

# Tweak Settings


For cPanel & WHM version 58

( [Home](#) >> [Server Configuration](#) >> [Tweak Settings](#) )

## Overview

This interface allows you to configure many cPanel & WHM settings. Tabs at the top of the interface categorize the settings, and the *All* tab displays all of the settings.

### Notes:

- Tweak settings are stored in the `/var/cpanel/cpanel.config` file. However, we recommend that system administrators use the *Tweak Settings* interface to make changes. For more information, read our documentation about [The cpanel.config File](#).
- Click the question mark next to each setting's description to learn more about the setting.
- The interface displays a warning icon () next to any setting for which you have not specified a value. This includes settings that are new, settings that WHM has set to a default value, or settings that your server selected dynamically. For more information, read [The cpanel.config File](#) documentation.

Click on the tabs below to read about each section's settings.

[cPAddons](#) [Site Software](#) [Compression](#) [Development](#) [Display](#) [Domains](#) [Logging](#) [Mail](#) [Notifications](#) [PHP](#) [Redirection](#) [SQL](#) [Security](#) [Software](#)  
[Stats](#) [Programs](#) [Stats and Logs](#) [Status](#) [Support](#) [System](#)

## cPAddons Site Software admin email

This setting specifies a contact email address that receives cPAddons' moderation requests. The system also notifies resellers if they choose to configure their contact email address in their cPanel interfaces.

To specify the cPAddon administrator's email address, enter the email address that you wish to use in the text box.

This setting defaults to *None*.

### Note:

A moderation request is a request from a user who wishes to install or upgrade a cPAddon. You **must** approve the request before the user installs or upgrades a cPAddon.

## cPAddons Site Software source automatic updates

This setting specifies whether you wish for cPanel & WHM to automatically update all of the cPAddons' source files.

This setting defaults to *On*.

## Max cPAddons Site Software installation requests

This setting specifies the maximum number of moderation requests that a single user can make at one time.

To specify a new value, enter the number of requests that you wish to allow in the text box.

This setting defaults to 99.

### Max cPAddons Site Software installation requests per addon

This setting specifies the maximum number of moderation requests per cPAddon that a single user can make at one time.

To specify a new value, enter the number of requests that you wish to allow per cPAddon in the text box.

This setting defaults to 99.

### cPAddons Site Software moderation notification

This setting allows you to select whether the cPAddons administrator receives notifications about pending moderation requests.

This setting defaults to *Off*.

### Allow cPAddons Site Software installations from non-cPanel sources

This setting allows you to install third-party scripts on your server.

This setting defaults to *On*.

### Allow cPAddons Site Software installations from modified sources

This setting allows users to install previously-altered cPAddons.

This setting defaults to *Off*.

**Note:**

\$body

### Notify reseller of cPAddons Site Software installations

This setting notifies resellers whenever their users **must** update their cPAddons.

This setting defaults to *On*.

### Notify root of cPAddons Site Software installations

This setting notifies the cPAddons Site Software administrator whenever their users **must** update their cPAddons.

This setting defaults to *On*.

## Notify cPanel users when they need to update their cPAddons Site Software installations

This setting notifies cPanel users whenever they **must** update their cPAddons.

Select any of the following options:

- *Allow users to choose (default)* — This option allows cPanel users to specify whether they wish to receive notifications about out-of-date cPAddons.
- *always* — This option allows cPanel & WHM to automatically notify users when their cPAddons are out-of-date.
- *never* — This option allows you to specify that users should **never** receive notifications when their cPAddons are out-of-date.

## gzip compression level

This setting allows you to set the gzip compression level for pigz, which is a gzip-compatible program that uses multiple CPU cores simultaneously.. Higher settings provide greater compression, but compress more slowly.

This setting's minimum value is 1 and the maximum value is 9. The default value is 6.

## Number of pigz processes

This setting allows you to set how many independent pigz processes the system uses to perform gzip compression.

This setting's minimum value is 1 and the maximum value is 128. The default value is the number of processor cores on your server.

**Note:**  
\$body

## Number of kilobyte chunks per compression work unit

This setting allows you to control the size (in 1024-byte (B) chunks) of compression work units that the system distributes to each pigz process.

This setting's minimum value is 128. This setting defaults to 4096.

## Standardized Hooks - Debug Mode

The Standardized Hooks System's debug mode helps to troubleshoot hook issues.

The following options are available:

- *Debug mode is off.* — The system does not display debug information or log it to the error log.
- *Debug mode is on. The system displays information about a hook while it executes, but does **not** log debug data to the error log.*
- *Debug mode is on. The system displays information about a hook while it executes **and** logs debug data to the error log.*

**Important:**  
This setting outputs a **large** amount of data.

- *Debug mode is on. The system displays information about every stage for every hookable event, even if no hooks exist for that stage.*

This setting defaults to *Debug mode is off*.

## Default login theme

This setting allows you to select the default login theme for cPanel users.

This setting defaults to *cpanel*.

## Display File Usage information in the cPanel stats bar (inode count)

This setting allows you to display the number of files and directories (inodes) that a cPanel account uses.

The *Statistics* section of cPanel's *Home* interface displays this information under the *File Usage* heading.

This setting defaults to *Off*.

## Number of accounts per page to display in "List Accounts"

This setting allows you to specify the number of accounts to display per page in WHM's *List Accounts* interface (*Home >> Account Information >> List Accounts*).

To specify a new value, enter the integer that you wish to use in the text box. You can also select either of the following options:

- *All* — View all of the accounts on your server whenever you or a reseller views WHM's *List Accounts* interface (*Home >> Account Information >> List Accounts*).
- *30 (default)* — View 30 accounts per page.

This setting defaults to *30*.

## Allow users to park subdomains of the server's hostname

This setting allows users to park subdomains on your server's main domain.

For example, if your server's main domain name is `example.com`, click *On* to redirect `user.example.com` visitors to that user's website.

This setting defaults to *Off*.

## Allow cPanel users to create subdomains across accounts

This setting allows a user to create an addon domain or subdomain of a domain that another user owns.

For example, if the user `bob` owns the domain `example.com`, the user `charlie` can create the `store.example.com` subdomain.

This setting defaults to *Off*.

**Warning:**

Do **not** enable this option. It can cause serious security issues.

## Allow WHM users to create subdomains across accounts

This setting allows WHM users to create an addon domain or a subdomain of a domain that another user owns.

For example, if the user `bob` owns the domain `example.com`, the WHM user `charlie` can create an account for the `store.example.com` subdomain.

This setting defaults to *Off*.

**Warning:**

Do **not** enable this option. It can cause serious security issues.

## Allow Remote Domains

This setting allows users to create parked and addon domains that resolve to other servers.

This setting defaults to *Off*.

**Warning:**

Do **not** enable this option. It can cause serious security issues.

## Allow resellers to create accounts with subdomains of the server's hostname

This setting allows resellers to create accounts with subdomains of your server's main domain.

For example, if your main domain name is `example.com`, enable this setting to redirect `user.example.com` visitors to the reseller's website.

This setting defaults to *Off*.

## Allow unregistered domains

This setting allows users to create domain names on the server that they do **not** register with a valid registrar.

This setting defaults to *Off*.

## Automatically add A entries for registered nameservers when creating a new zone

This setting specifies whether the system automatically creates [A entries](#) for a new domain's registered nameservers when a user creates a domain.

This setting defaults to *On*.

## Prevent cPanel users from creating specific domains

This setting prevents the creation of certain domains with domain names that the `/var/cpanel/commondomains` file contains.

If you enable this setting, cPanel users **cannot** create (as an addon or parked domain) any domain that the `/var/cpanel/commondomains` file or the `/usr/local/cpanel/etc/commondomains` file contains.

**Important:**

Do **not** edit the `/usr/local/cpanel/etc/commondomains` file directly. If you do, the system **will overwrite** your changes whenever cPanel & WHM updates.

## Check zone syntax

This setting allows you to have the system automatically check zone file syntax whenever a user saves or synchs DNS zone files.

This setting's value defaults to *On*.

## Check zone owner

This setting allows you to have the system automatically check a DNS zone's owner whenever a user saves or synchs DNS zone files.

This setting defaults to *On*.

## Enable DKIM on domains for newly created accounts

**DKIM (DomainKeys Identified Mail)** verifies a message's sender and integrity. It allows an email system to prove that a message is valid, **not** forged, and that it came from the specified domain.

This setting allows you to specify whether to enable DKIM for new accounts by default.

