Version 11.32 Release Notes

These Release Notes detail feature updates in cPanel & WHM version 11.32

Upgrade to version 11.32

Per our Operating System End Of Life Policy for cPanel & WHM FreeBSD systems and legacy Linux systems will not be able to upgrade to cPanel & WHM version 11.32

Systems that use `mbox`, or which have Exim updates disabled, will also not be able to upgrade to cPanel & WHM version 11.32.

Downgrade from 11.32 to earlier versions

In cPanel & WHM version 11.32, we added complete support for a downgrade to earlier cPanel & WHM versions.

However, once a system has upgraded to version 11.32, the following changes will block a downgrade to version 11.30:

* An upgrade to MySQL 5.5
* When you enable MyDNS-NG

It is no longer necessary to run a script, such as `/usr/local/cpanel/scripts/downgrade_cpanel` to downgrade from version 11.32 to version 11.30. To downgrade to version 11.30, change your tier in WHM's *Update Preferences* interface (*Main >> Server Configuration >> Update Preferences)* and run the `/usr/local/cpanel/scripts/upcp` script

Supported operating systems

The following table shows the operating systems that are supported in cPanel & WHM version 11.32:

OS	Version	Arch	Supported
CentOS	3	i386	N
CentOS	3	x86-64	N
CentOS	4	i386	Y
CentOS	4	x86-64	Y
CentOS	5	i386	Y
CentOS	5	x86-64	Y
CentOS	6	i386	Y
CentOS	6	x86-64	Y
CloudLinux	5	i386	Y
CloudLinux	5	x86-64	Y
CloudLinux	6	i386	Y
CloudLinux	6	x86-64	Y
FreeBSD	All	i386	N
FreeBSD	All	AMD64	N
RHEL	3	i386	N
RHEL	3	x86-64	N
RHEL	4	i386	Y
RHEL	4	x86-64	Y
RHEL	5	i386	Y
RHEL	5	x86-64	Y

| RHEL | 6 | i386 | Y |
| RHEL | 6 | x86-64 | Y |

New features

Update analysis reports

In cPanel & WHM version 11.32, we added a new feature called *Update Analysis* that records update (`upcp`) information on individual servers and reports back to cPanel.

After `upcp` runs, the update analysis process, `/usr/local/cpanel/scripts/gather-update-logs`, performs checks to confirm a successful update. Then, this process stores the update information as tarball files in the `/usr/local/cpanel/logs/update_analysis` file.

These tarball files will only be deleted if you do not report the update information to cPanel. You can enable or disable reports of updated information to cPanel via WHM's *Send update analysis to cPanel* interface (*Main* >> *Tweak Settings* >> *Send update analyses to cPanel*.) If reporting update information to cPanel is currently disabled, you can also enable this option from the *Send Update Analysis to cPanel* notification box in the following locations:

- The *Update Preferences* interface (*Main* >> *Update Preferences*).
- The *Upgrade to Latest Version* interface (*Main* >> *Upgrade to Latest Version*).

MyDNS-NG support

In cPanel & WHM 11.32, WHM supports the database-driven nameserver MyDNS-NG.

You can select this option in WHM's *Nameserver Selection* interface (*Main* >> *Service Configuration* >> *Nameserver Selection)*. When you make the selection, WHM installs MyDNS-NG version 1.2.8.31.

> **Important:**
> If you change your nameserver to MyDNS-NG, you will disqualify your cPanel & WHM installation from a downgrade to version 11.30. To effect a downgrade, change the nameserver to BIND or NSD, or disable the service.

Custom jailed shell (jailshell) mounts

System administrators can now define custom jailed shell mounts.

Account and package configuration options

In cPanel & WHM version 11.32, we have added new configuration options.

