How to Prevent Email Abuse

Overview

This document outlines some of the best practices that you can follow to avoid email abuse on your cPanel & WHM server.

Password Strength Configuration

If you increase the minimum password strength for your users' mail accounts, you can decrease the chance that a hacker will correctly guess their passwords.

To define minimum password strength for all of your users' authenticated features, use WHM's *Password Strength Configuration* interface (*WHM >> Home >> Security Center >> Password Strength Configuration)*.

> **Note:**
> We recommend that you set the default minimum password strength to at least `50`.

Enable cPHullk

cPHulk provides protection for your server against brute force attacks (a hacking method that uses an automated system to guess passwords). If you enable cPHulk, you can decrease the chance that a hacker can use a brute force attack to gain access to your server's mail accounts.

To enable this feature, navigate to WHM's *cPHulk Brute Force Protection* interface (*WHM >> Home >> Security Center >> cPHulk Brute Force Protection*) and click *Off* to toggle the feature's status.

SMTP restrictions

If you enable the *SMTP Restrictions* feature, spammers cannot directly interact with remote mail servers or work around mail security settings.

- This feature restricts outgoing email connection attempts to the mail transfer agent (MTA), the `mailman` system user, and the `root` user.
- This feature forces both scripts and users to use Exim's `sendmail` binary, which helps to prevent direct access to the socket.

To enable this feature, navigate to WHM's *SMTP Restrictions* interface (*WHM >> Home >> Security Center >> SMTP Restrictions*) and click *Enable*.

Tweak Settings

The following settings in the *Mail* section of WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings*) can help to prevent email abuse:

> **Note:**
> If you set the *Max hourly emails per domain* option to `500`, this allows each of the domains that you host to send 500 email messages per hour. For example, a domain uses a mailing list with 500 members. If this domain sends a message to the mailing list, then sends another email message in the same hour, the domain will exceed the *Max hourly emails per domain* limit.
>
> Use the *The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery* setting to specify a "soft limit." For example, if you set the *The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery* value to `150`, the domain can queue up to 250 messages to send in the next hour. In this scenario, the domain can queue the additional 25 email messages in the next hour.

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*

Important:
The system **only** enforces email send limits on remote email deliveries.
To prevent email abuse, we recommend that you specify a value that is **not** *Unlimited.*

Account-specific Max hourly emails per domain settings

Use WHM's *Edit a Package* interface (*WHM >> Home >> Packages >> Edit a Package*) or WHM's *Modify an Account* interface (*WHM >> Home >> Account Functions >> Modify an Account*) to specify values for an individual package or an individual account.

To enable this setting from the command line, you **must** perform the following steps to manually edit the `cpuser` file:

1. From the command line, open the `/var/cpanel/users/username` file, where `username` represents the desired account username.
2. In this file, add the `MAX_EMAIL_PER_HOUR` key and specify the value for the selected username:

```
MAX_EMAIL_PER_HOUR=500
```

3. Run the `/usr/local/cpanel/scripts/updateuserdomains` script.

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.

Important:
To prevent email abuse, we recommend that you select *On*.

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)*.

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.

PHP configuration

Warning:
Do **not** enable suEXEC with ModRuid2. suEXEC is **not** compatible with this module.

If you configure PHP and suEXEC, ModRuid2, or suPHP, you can improve server security. This configuration allows you to know which users run which processes system-wide.

- ModRuid2 and suPHP force CGI applications to run as the cPanel account user. In addition, ModRuid2 exploits some of the `POSIX.1e` capabilities in order to provide some performance enhancements over Apache's default suEXEC configuration.
  - For instructions to enable ModRuid2, read our Apache Module: ModRuid2 documentation.
  - For instructions to enable suPHP, read our Apache Module: SuPHP documentation.
- The suEXEC Apache module forces CGI and PHP applications to run as the cPanel account user. For instructions to enable suEXEC, read our Configure PHP and suEXEC documentation.

Experimental: Rewrite From: header to match actual sender

Any local cPanel user can use the `127.0.0.1` IP address to send mail without authentication. This can make it difficult for system administrators to determine which cPanel account sent the mail, especially when a malicious user spoofs an email address to disguise the origin of the email.

To require cPanel & WHM to put the actual sender in the header, enable the *Experimental: Rewrite From: header to match actual sender* option in WHM's *Exim Configuration Manager* interface *(WHM >> Home >> Exim Service Configuration >> Exim Configuration Manager)*.

After you enable this feature, you will see output that is similar to the following in the `/var/log/exim_mainlog` file:

```
2014-04-23 08:09:52 1Wcwvu-0000On-Sb From: header (rewritten was:
[fakemail@example.com], actual sender is not the same system user)
original=[fakemail@example.com] actual_sender=[spammer@spammer.com]
```

The `actual_sender` portion of the log entry shows that `spammer` is the cPanel account that sent the email. This information allows the system administrator to take action against the account to prevent additional spam.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- How to Prevent Email Abuse
- How to Configure PHP and suEXEC from the Command Line
- How to Set Email Send Limits
- How to Prevent Spam with Mail Limiting Features
- How to Keep your Email Out of the Spam Folder

- How to Create a Spam Email Filter
- How to Log in to the Sent and Spam Mail Folders Directly
- How to Create Mail Filter Rules For Mailing Lists

- How to Prevent Email Abuse
- How to Configure PHP and suEXEC from the Command Line
- How to Set Email Send Limits
- How to Prevent Spam with Mail Limiting Features
- How to Keep your Email Out of the Spam Folder

- WHM API 1 Functions - save_spamd_config
- UAPI Functions - Email::enable_spam_box
- UAPI Functions - Email::disable_spam_box
- cPanel API 1 Functions - Email::delspam
- cPanel API 1 Functions - Email::spamstatus