This setting defaults to *On*.

## Enable SPF on domains for newly created accounts

**SPF (Sender Policy Framework)** denies spammers the ability to send email when they forge your domain's name as the sender (spoofing). This authentication function adds IP addresses to a list of computers that you authorize to send mail from your domain name. It verifies that messages that your domain sends come from the listed sender, which reduces the amount of backscatter that you receive.

This setting allows you to specify whether to enable SPF for new accounts by default.

This setting defaults to *Off*.

## DNS request management application

This setting specifies the application that the system uses to handle DNS management requests.

To specify a new application, enter the path to the application that you wish to use in the text box.

This setting defaults to *dnsadmin, auto-detect SSL*.

## Proxy subdomains

This setting allows users to access cPanel & WHM services from standard HTTP ports, such as Port 80 and Port 443. This setting is useful if users **cannot** access the standard cPanel & WHM ports due to firewall restrictions.

If you enable this setting, the system automatically redirects visitors to the correct port when they access the following subdomains:

- `cpanel.example.com` redirects to the user's cPanel [cPanel Home Interface](#).
- `webmail.example.com` redirects to the user's [Webmail](#) interface.
- `webdisk.example.com` redirects to the user's [Web Disk](#).
- `whm.example.com` redirects to the user's [WHM](#) interface.

**Note:**  
\$body

This setting defaults to *On*.

**Important:**

- The settings that you select in the *Tweak Settings - Redirection* section do **not** apply to proxy subdomains.
- When you enable this setting, it creates an entry in your Apache configuration file (`httpd.conf`). This feature also requires that you **do not** manually disable `mod_rewrite` and `mod_proxy` in the `httpd.conf` file.

## Proxy subdomain creation

Proxy subdomains allow users to reach particular interfaces within cPanel or WHM when they enter a subdomain in a browser. For example, a user who enters `cpanel.example.com` reaches `example.com`'s *cPanel Home Interface*.

This setting allows WHM to automatically create DNS entries for the following subdomains for every user's account:

- `cpanel.example.com`
- `webmail.example.com`
- `webdisk.example.com`
- `whm.example.com`

**Note:**

\$body

This setting defaults to *On*.

**Important:**

You **must** add DNS entries for these subdomains to work. Use the `/usr/local/cpanel/scripts/proxydomains` file to create DNS entries manually.

## Thunderbird and Outlook autodiscover and autoconfig support (enables proxy subdomain and SRV record creation)

This setting automatically creates `autodiscover` and `autoconfig` proxy subdomains when you create a domain.

- `autoconfig.example.com`
- `autodiscover.example.com`

This setting also creates the `autodiscover` and `autoconfig` SRV records that local domains need for Outlook and Thunderbird email autoconfiguration.

**Note:**

If you turn off the *Proxy subdomains* option, the system disables this setting.

For more information about Autodiscover and AutoConfig, visit the [TechNet for Autodiscover](#) and [Mozilla's AutoConfig](#) websites.

## Preferred mail service to configure to use for Thunderbird and Outlook® autodiscover and autoconfig support

This setting allows you to choose the email transfer method to use with Thunderbird and Outlook with Autodiscover and AutoConfig support.

This setting defaults to *imap*.

**Notes:**

- We recommend that you select IMAP and **not** POP3.
- You **must** enable the *Thunderbird and Outlook autodiscover and autoconfig support (enables proxy subdomain and SRV record creation)* option in order to configure this setting.

## Host to publish in the SRV records for Outlook autodiscover support

Microsoft Outlook®'s Autodiscover service searches DNS for an SRV record for an email inbox's domain that points to a particular server for Autodiscover. By default, this server is `cpanel.emaildiscovery.cpanel.net`.

This setting allows system administrators to perform the following actions:

- Choose the host that the system publishes to the SRV records.
- Change the default host if they have an SSL-enabled host with an SSL certificate that a Certificate Authority signs.
- Use their own server for Outlook® Autodiscover. Enter that server's Fully Qualified Domain Name (FQDN) in the available text box.
- When you enable the *Host to publish in the SRV records for Outlook autodiscover support* feature, the system queries the server that you specify for the Autodiscover settings. You **must** have a custom XML file for this feature to function properly.

**Notes:**

- For more information about how to use a custom XML file, visit [Mozilla's autoconfiguration page](#), or the [Exchange's Autodiscover page](#).
- You must enable the *Thunderbird and Outlook autodiscover and autoconfig support (enables proxy subdomain and SRV record creation)* option in order to configure this option.

For more information about Microsoft Outlook's Autodiscover feature, visit [Microsoft's Support](#) website.

## Overwrite custom A records used for proxy subdomains

This setting allows the system to remove any existing custom [A records](#) that match proxy subdomains that you create or remove.

**Note:**

If you turn off the *Proxy subdomains* option, the system disables this setting.

This setting defaults to *Off*.

## Overwrite custom SRV records used by Outlook AutoDiscover support

This setting allows the system to remove any existing custom SRV records whenever the user adds or removes Outlook Autodiscover support.

This setting defaults to *Off*.

## Proxy subdomain override

This setting allows users to create cPanel, Webmail, Web Disk, and WHM subdomains that override automatically generated proxy subdomains.

For example, a user can direct visitors who access `cpanel.example.com` to a web page that the user configures, such as `mycontrolpanel.example.com`.



This setting defaults to *On*.

**Note:**

Proxy subdomains allow you to enter a subdomain in your browser to reach particular cPanel & WHM interfaces. For example, enter `cpANEL.example.com` to reach `example.com`'s cPanel interface.

## Restrict document roots to public\_html

This setting prevents the creation of addon domains and subdomains outside of a cPanel user's primary domain's document root (the `public_html` directory within the user's `/home` directory).

For example, if you enable this setting and then create the `example.com` addon domain, the system creates the `/home/username/public_html/example.com` directory rather than the `/home/username/example.com` directory.

This setting defaults to *Off*.

## Always use authoritative (registered) nameservers when creating a new DNS zone

This setting allows the server to use a new domain's authoritative nameservers (the nameservers on record with the domain's registrar). The server does **not** use the nameservers that domain's creator specified.

This setting defaults to *Off*.

## Log dnsadmin requests

This setting allows you to select whether to log `dnsadmin` requests in the `/usr/local/cpanel/logs/dnsadmin_log` file.

This setting's value defaults to *Off*.

## Enable verbose logging of DNS zone syncing

This setting causes your server to print DNS information to the command line interface whenever the system synchronizes a DNS zone.

This setting's value defaults to *Off*.

**Warning:**

This setting is for testing purposes only. Do **not** enable this option on a production server.

## Log successful logins

This setting causes your server to record successful login events for cPanel, Webmail, WHM, and DAV to their respective log files in the `/usr/local/cpanel/logs/` directory.

This setting's value defaults to *Off*.

## Max hourly emails per domain

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

This setting defaults to *Unlimited*.

**Notes:**

- This setting does **not** appear if you disable the *exim* service in WHM's [Service Manager](#) interface (*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*.

## The storage format for new accounts

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

You may choose from the following options:

- *mdbox* — An updated format which stores multiple messages in a file, and uses index files for message flags and keywords.
- *maildir* — Another format which stores folders as separate directories and messages as individual files. This format uses more inode resources than the *mdbox* format.

For more information about the storage formats, read [Dovecot's mbox](#) documentation and [Dovecot's maildir](#) documentation.

This setting defaults to *maildir*.

**Note:**

Accounts that you transfer to your server will retain their original mailbox format.

## 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. Because a domain may receive a large number of spam messages for nonexistent users, if you choose to process this mail, it can cost you server resources.

**Note:**

cPanel users can modify this forwarding destination in cPanel's [Default Address](#) interface (*Home >> Mail >> Default Address*).

You may choose from the following options:

- *System account (default)* — The system forwards unroutable mail to the cPanel user's main email account. If you choose this option, this account mainly collects spam.
- *Fail* — The system discards the message and sends a notification to the sender.

**Note:**

Select this setting if you receive email attacks.

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

**Note:**

\$body

## Discard FormMail-clone message with bcc:

This setting specifies whether to silently discard FormMail-clone messages that contain a `bcc:` header in the subject line. Messages that meet this criteria are typically spam.

This setting defaults to *On*.

**Note:**  
\$body

## 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 via 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 the message delivery fails.

This setting defaults to 15 minutes.

**Note:**  
\$body

## 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*.

**Note:**  
This feature requires Exim version 4.34 or later.

**Note:**  
\$body

## The percentage of email messages (above the domain'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. For example, if you set this value to 125, then 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.