You can now configure the following options when you create or manage packages and accounts via the WHM *Create a New Account*, *Modify an Account*, *Add a Package*, and *Edit a Package* interfaces:

- *Maximum Hourly Email by Domain Relayed* (This setting corresponds to *Max hourly emails* in *Tweak Settings*. A value of 0 means *unlimited*.)
- Maximum percentage of failed or deferred messages a domain may send per hour

You can also configure these options via our XML API. This change applies to the following API calls:

- Create Account (`createacct`) — Create a new cPanel account.
- Modify Account (`modifyacct`) — Modify an existing cPanel account.
- List Accounts (`listaccts`) — List cPanel accounts hosted on your system.
- Add Package (`addpkg`) — Add a new cPanel package.
- Edit Package (`editpkg`) — Edit an existing cPanel package.
- List packages (`listpkgs`) — List existing cPanel packages on your system.

Mail delivery reporting

In WHM, a new interface called *Mail Delivery Reports* appears. This screen allows you to search for mail that is sent and received by users on your system.

A few points to note about the *Mail Delivery Reports* functionality:

- Sorting columns will also re-run the report query. As a result, each time you sort a column, a different number of reports that match your query will be shown. If the report query includes the current day, it will indicate continuous mail activity.
- Results per *Advanced Search* query are limited to 5000.

Modified or replaced features

POP before SMTP authentication default

POP before SMTP authentication is not enabled by default as of 11.32. You can enable this option in WHM's *Antirelayd* interface (*Main >> Service Configuration >> Service Manager >> Antirelayd.*) SMTP authentication is still supported and enabled by default.

Outgoing email limit options

cPanel & WHM version 11.32 implements several changes to the way that cPanel & WHM limits outgoing email from your server.

The options that are listed below now appear in the *Tweak Settings* interface.

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

In previous versions of cPanel & WHM, when a domain reached the limit set for *Max hourly emails per domain* in *Tweak Settings*, additional messages sometimes failed, and sometimes were deferred. This new setting allows server owners to apply a consistent result to all domains on the server that exceed the hourly email limit.

The server owner uses this setting to indicate the quantity of messages that will be queued by the system and delivered in the next hour.

For example, if you set this value to 125%, then once the account reaches its hourly limit, Exim will queue any additional messages, up to 125% of the *Max hourly emails per domain* value. Once the account reaches 125% of the *Max hourly emails per domain* value, any additional outgoing messages are discarded.

To discard all messages sent by domains that have exceeded their limits, set this option at *100*.

By default, *The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery* is set to *125%*.

Count mailman deliveries towards a domain's Max hourly emails

Server administrators may choose to count emails to Mailman mailing lists against an account's outgoing email limit (which is set using the *Max hourly emails per domain* option in the *Tweak Settings* interface).

By default, the *Count mailman deliveries towards a domain's Max hourly emails* setting is *Off*.

> **Note**
> This setting should remain *Off* if you wish to accommodate users with large Mailman mailing lists. If you turn this setting *On*, your mailing list subscribers may not receive messages.

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

This new *Tweak Settings* option allows the server administrator to specify the percentage of email messages that must fail or be deferred in an hour in order for a domain to be restricted from sending email.

When this percentage of email messages fail or are deferred, the domain will not be able to send email for the remainder of the hour in which the restriction occurred. (The minimum number of messages which must fail or be deferred in order for this setting to take effect is 5.)

The default value for the *Maximum percentage of failed or deferred messages a domain may send per hour* setting is *Unlimited*.

Dormant mode for three daemons

The `cpdavd`, `cphulkd`, and `cpsrvd` daemons now offer a special *Dormant* mode. *Dormant* mode offers a significant reduction in memory use by the daemon. When the daemon is idle, the daemon process is replaced with a listener process. Upon the detection of network activity on the port, the listener process starts the daemon to handle the request.

You can enable reduced memory consumption for individual daemons via the *Dormant services* option in the *Tweak Settings* interface.

Keep in mind that enabling Dormant Mode for a daemon will cause slight delays in responding to new connections, since the listener process must start the daemon.

