

# Spamd Startup Configuration

(WHM >> Home >> Email >> Spamd Startup Configuration)

- [Overview](#)
- [Configure options](#)
- [Additional documentation](#)

## Overview

Apache SpamAssassin™ is a spam filter utility that examines incoming email and tests for spam characteristics. If you enable Apache SpamAssassin on your server, the Apache SpamAssassin daemon (`spamd`) provides the Apache SpamAssassin service to your mail server.

Use the *Spamd Startup Configuration* interface to configure the startup options for the Apache SpamAssassin daemon.

### Notes:

- To enable or disable Apache SpamAssassin, use the *Enable Apache SpamAssassin™ spam filter* setting in WHM's *Tweak Settings* interface (WHM >> Home >> Server Configuration >> Tweak Settings).
- To enable or disable the `spamd` daemon from the command line, run either of the following series of commands:
  - Enable spamd

```
rm -f /etc/spamddisable
touch /etc/spamdenable
find /etc/chkserv.d/spamd -exec rm -v {} \;
/usr/local/cpanel/scripts/restartsrv_tailwatchd
/usr/local/cpanel/scripts/restartsrv_spamd
```

- Disable spamd

```
rm -f /etc/spamdenable
touch /etc/spamddisable
find /etc/chkserv.d/spamd -exec rm -v {} \;
/usr/local/cpanel/scripts/restartsrv_tailwatchd
/usr/local/cpanel/scripts/restartsrv_spamd
```

- To enable or disable dormant mode for the `spamd` daemon, use the *Dormant services* setting in WHM's *Tweak Settings* interface (WHM >> Home >> Server Configuration >> Tweak Settings).
- For more information on Apache SpamAssassin, read our [Spam Filters](#) documentation.

## Configure options

To configure the options that the Apache SpamAssassin daemon uses at startup, perform the following steps:

- Enter the desired value for the option that you wish to change.
- Click Save.

The following table describes the available options:

Option	Description	Default value	Minimum value
--------	-------------	---------------	---------------

<i>Allowed IPs</i>	<p>To only allow connections from specific IP addresses to access the <code>spamd</code> daemon, enter a comma-separated list of IP addresses in the <i>Allowed IPs</i> text box. If you do not enter a value, the <code>spamd</code> daemon allows connections from any IP address.</p> <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p><b>Warning:</b> If you restrict access to the <code>spamd</code> daemon, you <b>must</b> include the local IPv4 address (<code>127.0.0.1</code>) to ensure that the <code>chkdsk</code> daemon can access the <code>spamd</code> daemon. Also, if you use IPv6 on your server, you <b>must</b> also include the local IPv6 address (<code>:::1</code>).  If you do not include these IP addresses in the <i>Allowed IPs</i> list, the <code>spamd</code> daemon will fail.</p> </div>	<code>127.0.0.1, :::1</code>	
<i>Maximum Connections per Child</i>	Defines the maximum number of connections that a <code>spamd</code> child process may have. After a <code>spamd</code> child process reaches the maximum number of connections, the <code>spamd</code> daemon will abandon the child process.	200	1
<i>Maximum Children</i>	<p>Defines the maximum number of child processes that a <code>spamd</code> process can spawn at startup.</p> <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> The <code>/usr/local/cpanel/scripts/vps_optimizer</code> script optimizes this value for the amount of memory on your server.</p> </div>	5	1
<i>PID File</i>	Defines a custom location of the <code>spamd.pid</code> file.	<code>/var/run/spamd.pid</code>	
<i>TCP Timeout</i>	Defines the amount of time, in seconds, that you wish for the <code>spamd</code> daemon to wait before it abandons a TCP connection. If you set the value to 0, the <code>spamd</code> daemon will not abandon TCP connections.	30	1
<i>TCP Child Timeout</i>	Defines the amount of time, in seconds that you wish for a child process to wait before it abandons a TCP connection. If you set the value to 0, the <code>spamd</code> daemon child processes will not abandon TCP connections.	300	1

## Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- [Spamd Startup Configuration](#)

- [The cPanel Update Configuration File - cupdate.conf](#)
- [Tweak Settings - Mail](#)
- [Spam Filters](#)
- [BoxTrapper](#)
- [Configure Greylisting](#)
- [Spamd Startup Configuration](#)
- [How to Configure the Apache SpamAssassin Report\\_Safe Option](#)
- [Scan Outgoing Mail](#)
- [How to Set Email Send Limits](#)
- [The cPanel Update Configuration File - cupdate.conf](#)
- [UAPI Functions - Email::enable\\_spam\\_box](#)
- [UAPI Functions - Email::disable\\_spam\\_box](#)
- [cPanel API 1 Functions - Email::delspam](#)
- [cPanel API 1 Functions - Email::spamstatus](#)
- [UAPI Functions - Email::add\\_spam\\_filter](#)