To force the failure of all outgoing messages after the domain reaches its limit, set this option to 100.

This setting defaults to 125.

**Note:**  
\$body

## 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*.

**Note:**  
Set this value to *Off* if you wish to accommodate users with large Mailman mailing lists. If you set this value to *On*, 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 percentage of failed or deferred messages that your domain may send per hour.

This setting defaults to *unlimited*.

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.

If only one of these conditions is true, the system does **not** block outgoing mail. The system examines all outgoing and local mail over the previous hour to determine whether these conditions are true. For more information, read our [Mail Limiting Features](#) documentation.

**Notes:**

- This setting does **not** appear if you disable the *exim* service in WHM's *Service Manager* interface (*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.

This setting defaults to 5.

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.

If only one of these conditions is true, the system does **not** block outgoing mail. The system examines all outgoing and local mail over the previous hour to determine whether these conditions are true. For more information, read our [Mail Limiting Features](#) documentation.

**Notes:**

- This setting does **not** appear if you disable the *exim* service in WHM's *Service Manager* interface (*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

This setting allows you to only allow the `root`, `exim`, and `mailman` users to send email messages. Enable this setting to deny other users on the system the ability to send mail. 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 *Off*.

## 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 on an IP address who authenticated against the POP3 or IMAP service in the last 30 minutes to send emails via SMTP again without the need to re-authenticate. An open email relay on an IP address poses a security risk.

This setting defaults to *Off*.

**Warning:**

We recommend that you do **not** enable this option because it may compromise your users' privacy. We **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 (*Home >> Service Configuration >> Service Manager*).
- This setting does **not** appear if you disable the *RecentAuthedMailTracker* setting in WHM's *Service Manager* interface (*Home >> Service Configuration >> Service Manager*).

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

**Note:**

This setting requires Exim 4.34 or later

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 may compromise you users' privacy.

**Note:**

\$body

## Enable BoxTrapper spam trap

This setting allows you to enable BoxTrapper. BoxTrapper is 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 (*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. If you enable this setting, the amount of disk space that mail uses will double.

This setting defaults to *Off*.

**Note:**

\$body

## 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

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™. Apache SpamAssassin is 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 [Apache SpamAssassin](#) interface (*Home >> Mail >> Apache SpamAssassin*). You may 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 (*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 can receive 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 *Off*.

## Enable SquirrelMail webmail

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

This setting defaults to *On*.

## Prefix “mail.” onto Mailman URLs

This setting specifies whether the system should prefix Mailman URLs with `mail.`

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 (*Home >> Mail >> Email Accounts*).

This setting defaults to *32768 MB*. The maximum value is 4 Terabytes (TB).

### Default quota option for new email accounts

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

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

**Note:**

To modify your notification templates, read our [Notification Templates](#) documentation.

### System disk space usage warnings

This setting allows you to enable disk space usage warnings. This setting defaults to *On*.

After you enable disk space usage warnings, the following additional settings become available:

#### Account system disk usage “warn” percentage

This setting allows you to specify the threshold at which a user's disk usage enters the *warn* state, or to disable this notification. This setting defaults to *82.55%*.

#### Account system disk usage “critical” percentage

This setting allows you to specify the threshold at which a user's disk usage enters the *critical* state, or to disable this notification. This setting defaults to *92.55%*.

### Disk quota usage warnings

This setting allows you to enable disk quota usage warnings. The system sends these warnings to cPanel users who approach their disk space quota. This setting defaults to *On*.

After you enable disk space usage warnings, the [disk quota usage settings](#) become available.

### Out of memory warnings

This setting allows you to enable out of memory warnings. The system sends these warnings to cPanel users whose accounts no longer possess memory space. This setting defaults to *On*.



### **Account disk quota "warn" percentage**

This setting allows you to specify the threshold at which a user's disk quota usage enters the *warn* state, or to disable this notification. This setting defaults to *80%*.

### **Notify admin or reseller when disk quota reaches "warn" state**

This setting allows you to specify whether the server sends a notification to the owner of the cPanel account that is in the *warn* state. This setting defaults to *Off*.

### **Account disk quota "critical" percentage**

This setting allows you to specify the threshold at which a user's disk quota usage enters the *critical* state, or to disable this notification. This setting defaults to *90%*.

### **Notify admin or reseller when disk reaches "critical" state**

This setting allows you to specify whether the server sends a notification to the owner of the cPanel account that is in the *critical* state. This setting defaults to *On*.

### **Account disk quota "full" percentage**

This setting allows you to specify the threshold at which a user's disk quota usage enters the *full* state, or to disable this notification. This setting defaults to *98%*.

### **Notify admin or reseller when disk quota reaches "full" state**

This setting allows you to specify whether the server sends a notification to the owner of the cPanel account that is in the *full* state. This setting defaults to *On*.

## **Enable mailbox usage warnings**

This setting allows you to enable mailbox usage warnings. The system sends these warnings to cPanel users whose mailboxes are almost full. This setting defaults to *Off*.

After you enable mailbox usage warnings, the following additional settings become available:

### **Mailbox disk quota "warn" percentage**

This setting allows you to specify the threshold at which a user's mailbox enters the *warn* state, or to disable the notification. This setting defaults to *80%*.

### Mailbox disk quota “critical” percentage

This setting allows you to specify the threshold at which a user’s mailbox enters the *critical* state, or to disable the notification. This setting defaults to *90%*.

### Mailbox disk quota “full” percentage

This setting allows you to specify the threshold at which a user’s mailbox enters the *full* state, or to disable the notification. This setting defaults to *98%*.

### Bandwidth limit check

This setting allows you to select whether to automatically suspend HTTP service for accounts that exceed their bandwidth limit. Disable this option to disable all bandwidth notifications and handle all accounts as though they have unlimited bandwidth. This setting defaults to *On*.

### Send bandwidth limit notification emails

This setting allows you to specify whether the server sends notification emails to accounts that approach their bandwidth limits. This setting defaults to *Off*.

After you enable this option, the following additional settings become available:

#### Bandwidth usage warning: 70%

This setting allows you to specify whether to send an email notification to users who have used 70% of their bandwidth. This setting defaults to *Off*.

#### Bandwidth usage warning: 75%

This setting allows you to specify whether to send an email notification to users who have used 75% of their bandwidth. This setting defaults to *Off*.

#### Bandwidth usage warning: 80%

This setting allows you to specify whether to send an email notification to users who have used 80% of their bandwidth. This setting defaults to *On*.

#### Bandwidth usage warning: 85%

This setting allows you to specify whether to send an email notification to users who have used 85% of their bandwidth. This setting defaults to *Off*.

### Bandwidth usage warning: 90%

This setting allows you to specify whether to send an email notification to users who have used 90% of their bandwidth. This setting defaults to *Off*.

### Bandwidth usage warning: 95%

This setting allows you to specify whether to send an email notification to users who have used 95% of their bandwidth. This setting defaults to *Off*.

### Bandwidth usage warning: 97%

This setting allows you to specify whether to send an email notification to users who have used 97% of their bandwidth. This setting defaults to *Off*.

### Bandwidth usage warning: 98%

This setting allows you to specify whether to send an email notification to users who have used 98% of their bandwidth. This setting defaults to *Off*.

### Bandwidth usage warning: 99%

This setting allows you to specify whether to send an email notification to users who have used 99% of their bandwidth. This setting defaults to *Off*.

### Permit Security Advisor State Change notifications.

This setting controls whether your system will send Security Advisor State Change notifications.

**Note:**

To permanently disable these notifications, you **must** enable this setting and then disable the *Security Advisor State Change* option in WHM's [Contact Manager](#) interface (*Home >> Server Contacts >> Contact Manager*).

**Note:**

\$body

### cPanel PHP max execution time

This setting specifies the number of seconds that a cPanel PHP script can run before the system terminates it. This limit prevents poor server performance due to poorly-written scripts.

This setting defaults to 90 seconds.

## cPanel PHP max POST size

This setting specifies the maximum size, in Megabytes (MB), of a POST request.

This setting defaults to 55 MB.

## cPanel PHP max upload size

This setting specifies the maximum file size, in Megabytes (MB), that a PHP script may upload.

The maximum value that you can specify is 2047 MB. This setting defaults to 50 MB.

## cPanel PHP loader

This setting specifies the PHP loader through which cPanel & WHM executes internal PHP scripts.