Configurable timeout threshold for FTP backups

In cPanel & WHM version 11.32, you can configure the timeout threshold that is used when you copy backups via FTP. To configure this option, navigate to WHM's *Configure Backup* feature (*Main >> Backups >> Configure Backups)*.

The default threshold is 120 seconds.

> **Note:**
> This threshold only applies to backups that are created by `cpbackup`, the system-wide backup utility.

Prevent cPanel users from creating specific domains.

In cPanel & WHM version 11.32, we renamed WHM's *Block Common Domain Usage* option on the *Tweak Settings* interface. It is now labeled *Prevent cPanel users from creating specific domains*.

We also extended this option, which allows you to prevent the creation of specific domains by cPanel users.

To see which domains are blocked by default when you select this option, view the `/usr/local/cpanel/etc/commondomains` file.

To add domains to this list (and block their creation on your server):

1. Create the `/var/cpanel/commondomains` file.
2. In `/var/cpanel/commondomains`, list the domains for which you wish to prevent the creation of by cPanel users.
   - You must separate domains with a new line.

Restrict outgoing SMTP to root, Exim, and Mailman

Prior to cPanel & WHM version 11.32, the *Restrict outgoing SMTP to root, exim, and mailman* option on the *Tweak Settings* screen would block any attempt to work around the Exim Sendmail binary.

In version 11.32, when this option is set to *On*, cPanel & WHM redirects the outgoing connection attempt to the local mail server.

Email authentication support

Exim is updated to version 4.77. With this comes an end of support for DomainKeys signing of outgoing messages.

Verification of DomainKeys signed messages is still possible by means of integration with SpamAssassin. However, we urge all cPanel & WHM users to update to the DKIM method of email authentication.

cPanel & WHM's existing DomainKeys implementation was converted to DKIM, and extended in a number of ways. Wherever possible, Perl modules and command line utilities were renamed from DomainKeys to DKIM. For example, the utility scripts `/usr/local/cpanel/bin/domain_keys_installer` and `/usr/local/cpanel/bin/domain_keys_uninstaller` were renamed to `/usr/local/cpanel/bin/dkim_keys_install` and `/usr/local/cpanel/bin/dkim_keys_uninstall`. Any existing scripts you created that relied upon our DomainKeys implementation should be examined for compatibility with DKIM.

WHM now also provides an indication of whether an account has DKIM and SPF enabled. This status is recorded in the cPanel user file (stored in

`/var/cpanel/users`) as one of the following directives:

- `HASDKIM`
- `HASSPF`

A value of `1` means support is enabled; a value of `0` means support is disabled.

For DKIM, the directive is used to determine whether a key needs to be generated and installed when adding domains to an existing cPanel account. The values can be set via one of the following methods:

1. When you create an account.
2. Via the *Modify an Account* interface in WHM.
3. Via the *Email Authentication* interface in cPanel.

The following API 2 functions are related to DKIM.

- `Email::set_email_signing` — Enables or disables DKIM for an account.
- `Email::get_email_signing` — Indicates whether DKIM is supported and enabled for an account.

Prior versions of cPanel & WHM would perform DKIM validation on incoming email by means of SpamAssassin. Signature failure affects SpamAssassin scoring, which can be used to determine whether the system should deliver the message.

In 11.32, an ACL is provided that will cause Exim to reject messages that fail DKIM signature validation. The ACL only applies to messages that contain a DKIM signature.

> **Notes:**
> - Any event which modifies a message after signing will cause DKIM verification to fail. (For example, mailing lists commonly modify the message body by adding a mailing list signature.)
> - Because Exim is compiled with DKIM and SPF support, it will always verify syntactically valid signatures in incoming email messages, even if DKIM and SPF are disabled. This could degrade the server's performance. For more information, visit the E xim documentation

Account creation and modification options

The WHM *Create a New Account* and *Modify an Account* features now provide a way to create DKIM and SPF records.

