setting enables Mailman on your server. Mailman is third-party software that manages [mailing lists](#).

This setting defaults to *On*.

Enable Roundcube webmail

This setting enables the Roundcube webmail client. Webmail allows cPanel users to access their email accounts with an Internet connection and a web browser.

This setting defaults to *On*.

Enable the Apache SpamAssassin™ spam filter

This setting enables Apache SpamAssassin, a spam filtration program that scores incoming email and checks that score against a predefined limit. If the spam score exceeds this limit, the server takes the action that the domain owner specified in cPanel's [Spam Filters](#) interface (*cPanel >> Home >> Mail >> Apache SpamAssassin*). You can discard mail or place it in a spam folder.

This setting defaults to *On*.

⊘

For more information, see the Apache SpamAssassin website.

> ⊘ **Warning:**
>
> If you make changes to Apache SpamAssassin's configuration, you **must** run the `/usr/bin/sa-compile` script for your changes to take effect.

> ⚠ **Note:**
>
> This setting does **not** appear if you disable the *Exim* service in WHM's *Service Manager* interface *(WHM >> Home >> Service Configuration >> Service Manager)*.

Enable Apache SpamAssassin™ Spam Box delivery for messages marked as spam (user configurable)

This setting enables Apache SpamAssassin's spam box feature. The spam box receives incoming mail that Apache SpamAssassin marks as spam. This is useful for users who receive a message that the system falsely flags as spam.

This setting defaults to *On*.

Prefix "mail." onto Mailman URLs

This setting specifies whether the system should prefix Mailman URLs with `mail.` For example, `http://mail.domain.com/mailman`.

This setting defaults to *Off.*

Default user-defined quota value for new email accounts

This setting defines the default quota that appears in cPanel's *Email Accounts* interface (*cPanel >> Home >> Mail >> Email Accounts*).

This setting defaults to *32768 MB*. The maximum value is 4,294,967,296 MB (4 Terrabytes).

Default quota option for new email accounts

This setting defines the preselected quota option in cPanel's *Email Accounts* interface (*cPanel >> Home >> Mail >> Email Accounts*).

This setting's value defaults to *User-defined*.

Age, in days, of content to purge users' Horde cache files

This setting determines the minimum age, in days, of files that the system will automatically purge users' Horde cache files.

This setting accepts a minimum value of *1* and defaults to *Disabled*.

Additional documentation

- Tweak Settings - Mail
- SMTP Restrictions
- Reset a Mailman Password
- Spamd Startup Configuration
- The cPanel Update Configuration File - cpupdate.conf