This setting defaults to *none*.

**Note:**

You may select more than one PHP loader.

**Note:**

When a user accesses cPanel, WHM, or Webmail on an SSL/TLS port with the HTTP protocol, the web server redirects the user to the URL of the server's hostname with the HTTPS protocol. For example, if the server's hostname is `host.examplehost.com`, `http://www.example.com:2083` will direct the user to the `https://host.examplehost.com:2083` location.

**Important:**

The *Always redirect to SSL*, *Non-SSL redirect destination*, and *SSL redirect destination* settings apply when visitors attempt to access the following URLs:

```
www.example.com/cpanel
www.example.com/webmail
www.example.com/whm
```

These settings do **not** apply to the following URLs:

```
cpanel.example.com
webmail.example.com
whm.example.com
```

## Always redirect to SSL

This setting allows you to redirect users to the proper SSL/TLS ports when they visit specific URLs. This setting defaults to *Off*.

**Notes:**

- To force SSL with the above URLs, enable the *Require SSL* option in the *Security* section of the *Tweak Settings* interface.
- When you enable this option, users **cannot** send their passwords to these links without encryption.
- cPanel's *Calendars and Contacts* interface (*Home >> Email >> Calendars and Contacts*) **requires** that your third-party client

supports redirection.

**Important:**

The *Require SSL* option **does** function with proxy subdomains. However, the *Redirect* option does **not** function with proxy subdomains.

## Non-SSL redirect destination

This setting allows you to specify how to redirect users who access cPanel & WHM without SSL. Select one of the following options:

- *Hostname* — Redirects users to the server's hostname (for example, `host.example.com:2082`, where `host.example.com` is the server's hostname).
- *Origin Domain Name* — Redirects a user to their main domain (for example, `example.com:2082`, where `example.com` is the user's domain).

This setting defaults to *Origin Domain Name*.

## SSL redirect destination

This setting allows you to specify how to redirect users who access cPanel & WHM with SSL. Select one of the following options:

- *SSL Certificate Name* — Redirects users to the domain that the website's SSL certificate secures. You can view this certificate in WHM's [Manage Service SSL Certificates](#) interface (*Home >> Service Configuration >> Manage Service SSL Certificates*).
- *Hostname* — Redirects users to the server's hostname (for example, `host.example.com:2083`, where `host.example.com` is the server's hostname).
- *Origin Domain Name* — Redirects a user to their main domain (for example, `example.com:2083`, where `example.com` is the user's domain).

This setting defaults to *SSL Certificate Name*.

## Logout redirection URL

This setting allows you to redirect users to a specific URL after they log out of cPanel. This setting defaults to *No redirection*.

## Include databases in disk usage calculations

If you enable this setting, your server will include databases in disk usage calculations.

This setting's value defaults to *On*.

## Use INFORMATION\_SCHEMA to acquire MySQL® disk usage

If you enable this setting, your server will use MySQL's `INFORMATION_SCHEMA` view to include disk usage by all MySQL tables in the disk usage totals.

If you disable this setting, cPanel & WHM queries the filesystem for MySQL's disk usage information. Table type usage and local configuration may cause inaccuracy in the disk usage totals.

This setting's value defaults to *On*.

**Note:**

If you use a remote MySQL server, you **must** select *On* in order to calculate MySQL disk usage.

**Warning:**

This setting causes MySQL to become unresponsive until data collection finishes, which may degrade your system's performance.

## Use pre-4.1-style MySQL<sup>®</sup> passwords

This setting allows you to select whether you wish to use old pre-MYSQL 4.1 passwords with your current version of MySQL. This can be useful if you experience authentication problems with PHP scripts.

This setting's value defaults to *Off*.

### Important:

- You **must** restart MySQL to apply this setting. Use WHM's [SQL Server \(MySQL\)](#) interface (*Home >> Restart Services >> SQL Server (MySQL)*) to restart MySQL.
- This setting **only** applies to MySQL 5.5 and earlier. MySQL 5.6 removed support for old-style passwords.
- Your server will **not** automatically reset old-style passwords when you change this setting to *Off*. Any users with old-style passwords **cannot** authenticate until you or they reset their passwords. To reset old-style passwords, use cPanel's [Password & Security](#) interface (*Home >> Preferences >> Password & Security*) or WHM's [Password Modification](#) interface (*Home >> Account Functions >> Password Modification*).
- To determine whether any users have old-style passwords, run the following query in the MySQL command prompt:

```
mysql> SELECT user, Length(Password) FROM mysql.user;
```

Users who return a 16-character length use the pre-4.1-style MySQL password.

## Allow cPanel & WHM to determine the best value for your MySQL `open_files_limit` configuration

This setting allows cPanel & WHM to determine the best value for your MySQL `open_files_limit` setting in your `my.cnf` configuration file. The system uses the total number of open tables in your databases to determine this value.

Newer versions of MySQL require additional file descriptors for each open table. A server with a large number of open tables (for example, servers with multiple installations of WordPress®) may require an `open_files_limit` value that is greater than the default value of 2048. However, an extremely large `open_files_limit` setting requires more memory, and may cause performance issues.

This setting's value defaults to *On*.

## Allow cPanel & WHM to determine the best value for your MySQL `max_allowed_packet` configuration

This setting allows cPanel to determine the best value for your MySQL `max_allowed_packet` setting in your `my.cnf` configuration file.

The `max_allowed_packet` setting determines the maximum size of a single packet for any generated or intermediate string. If you use very long BLOB columns or long strings, this setting **must** be large enough to handle them properly. However, an extremely large `max_allowed_packet` setting may catch unnecessarily large packets, and may cause performance issues.

This setting's value defaults to *On*.

## Allow cPanel & WHM to determine the best value for your MySQL `innodb_buffer_pool_size` configuration

This setting allows cPanel & WHM to determine the best value for your MySQL `innodb_buffer_pool_size` setting in your `my.cnf` configuration file.

The `innodb_buffer_pool_size` setting determines the size of the memory buffer, in bytes, that the InnoDB storage engine uses to cache data and indexes of its tables. However, an extremely large `innodb_buffer_pool_size` setting requires more memory, and may cause performance issues.

If you select *On* for this setting, the system uses the following defaults:

- For servers with less than 512 Megabytes (MB) of RAM, the system sets the `innodb_buffer_pool_size` setting to 8 MB.
- For servers with between 512 MB and 4 Gigabytes (GB) of RAM, the system sets the `innodb_buffer_pool_size` setting to a proportional value that is between 8 and 128 MB.
- For servers with more than 4 GB of RAM, the system sets the `innodb_buffer_pool_size` setting to 128 MB.

This setting's value defaults to *Off*.

## Require a username prefix on names of new databases and database users

When you enable database prefixing, the system prefixes database names and database usernames with the first eight characters of the system username and an underscore (`_`). This makes it easier for you to determine which user owns a given database, but it reduces the number of characters that users can use for names of databases and database users.

**Note:**

If you change the system account name, database names and database usernames that the account owns do **not** change.

This setting's value defaults to *On*.

## Allow autocomplete in login screens.

This setting specifies whether users can save their cPanel, WHM, and Webmail passwords in the browser's cache.

This setting defaults to *On*.

## CGIEmail and CGIEcho

This setting controls whether CGIEmail and CGIEcho exist on the system. These two legacy `cgi-sys` scripts interpret files in a user's `public_html` directory as potential input templates if they contain square bracket (`[ ]`) characters.

**Warning:**

The *CGI Center* interface (*Home >> Software and Services >> CGI Center*) **only** exists for the cPanel x3 theme. You **cannot** create new CGI scripts with the cPanel Paper Lantern theme.

This setting defaults to *On* for backward compatibility.

## Hide login password from cgi scripts

This setting hides the `REMOTE_PASSWORD` variable from scripts that the `cpsrvd` daemon's CGI handler executes. Set this value to *On* to hide the `REMOTE_PASSWORD` variable.

**Warning:**

The *CGI Center* interface (*Home >> Software and Services >> CGI Center*) **only** exists for the cPanel x3 theme. You **cannot** create new CGI scripts with the cPanel Paper Lantern theme.

This setting defaults to *Off*.

**Note:**

This setting does **not** hide the `REMOTE_PASSWORD` variable from phpMyAdmin.

## Cookie IP validation

This setting validates IP addresses for cookie-based logins. Enable this setting to deny attackers the ability to capture cPanel session cookies in order to gain access to your server's cPanel and WHM interfaces.