For SPF, WHM uses a default record of `v=spf +a +mx+ipv4:local_address` `?all`.

Resellers and root users may add a custom SPF record to the appropriate Zone Template. However, if you customize the SPF record in this fashion, it will disable the SPF control in the *Create a New Account* and *Modify an Account* interfaces.

In addition, the WHM *Modify an Account* feature now offers a method you can use to enable or disable DKIM and SPF entries for all zones that are owned by the account.

MySQL configuration and upgrade considerations

MySQL 5.0 configuration

In cPanel & WHM version 11.32, fresh installations of MySQL 5.0 will be configured to use the InnoDB file per-table setting (`innodb_file_per _table`). (This configuration also applies to later versions of MySQL which are compatible with the InnoDB file per-table setting.)

The InnoDB file per-table setting stores all InnoDB data in a single file, which improves the reliability of the InnoDB table. This setting reduces the possibility that a single corrupt InnoDB table will impact other InnoDB tables.

This configuration setting may cause a performance reduction on some systems due to the way MySQL updates files that store InnoDB data.

You may change this configuration setting in the `/etc/my.cnf` file.

MySQL 5.5 upgrade considerations

11.32 includes support for MySQL 5.5.

MySQL 5.5 uses its native InnoDB instance instead of the InnoDB plugin. When the server administrator uses WHM's *MySQL Upgrade* interface to upgrade MySQL to version 5.5, the `/etc/my.cnf` file is modified to disable the InnoDB plugin. The presence of the plugin in the `/etc/my.c`

`nf` file can cause a fatal error during installation. This error will result in a corrupted MySQL installation.

The following entries are removed from `/etc/my.cnf` if they are found:

- `ignore-builtin-innodb`
- `plugin-load=innodb=ha_innodb_plugin.so`
- `plugin-load=innodb=ha_innodb_plugin.so;innodb_trx=ha_innodb_plugin.so;innodb_locks=ha_innodb_plugin.so;innodb_lock_waits=ha_innodb_plugin.so;innodb_cmp=ha_innodb_plugin.so;innodb_cmp_reset=ha_innodb_plugin.so;innodb_cmpmem=ha_innodb_plugin.so;innodb_cmpmem_reset=ha_innodb_plugin.so`

A number of deprecated configuration directives will cause fatal errors when used with MySQL 5.5. To reduce the chance of fatal errors during the upgrade, the *MySQL Upgrade* function in WHM will perform the following actions:

1. Temporarily move `/etc/my.cnf` to `/etc/my.cnf.rpmsave`. Once the upgrade is complete, the original version of `/etc/my.cnf` is restored.
2. Comment out any directives in `/etc/my.cnf` that are known to be incompatible with MySQL 5.5.

> **Warning:**
> If you manually change the MySQL version and run the `/usr/local/cpanel/scripts/mysqlup` script, it will not afford you the same protections as the WHM *MySQL Upgrade* feature will. We recommend that you change your MySQL version with WHM's *MySQL Upgrade* interface (*Main >> Software >> MySQL Upgrade)* in WHM to change your MySQL version.

Run dnsadmin

Normally, a new `dnsadmin` process is started for each zone-related action in cPanel & WHM.

In cPanel & WHM version 11.32, server administrators can choose to run `dnsadmin` as a standalone daemon. This improves speed, but increases memory usage.

To enable `dnsadmin` as a standalone daemon, navigate to WHM's *Service Manager* interface and select the *Enabled* checkbox for *dnsadmin*.

Run optimizefs

By default, the `optimizerefs` utility runs with an ionice priority of `6`. (To learn more about ionice, see the ionice man page.)