Select one of the following options:

- *disabled* — Does **not** validate IP addresses.
- *loose* — The access IP address and the cookie IP address **must** be in the same class C subnet.
- *strict* — The access IP address and the cookie IP address **must** match exactly.

This setting defaults to *strict*.

**Note:**

If you enable this setting, we recommend that you also disable the *Proxy subdomain* settings in the *Domains* section of the *Tweak Settings* interface (*Home >> Server Configuration >> Tweak Settings*).

## Generate core dumps

This setting specifies whether cPanel & WHM's services create core dumps. Use core dumps to debug a service.

This setting defaults to *Off*.

**Warning:**

Core dumps contain sensitive information. Make certain that you keep them secure.

## Send passwords when creating a new account

This setting allows you to send new users their passwords in plaintext over email when you create a new account.

This setting defaults to *Off*.

**Warning:**

We **strongly** recommend that you **do not** enable this setting. **It is a security risk.**

## Blank referrer safety check

This setting only permits cPanel & WHM to perform functions when the browser provides a referral URL. Each attempt to submit data to cPanel & WHM **must** have a referral URL. This helps to prevent cross-site request forgery (XSRF) attacks.

This setting defaults to *Off*.

**Warning:**

Exercise caution when you enable this setting. It may break the system's integration with other systems, login applications, and billing software.



**Note:**

The visitor or application that queries the server **must** enable cookies for this setting to take effect.

## Referrer safety check

This setting only permits cPanel & WHM to perform functions when the browser provides a referral URL that **exactly** matches the destination URL. Each attempt to submit data to cPanel & WHM **must** have a referral URL for which the domain or IP address and port number exactly match those of the destination URL. This helps the system prevent cross-site request forgery (XSRF) attacks.

This setting defaults to *Off*.

**Warning:**

Exercise caution when you enable this setting. It may break the system's integration with other systems, login applications, and billing software.

**Note:**

The visitor or querying application **must** enable cookies for this setting to take effect.

## Require SSL

This setting requires that passwords and other sensitive information use SSL encryption.

This setting defaults to *On*.

**Note:**

We **strongly** recommend that you enable this setting.

## Allow PHP to be run when logged in as a reseller to WHM

This setting allows you to specify whether resellers can run PHP code in WHM.

This setting defaults to *Off*.

**Warning:**

Exercise caution when you enable this setting. WHM's PHP code runs as the `root` user.

## Allow apps that have not registered with AppConfig to be run when logged in as a reseller in WHM

This setting allows you to specify whether unregistered AppConfig applications can run when you log in to WHM as a reseller. If you disable this setting, resellers can **only** run registered AppConfig applications.

This setting defaults to *Off*.

## Allow apps that have not registered with AppConfig to be run when logged in as root or a reseller with the "all" ACL in WHM

This setting allows you to specify whether unregistered AppConfig applications can run when you log in as a `root` user. If you disable this setting, `root` users can **only** run registered AppConfig applications.

This setting defaults to *Off*.

## This setting allows WHM applications and addons to execute even if an ACL list has not been defined.

This setting allows you to control whether registered AppConfig applications and addons run if a required ACL is **not** defined. If you disable this setting, cPanel & WHM forces registered AppConfig applications and addons to set an ACL list before they run.

This setting defaults to *Off*.

## This setting allows cPanel and Webmail applications and addons to execute even if a feature list has not been defined.

This setting allows you to control whether registered AppConfig cPanel and Webmail apps can run if a required features list is **not** defined. If you disable this setting, cPanel & WHM forces registered AppConfig cPanel and Webmail apps to set a *Required Features* list before they run.

This setting defaults to *Off*.

## Use MD5 passwords with Apache

This setting specifies whether the system uses MD5 hashing for new passwords in Apache `.htpasswd` files. When you disable this option, Apache uses crypt hashing. Because Apache `.htpasswd` files can contain a mix of crypt-encoded and MD5-encoded passwords without issue, this setting does **not** change the encoding of any existing passwords.

This setting defaults to *On*.

### Note:

MD5-encoded passwords are more secure than crypt-encoded passwords. Crypt only uses the first eight characters of the password for authentication, but the system allows MD5 passwords of length.

## EXPERIMENTAL: Jail Apache Virtual Hosts using `mod_ruid2` and cPanel® jailshell.

This setting enables the *JailManager* TailWatch Driver module. *JailManager* keeps each VirtFS filesystem jail shell in sync with the root filesystem. *JailManager* also returns the VirtFS filesystem jailed shells to a usable state when the system reboots. You do **not** need to enable or disable *JailManager* in the *Service Manager* interface because this setting controls the module's state.

When you enable this setting, the `mod_ruid2` module uses the `chroot` command on Apache virtual hosts. This action runs Apache virtual hosts in an environment with an altered `root` directory.

This setting defaults to *Off*.

### Notes:

- This option is **only** available if you compile Apache through EasyApache and installed `mod_ruid2` version 0.9.4a or later.
- You can use this option with CentOS or RHEL 6 or 7, or Amazon Linux. The `mod_ruid2` module is **not** compatible with

After you enable this option, each user who configured `jailshell` or `noshell` as the shell experiences the following changes:

- The `chroot` command jails the user's Apache Virtual Hosts into the `/home/virtfs` directory.
- The system adds the `RDocumentChRoot` directive to the user's Virtual Host.

```
<IfModule mod_ruid2.c>
    RMode config
    RUidGid kellyp kellyp
==>    RDocumentChRoot /home/virtfs/kellyp /home/kellyp/public_html <==
</IfModule>
```

- The system limits the user's filesystem view to their `/home/virtfs/$USER` filesystem. Various jail shell-related options in the *Tweak Settings* interface (*Home >> Server Configuration >> Tweak Settings*) control the `/home/virtfs/$USER` filesystem configuration.

## Signature validation on assets downloaded from cPanel & WHM mirrors

This setting specifies the type of GnuPG (GPG) key signature file (keyring) that the system uses to verify and sign files that you download from cPanel & WHM `httpupdate` mirrors.

For more information about these GPG keys, read our [cPanel & WHM Download Security](#) documentation.

Select one of the following options:

- *Off* — The system does **not** validate any digital signatures.
- *Release Keyring Only* — Use the Release GPG keyring to validate downloads. The system uses Release keyrings to validate official releases from cPanel & WHM `httpupdate` mirrors.
- *Release and Development Keyrings* — Use the Release and Development GPG keyrings to validate downloads. The system uses Development keyrings to validate test and development releases from cPanel & WHM `httpupdate` mirrors.

This setting defaults to *Release Keyring Only*.

### Warning:

This setting does **not** provide effective security control.

## Verify Signatures of 3rdparty cPAddons

This setting verifies all 3rdparty cPAddons' GPG keys.

This setting is **only** available if you enable the *Signature validation on assets downloaded from cPanel & WHM mirrors* setting.

This setting defaults to *Off*.

### Warning:

This setting is **experimental** and is **not** effective for security control.

## Allow weak checksum schemes

This setting configures the system to allow MD5 hashings when it performs integrity checks on cPanel updates that you download.

This setting defaults to *Off*.

**Warning:**

- This setting is **only** required if you configure your system to download custom RPMs, cPADDONS, or EasyApache updates from non-cPanel sources.
- If you enable this setting, the overall security of your system decreases.

## Enable FormMail-clone CGI

**Warning:**

The *CGI Center* interface (*Home >> Software and Services >> CGI Center*) **only** exists for the cPanel x3 theme. You **cannot** create new CGI scripts with the cPanel Paper Lantern theme.

This setting allows your users to enable the FormMail-clone CGI script in cPanel's deprecated x3 theme's *CGI Center* interface (*Home >> Software and Services >> CGI Center*). This script allows users to publish a form through which their websites' visitors can email them.

This setting defaults to *Off*.

**Note:**

If your cPanel users do **not** use this script properly, it could pose security risks for your server. **We recommend that you select *Off*.**

## Dormant services

This setting configures the system to unload idle services from memory after up to ten minutes of inactivity, and then loads listening devices that correspond to it. This setting reduces memory usage, but delays responses from dormant services. When you enable this setting for a service, that service will immediately enter dormant mode whenever you reboot your server or restart the service.

You can enable this behavior for the following services:

- *cpdavid* — cPanel's WebDav daemon.
- *cphulkd* — cPanel's brute force protection daemon.
- *cpsrvd* — The cPanel & WHM service manager daemon.
- *dnsadmin* — cPanel's DNS management daemon.

**Warning:**

If your server uses a [custom dnsadmin plugin](#), you **must** disable dormant mode for dnsadmin.

- *spamd* — The Apache SpamAssassin™ daemon.

The system enables this setting for each service by default.

**Note:**

Tailwatch checks do **not** prevent or interrupt dormant mode.

## Maintenance cPanel RPM Check

This setting allows you to specify whether the system runs the `/scripts/check_cpanel_rpms` script to check cPanel RPMs for problems during nightly maintenance. If these checks encounter problems, the system sends a notification to the administrator. For more information, read our [The check\\_cpanel\\_rpms Script](#) documentation.

This setting defaults to *On*.

**Warning:**

We **strongly** recommend that you do **not** disable this setting. If you disable this setting, the system does **not** check existing RPMs for problems during updates **or** maintenance. This could leave your system vulnerable to unnoticed tampering or other risks.

## Maintenance cPanel RPM Digest Check

**Note:**

This setting is **only** available if you have enabled the *Maintenance cPanel RPM Check* setting.

This setting allows you to specify whether the system runs a digest check against existing RPMs during nightly maintenance. This check ensures that RPM files are **not** corrupt, and that **nothing** has tampered with them.

If you disable this setting, the system runs the `/scripts/check_cpanel_rpms` script with the `--no-digest` option. For more information, read our [The check\\_cpanel\\_rpms Script documentation](#).

This setting defaults to *On*.

**Important:**

We **strongly** recommend that you enable this setting. If you disable this setting, the `/scripts/check_cpanel_rpms` script **only** validates file sizes, and files may change without detection.

**Note:**

Statistical analysis programs allow your users to view information about their site visitors. For more configuration options, use WHM's [Statistics Software Configuration](#) interface (*Home >> Server Configuration >> Statistics Software Configuration*).

## Awstats reverse DNS resolution

This setting allows you to specify whether [AWStats](#) interprets visitors' domain names as IP addresses. Disable this option to conserve server resources. This setting defaults to *Off*.

## Enable Analog stats

This setting allows you to enable the [Analog](#) statistical analysis program. This setting defaults to *On*.

## Enable AWStats stats

This setting allows you to enable the [AWStats](#) statistical analysis program. This setting defaults to *On*.

## Enable Webalizer stats

This setting allows you to enable the [Webalizer](#) statistical analysis program. This setting defaults to *On*.

### Allow users to update Awstats from cPanel

This setting controls whether cPanel users may update their [AWStats](#) software.

This setting defaults to *Off*.

### Delete each domain's access logs after stats run

This setting controls whether the system deletes each domain's access log after it processes statistics. Enable this setting to help conserve disk space.

This setting defaults to *On*.

### Archive logs in the user's home directory at the end of each stats run unless configured by the user

This setting archives logs in the user's home directory. The system archives the logs at the end of each statistics cycle.

This setting defaults to *On*.

**Note:**

If you configure this setting to *Off*, the system will **not** archive logs.

### Remove the previous month's archived logs from the user's home directory at the end of each month unless configured by the user

This setting controls whether the system removes the archived log files from the user's home directory at the end of each month.

This setting defaults to *On*.

**Note:**

If you configure this setting to *Off*, the system retains archived logs.

### Extra CPUs for server load

This setting allows you to specify a value to add to the number of physical CPUs in your server. The sum of these two numbers becomes the value at which the `cpuwatch`, `cpanellogd`, `backups`, and CPU statistics daemons consider the system to be in a critical load state.

This setting defaults to 0.

### Include password in the raw log download link in cPanel (via FTP)

This setting controls whether the system includes the password in the raw log download link in cPanel's [FTP Accounts](#) interface (*Home >> Files*

>> *FTP Accounts*).

This setting defaults to *On*.

## Keep master FTP log file

This setting allows you to ensure that the system does **not** delete the `/usr/local/apache/domlogs/ftpxferlog` file whenever the system parses FTP logs.

This setting defaults to *Off*.

## Keep log files at the end of the month

This setting allows you to keep domain log files at the end of each month in the `/home/user/logs` directory. If you disable this option, the system deletes these log files.

This item defaults to *Off*.

**Note:**

We **strongly** recommend that you select *Off*. Log files can quickly consume your server's disk space.

## Keep stats logs

This setting allows you to retain the statistics log (`/usr/local/cpanel/logs/stats_log`) between cPanel & WHM restarts.

This setting defaults to *Off*.

**Note:**

If you use WHM's [cPanel Log Rotation Configuration](#) interface (*Home >> Service Configuration >> cPanel Log Rotation Configuration*) to archive the log on a monthly basis, the system may delete the log after it archives the log.

## Apache log file chmod value

This setting allows you to set the Apache log file's `chmod` value. The `chmod` value sets permissions for who can read, write to, and execute a file.

This setting defaults to *0640*.

**Notes:**

- For more information on the `chmod` command, run the `man chmod` command from the command line interface.
- For more information about file permissions, read Wikipedia's [File system permissions](#) article.

## Show bandwidth usage in Megabytes by default in WHM

This setting allows you to specify whether WHM displays bandwidth usage in Megabytes.

This setting defaults to *Off*.

## Stats log level

This setting allows you to specify how much information the server should include in the `/usr/local/cpanel/logs/stats_log` file.

This setting accepts integers between 1 and 10.

This setting defaults to 1.

**Note:**  
\$body

## Log rotation size threshold

This setting allows you to specify a threshold above which the `cpanellogd` daemon rotates log files.

This setting defaults to 300 Megabytes.

## The interval, in days, to retain Exim stats in the database

This setting allows you to specify the number of days during which you wish to keep Exim statistics.

This setting defaults to 90.

## The number of days to keep record of ModSecurity™ rule hits.

This setting allows you to specify the number of days that you wish to maintain your hits records in the `modsec` database.

This setting defaults to 7.

## Number of days to retain upcp logs before purging them

This setting allows you to specify the number of days that you wish to retain logs from the `upcp` nightly maintenance script.

This setting accepts integers between 3 and 999.

This setting defaults to 45 days.

## Critical load threshold

This setting allows you to specify the minimum CPU load above which the following interfaces display the server load in red text:

- WHM's *Service Status* interface (*Home >> Server Status >> Service Status*).
- The *Server Status* section of the Stats table on cPanel's *Home* interface.

This setting defaults to 2.



**Note:**

\$body

**Note:**

Many of the options in this section of the *Tweak Settings* interface allow you to specify whether to send anonymized data to cPanel for analysis. For more information about how cPanel, Inc. uses this data, read our [Server Usage Analysis Data Collection Policy](#).

## Send error reports to cPanel for analysis

This setting allows you to specify whether you wish to send anonymized error reports to cPanel, Inc. for analysis. This setting defaults to *On*.

## Send information about server configuration to cPanel for analysis

This setting allows you to specify whether you wish to send anonymized information about your server configuration to cPanel, Inc. for analysis. This setting defaults to *On*.

## Send information about server usage to cPanel for analysis

This setting allows you to specify whether you wish to send anonymized information about how you use cPanel & WHM to cPanel, Inc. for analysis. This setting defaults to *Off*.

## Update analysis retention interval

This setting allows you to specify how long to keep the update analysis log files that you send to cPanel, Inc.

The following options are available:

- *Disable message retention* — Select this option if you no longer wish to keep update analysis log files.
- *90 Days* — Select this option to keep update analysis log files for 90 days. **This is the default option.**
- *Save indefinitely* — Select this option to keep update analysis log files indefinitely.
- *days* — Select this option to enter the number of days that you wish to keep the log files.

The system stores update analysis log files in the `/usr/local/cpanel/logs/update_analysis` directory.

## Accounts that can access a cPanel user account

This setting allows you to specify which users can log in to a cPanel account. This setting defaults to *Root, Account-Owner, and cPanel User*.

- *Root* is the server owner.
- *Account-Owner* is the account's owner (the `root` user or a reseller).
- *cPanel User* is the cPanel account user.

**Note:**

If you disallow `root` or reseller logins to cPanel accounts, the disallowed `root` user or reseller **cannot** access the following items:

- The cPanel icon in WHM's *List Accounts* interface (*Home >> Account Information >> List Accounts*), which provides access to the user's cPanel account.
- The *Live Editor* feature in WHM's *x3 Branding* interface (*Home >> cPanel >> x3 Branding*).
- The *Customize HTML pages* feature in WHM's *Legacy Configure Customer Contact* interface (*Home >> Support >> Legacy Configure Customer Contact*).