In cPanel & WHM version 11.32, server administrators can disable `optimizefs`. To disable this utility, create the following flag file: `/var/cpanel/optimizefsdisable`

BoxTrapper functionality

We have made the following updates to BoxTrapper:

- **Verification link** — When BoxTrapper is enabled in cPanel & WHM version 11.32, verification emails will include a verification link. To prompt BoxTrapper to deliver the original email to the intended recipient's account, the original sender can either reply to the verification email or click the verification link.
- **Whitelisting by association** — If the address in the *From* field of an incoming email is whitelisted, then BoxTrapper will automatically whitelist the addresses in the *To* and *CC* fields. To turn this feature on and off, select the *Auto Whitelist To and From lines from whitelisted senders (whitelist by association)* checkbox on the cPanel *BoxTrapper Configuration* screen.
- **Deliver messages with a spam score lower than -2.5 (adjustable)** — When BoxTrapper receives an email with a spam score lower than the value set in the *Minimum SpamAssassin Spam Score required to bypass BoxTrapper* setting on the *BoxTrapper Configuration* screen, it automatically delivers the message. The default value for this setting is *-2.5*.

cPAddons available for installation by default

In cPanel & WHM version 11.32, the list of cPAddons which are available for installation by default has changed. Formerly, this list included:

- YaBB
- phpMyChat
- AgoraCart

This list now includes:

- WordPress®

Update Preferences interface version number display

In cPanel & WHM version11.32, the WHM *Update Preferences* interface (*Main >> Server Configurations >> Update Preferences)* will show the current version number beside each release tier option.

FrontPage® extensions default

In cPanel & WHM version 11.32, you must enable FrontPage extensions for new accounts. Unlike prior versions of cPanel & WHM, FrontPage extensions are disabled by default.

This change will apply to accounts you create in WHM's *Create a New Account* interface (*Main >> Account Functions >> Create a New Account*) and the following scripts:

- `/usr/local/cpanel/scripts/wwwacct`
- `/usr/local/cpanel/bin/wwwacct`
- `/usr/local/cpanel/bin/createacct`

Password strength configuration

cPanel & WHM version 11.32 addresses discrepancies between the *Password Strength Configuration* feature and the password strength security policy in the *Configure Security Policies* feature. For instance, in previous versions, enabling or disabling one feature could cause an issue with the other.

The following changes are included in version 11.32:

- The *Password Strength* feature on the *Configure Security Policies* screen only allows you to enable a password strength check at the time of login.
- The *Password Strength Configuration* feature determines the minimum password strength at a variety of checkpoints.
- If *Password Strength* is enabled on the *Configure Security Policies* screen, cPanel & WHM will use the *Default Required Password Strength* setting from the *Password Strength Configuration* feature.

Roundcube requirement matching

As of cPanel & WHM version 11.32, cPanel & WHM will analyze the Roundcube database schema within the account archive (`cpmove`) during account transfers. If necessary, cPanel & WHM will upgrade or downgrade the schema based upon the Roundcube requirements of the destination server.

> **Note:**
> Only MySQL database schemas are addressed by this feature. SQLite database schemas will not be upgraded or downgraded to match the requirements of the destination server.

Exim directives configuration

When `exim.conf` is generated, cPanel & WHM version 11.32 sets the `queue_only_load` and `deliver_queue_load_max` Exim directives dynamically, according to the number of CPUs available. These Exim directives are configured using the following formulas:

- `queue_only_load` = 6 x (The total number of available CPUs on your server)
- `deliver_queue_load_max` = 3 x (The total number of available CPUs on your server)

The total number of available CPUs on your server is equal to the value that is calculated from `/proc/cpuinfo` plus the *Extra CPUs for server load* value that is specified in WHM's *Tweak Settings* interface.

> **Note:**
> An upgrade to cPanel & WHM version 11.32 will reset your Exim directives configuration.

Integrate custom code

In the past, cPanel & WHM has offered several methods for integrating custom code into our software, including:

- function hooks
- script hooks
- custom event handlers

As of cPanel & WHM version 11.32, the Standard Hooks system replaces these individual methods with one overarching system.