---

## Allow server-info and server-status

This setting allows you to specify additional IP addresses and hostnames that can access the `example.com/server-status` page, where `example.com` represents the domain's name. If you installed the `mod_info` Apache module, this setting also applies to the `example.com/server-info` page. Enter the desired IP addresses or hostnames in the text box, one IP address or hostname per line.

### Important:

- We **strongly** recommend that you use caution when you allow access to these pages. They display sensitive information about your server.
- cPanel & WHM does **not** install the `mod_info` Apache module by default. To use this module, you must use either [Raw Options](#) in EasyApache 3, or install it with `yum` in EasyApache 4.

## Allow cPanel users to install SSL Hosts

This setting allows you to specify whether to allow cPanel users to install SSL hosts.

This setting defaults to *On*.

## Send anonymous usage data to cPanel

This setting allows you to specify whether to send anonymized usage information to cPanel, Inc. cPanel, Inc. uses this data to improve the product's functionality.

This setting defaults to *On*.

## Apache non-SSL IP/port

This setting allows you to specify a new port or IP address that Apache uses to listen for requests and serve web pages over an unsecured connection.

This setting defaults to `0.0.0.0:80`, which indicates that Apache uses port 80 to serve content on an unsecured connection for all of your server's IP addresses.

### Warning:

Enter an IP address to prevent Apache's ability to listen on all other IP addresses. This setting could deny HTTP traffic the ability to route correctly, which renders your site inaccessible to visitors.

## Apache SSL port

This setting allows you to specify a new port or IP address that Apache uses to listen for requests and serve web pages over a secure connection.

This setting defaults to `0.0.0.0:443`, which indicates that Apache uses port 443 to serve content on a secure connection for all of your server's IP addresses.

---

**Warning:**

Enter an IP address to prevent Apache's ability to listen on all other IP addresses. This setting could deny HTTP traffic the ability to route correctly, which renders your site inaccessible to visitors.

## cPanel & WHM API Shell (for developers)

This setting allows you to add the following interfaces, which allow the `root` user and resellers to test [API functions](#) directly:

- WHM's [API Shell](#) interface ([Home](#) >> [Development](#) >> [API Shell](#))
- cPanel's [API Shell](#) interface ([Home](#) >> [Advanced](#) >> [API Shell](#))

**Note:**

To enable this feature for cPanel, you **must** grant the [API Shell](#) feature to the desired `root` user and resellers in WHM's [Feature Manager](#) interface ([Home](#) >> [Packages](#) >> [Feature Manager](#)), and then refresh your browser window.

This setting defaults to *Off*.

## BIND deferred restart time

This setting allows you to specify the time (in seconds) that the `dnsmadmin` service waits before it restarts BIND. The system silently discards additional restart requests in this time period.

**Notes:**

- On busy servers, we recommend that you set this number to 300 or 600 to prevent multiple subsequent restarts.
- If your system experiences very few DNS changes, we recommend that you use the default setting of 0.

## The number of seconds between ChkServd service checks

This setting allows you to specify the number of seconds between each `chkserverd` daemon service check. You can specify any value between 60 and 7200. This setting defaults to 300.

**Note:**

Before you set a value below 300, we recommend that you use the `/var/log/chkserverd` file to verify the length of your system's `chkserverd` checks. The settings that you choose in WHM's [Service Manager](#) interface ([Home](#) >> [Service Configuration](#) >> [Service Manager](#)) affect the length of these checks.

## The number of times ChkServd allows a previous check to complete before termination

This setting allows you to specify the number of times that the `chkserverd` daemon allows a check to complete before termination. You can specify any value between 1 and 20.

This setting defaults to 2.

## The option to enable or disable ChkServd HTML notifications

This setting allows you to enable or disable HTML notifications for the `chkserverd` daemon.

This setting defaults to *On*.

### The option to enable or disable ChkServd recovery notifications

This setting allows you to enable or disable recovery notifications for the `chkserverd` daemon.

This setting defaults to *On*.

### Conserve memory

This setting allows you to specify whether to conserve memory (RAM) at the expense of more CPU usage and disk I/O.

This setting defaults to *Off*.

### cpsrvd username domain lookup

This setting allows you to specify whether WHM automatically supplies a username (based on the account name) when a cPanel user enters a login password.

This setting defaults to *Off*.

### Gzip page compression

This setting allows you to specify whether to use gzip compression when you view cPanel & WHM interfaces in your web browser. This helps to reduce bandwidth usage.

This setting defaults to *On*.

### Allow Sharing Nameserver IPs

This setting allows you to specify whether users can share nameserver IP addresses. Select *On* to decrease the number of IP addresses that you need in your IP address pool.

This setting defaults to *Off*.

### Cache disk quota information

This setting allows you to specify whether WHM caches disk usage information. If you select *On*, the cache process may result in disk usage information that is up to 15 minutes out-of-date.

This setting defaults to *On*.

**Warning:**

If you disable this setting, you may experience in a large performance degradation.

## Reverse DNS lookup upon connect

This setting allows you to specify whether cPanel & WHM attempts to resolve a client's IP address to a domain name whenever a user connects to a cPanel service. This setting defaults to *Off*.

**Warning:**

If you enable this setting, it may degrade your server's performance.

## Enable optimizations for the C compiler

This setting allows you to specify whether the compiler optimizes code for your system. This setting defaults to *Off*.

**Warning:**

On some systems, compiler optimizations can trigger a bug in system libraries.

## Max HTTP submission size

This setting allows you to specify the maximum file size, in Megabytes, that a user can upload to your server. This setting applies to all uploads and form submissions in cPanel & WHM, which includes Webmail, cPanel's *File Manager* interface (*Home >> Files >> File Manager*), and phpMyAdmin.

Enter a value between 1 and 10240.

This setting defaults to *Unlimited*.

## File upload required free space

This setting allows you to specify the minimum filesystem quota space that the system requires after a file uploads to your server. This helps ensure that users do not meet or exceed their quota limits. This setting applies to all uploads and form submissions in cPanel & WHM, which includes Webmail, cPanel's *File Manager* interface (*Home >> Files >> File Manager*), and phpMyAdmin.

This setting defaults to 5 MB.

## Interval, in days, between rebuilds of the FTP quota and disk usage data (applies to Pure-FTPd only)

This setting allows you to specify the number of days between rebuilds of the FTP quota and disk usage data for Pure-FTP.

This interval allows the system to consider account disk usage information for files that other processes modify or add to a user's root FTP directory. A higher setting will reduce disk I/O, but lower the accuracy of the usage data. A lower setting will improve accuracy, but will consume more disk I/O.

This setting defaults to 30 days.

## Depth to recurse for .htaccess checks

This setting allows you to specify the maximum number of directories deep to look for `.htaccess` files when you change the PHP handler.

**Warning:**

We **strongly** recommend that you do **not** enter a value that is higher than 10. A value that is higher than 10 can degrade your server's performance.

**Note:**

This setting comments out any `AddHandler` directive lines in your users' `.htaccess` files that change how the system handles PHP.

For example, if the `/home/user/public_html/` directory is your document root, and 2 is the value for this setting, the system searches the following directories for `.htaccess` files:

- `/home/user/public_html/`
- `/home/user/public_html/directory1/`
- `/home/user/public_html/directory2/`

The system does **not** search the following directory:

- `/home/user/public_html/directory1/directorya/`

This setting defaults to 2.

## Enable legacy warnings

This setting allows you to specify whether you receive warnings about features that future cPanel & WHM releases will deprecate. This setting defaults to *On*.

**Warning:**

If you disable this setting, you will **not** receive warnings about features that future releases remove. This could lead to a non-functional server when we remove these features.

## Listen on IPv6 Addresses

This setting causes the `cpsrvd` daemon, and other cPanel & WHM services, to listen on IPv6. If you do not enable this setting, WHM, cPanel, Webmail, and Web Disk will **not** function via IPv6.

This setting defaults to *Off*.

**Warning:**

After you enable this setting, you **must** run the following scripts from the command line:

- `/scripts/restartsrv_cpsrvd`
- `/scripts/restartsrv_cpdavd`
- `/scripts/restartsrv_nsd`

## I/O priority level at which bandwidth usage is processed

This setting allows you to specify the sever's I/O priority for bandwidth log processing. Enter a value between 0 and 7.

This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

## I/O priority level at which stats logs are processed

This setting allows you to specify the server's I/O priority when it processes statistics logs. Enter a value between 0 and 7.

This setting defaults to 7.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

## I/O priority level at which nightly backups are run

This setting allows you to specify the disk's I/O priority for nightly backups. Enter a value between 0 and 7.

This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

## I/O priority level at which cPanel-generated backups are run

This setting allows you to specify the server's I/O priority for cPanel-generated user backups. Enter a value between 0 and 7.

This setting defaults to 7.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

## I/O priority level for user-initiated processes

This setting allows you to specify the server's I/O priority for certain user-initiated processes. This setting applies to a few especially I/O-intensive user functions, such as actions that cPanel's *File Manager* interface (*Home >> Files >> File Manager*) initiates. Enter a value between 0 and 7.

This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

### I/O priority level at which quota checks are run

This setting allows you to specify the server's I/O priority for quota checks. Enter a value between 0 and 7. This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

### The I/O priority level at which FTP quota checks are run (when Pure-FTPd is enabled)

This setting allows you to specify the server's I/O priority for FTP quota checks for Pure-FTPd. Enter a value between 0 and 7.

This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

### I/O priority level at which email\_archive\_maintenance is run

This setting allows you to specify the server's I/O priority level for the `email_archive_maintenance` script. Enter a value between 0 and 7.

This setting defaults to 6.

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

### I/O priority level at which dovecot\_maintenance is run

This setting allows you to specify the server's I/O priority level for the `dovecot_maintenance` script, which cPanel & WHM uses to maintain



mailboxes. Enter a value between 0 and 7.

This setting defaults to 7

**Notes:**

- Your operating system's kernel **must** support `ionice`, and `ionice` **must** exist on the server, for this setting to function properly.
- This setting specifies the "best effort" priority.
- A value of 0 grants the highest priority, while a value of 7 grants the lowest.

## Use cPanel® jailshell by default

This setting allows you to configure accounts to use the cPanel jailshell by default.

This setting defaults to *Off*.

**Notes:**

- We **strongly** recommend that you enable these options.
- Jailed shell systems, by default, mount all filesystems with the `noexec` option. The `noexec` option blocks the operation of `setuid` and `setgid` commands, such as the `ping` command. However, this does **not** apply to Exim's `/usr/sbin/` directory.
- For more information, read our [How to Create Custom Jailed Shell Mounts](#) documentation.

## Jailed /proc mount method

This setting allows you to permit the use of the `/proc` virtual filesystem in a jailshell.

**Note:**

If the system runs any version of Red Hat® Enterprise Linux (RHEL), CentOS, or CloudLinux™ on XenPV, the `/proc` virtual filesystem inside of the jailshell behaves in the same way that it does on version 5 of RHEL, CentOS, or CloudLinux.

You can choose from the following options:

- *Always mount a full /proc* — The `/proc` virtual filesystem has full privileges.
- *Mount limited /proc for RHEL, CentOS, and CloudLinux™ 6, Full /proc for RHEL, CentOS, CloudLinux, or xenpv 5 or 7*
  - In version 6 of RHEL, CentOS, and CloudLinux, and on Amazon Linux, the system limits the `/proc` virtual filesystem to the processes in the user's jailshell session.
  - In version 7 of RHEL, CentOS, and CloudLinux, the `/proc` virtual filesystem includes **all** processes.
- *Mount limited /proc for RHEL, CentOS, and CloudLinux™ 6, No /proc for RHEL, CentOS, CloudLinux, or xenpv 5 or 7*
  - In version 6 of RHEL, CentOS, and CloudLinux, and on Amazon Linux, the system limits the `/proc` virtual filesystem to the processes in the user's jailshell session.
  - In version 7 of RHEL, CentOS, and CloudLinux, the system does **not** mount the `/proc` virtual filesystem inside the jail.

This setting defaults to *Mount limited /proc for RHEL, CentOS, and CloudLinux™ 6, Full /proc for RHEL, CentOS, CloudLinux, or xenpv 5 or 7*.

## Jailed /bin mounted suid

This setting allows you to permit the use of the `setuid` option in the `/bin` directory in a jailshell. This setting defaults to *Off*.

System administrators who wish to run `setuid` commands, such as the `/bin/ping` command, may wish to use this setting.

**Note:**

This setting does not affect servers that run CentOS 7, RHEL 7, or CloudLinux 7.

## Jailed /usr/bin mounted suid

This setting allows you to permit the use of the `setuid` option in the `/usr/bin` directory in a jailshell.

System administrators who wish to run `setuid` commands (for example, the `/usr/bin/crontab` command) may wish to use this setting.

**Note:**

We do **not** recommend that you enable this setting. When you enable this setting, users can install a crontab that runs outside of their jailed shells. This action allows users to escape from the jailed environment.

This setting defaults to *Off*.

## Max cPanel process memory

This setting allows you to specify the maximum amount of memory that a cPanel process can use before the system automatically kills it.

Select *Unlimited* if you do **not** want to impose a memory limit on cPanel processes.

This setting defaults to 512 MB.

**Important:**

We **strongly** recommend that you specify a value of 512 or **higher**.

## Max cPanel/WHM/Webmail service handlers

This setting allows you to specify the maximum number of concurrent connections for the cPanel daemon, `cpssrzd`.

This setting defaults to 160.

## Send language file changes to cPanel

This setting allows you to select whether to send changes to your cPanel & WHM language files to cPanel during software updates.

This setting defaults to *On*.

## Remote WHM timeout

This setting allows you to specify the number of seconds to allow a connection between this server and other remote WHM servers to remain idle before it times out.

This setting defaults to 35 seconds.

## Disk usage/quota bailout time

This setting allows you to specify the maximum amount of time, in seconds, during which the system may attempt to retrieve disk usage and quota information before it considers the data to be unavailable.

This setting defaults to 60 seconds.

## Reset Password for cPanel accounts

This setting enables the *Reset Password* feature for cPanel account users. The *Reset Password* feature uses the account's contact email address to verify a password reset request. The email contains a security code that verifies whether the user can access to the Subaccount's contact email address as part of the password reset verification process. The link to request this email displays in the cPanel login interface.

This setting defaults to *off*.

**Important:**

To use this feature, the cPanel user **must** set the contact email address in cPanel's [Contact Information](#) interface (*Home >> Preferences >> Contact Information*).

## Reset Password for Subaccounts

This setting enables the *Reset Password* feature and new Subaccount invites for cPanel Subaccount users. The *Reset Password* feature uses the Subaccount's contact email address to verify a password reset request. The email contains a security code that verifies whether the user can access to the contact email address as part of the password reset verification process. The link to request this email displays in the cPanel login interface.

This setting defaults to *off*.

**Important:**

To use this feature, you **must** set the Subaccount's contact email address in cPanel's [User Manager](#) interface (*Home >> Preferences >> User Manager*).

## Server Locale

This setting allows you to specify the locale that the system uses whenever a user selects a cPanel locale that does **not** exist, or whenever a user's web browser requests an invalid locale in the HTTP `Accept-Language` header. Set this value to a locale that administrators, resellers, and users may understand.

**Warning:**

When you modify this setting and click *Save*, the system applies the new language to your WHM interface **immediately**.

## Send a notification when a user's backup has errors

This setting allows you to specify whether the server notifies you when a user's cPanel backup file contains errors.

This setting defaults to *Off*.

## Allow other applications to run the cPanel and admin binaries

This setting allows you to specify whether cPanel and admin binaries run from applications other than the cPanel server daemon (`cpssrvd`). This setting is useful for advanced administrators who are familiar with Perl scripting and who wish to run cPanel from their own custom programs.

This setting defaults to *Off*.

## Enable WHOIS lookups for the nameserver IP manager

This setting allows you to specify whether to allow WHM's *NS Record Report* interface (*Home >> DNS Functions >> NS Record Report*) to perform WHOIS lookups.

This setting defaults to *On*.

## ChkSrvd TCP check failure threshold

This setting allows you to specify the number of times that a `chkserverd daemon` TCP check must fail before the system restarts the service and sends a notification. On heavily loaded systems, these types of service checks fail occasionally, which produces erroneous indications that services are down.

This setting defaults to 3.

### Notes:

- We recommend a value of three or higher for most systems.
- To disable notifications and restarts, select *Disable notifications and restarts from TCP checks*.

## Number of seconds an SSH connection related to an account transfer may be inactive before timing out

This setting allows you to specify a number of seconds of inactivity after which account transfers' SSH connections time out. Enter any number between 900 and 172800.

This setting defaults to 500 seconds.