This system also adds benefits, such as the capability to provide privilege escalation. It also allows multiple hooks to run for the same event, which was impossible previously without manual intervention.

/var/cpanel/sysinfo.config file updates

We have improved the way `/var/cpanel/sysinfo.config` works within cPanel & WHM version 11.32. This file contains internal code that describes the local operating system, which includes code that manages RPM updates and our update system.

Previously, `/var/cpanel/sysinfo.config` was generated once without further updates. Now, cPanel & WHM updates this file nightly.

> **Note:**
> Instructions on how to override the values in the `/var/cpanel/sysinfo.config` file are available within the file itself.

Cpanel::Config::Flushconfig::flushConfig() functionality

As of cPanel & WHM version 11.32, the module that handles reading and writing of configuration files (`Cpanel::Config::Flushconfig::flushConfig()`) is multi-thread safe. As a result, this module may transform symlinks and hardlinks into regular files.

The following major files are affected:

- `/etc/wwwacct.conf`
- `/etc/wwwacct.conf.shadow`
- `/etc/quota.conf`
- `/etc/cpbackup.conf`
- `/etc/cpbackup.conf.shadow`
- `/var/cpanel/cpanel.config`
- `cpuser` files in `/var/cpanel/users/`

WHM, cPanel, and Webmail interface login screens

We have improved the login screens for WHM, cPanel, and Webmail in cPanel & WHM version 11.32.

The updated login screens allow the user to choose a locale when they log in. This locale setting will apply to the current browser session only. It does not change the cPanel locale preference that is set in *Choose Language*, which remains in effect.

> **Note:**
> If your browser's `Accept-Language` header is set, then the login screen will attempt to display the chosen locale by default. If the locale that is requested by the browser header is not available, the login interface will appear in English, unless you choose a different locale.

Feature list upgrades

In cPanel & WHM 11.32, the *Email Trace* replaces the *Email Delivery Route* feature.

When you upgrade to version 11.32 from version 11.30, WHM will upgrade your cPanel feature lists (which appear in the WHM *Feature Manager* interface) as follows:

- Feature lists with *Email Delivery Route* enabled in cPanel will have the new *Email Trace* feature enabled.
- Feature lists with *Email Delivery Route* disabled in cPanel will have the new *Email Trace* feature disabled.

When you upgrade to version 11.32 from an 11.31 development release, WHM will upgrade your feature lists as follows:

- Feature lists with *Email Delivery Route* enabled in cPanel will have the new *Email Trace* feature enabled.
- Feature lists with *Email Delivery Route* disabled in cPanel will have the new *Email Trace* feature disabled.
- Feature lists with *Email Delivery Reports* enabled in cPanel will have the new *Email Trace* feature enabled.
- Feature lists with *Email Delivery Reports* disabled in cPanel will have the new *Email Trace* feature disabled.

> **Note:**
> *Email Delivery Reports* only appeared in 11.31 development releases of cPanel & WHM.

Default data retention length

To provide data for the new mail delivery reporting system, we have changed the default data retention length in the eximstats database from 16 days to 90 days. (The data retention length is also customizable via the *Tweak Settings* option entitled *The interval, in days, to retain Exim stats in the database.*)

In addition, a command line utility is available so you can import data from archived Exim log files to the `eximstats` database.

Appendix A: Provided third-party applications

cPanel & WHM version 11.32 includes the following third-party applications. This section lists the applications' version numbers and the minor build of cPanel & WHM that corresponds to each version.

Third-party application	Version	Corresponding cPanel & WHM minor version
Exim	4.77-1	11.32.0
MySQL 5.1 [1]	5.1.59-0	11.32.0
MySQL 5.5 [2]	5.5.17-1	11.32.0
NSD	3.2.9-1	11.32.0
Pure-FTPd	1.0.35-1	11.32.0
Pro-FTPd	1.3.4-0	11.32.0
Courier	4.10.0-1	11.32.0
Horde Groupware	1.2.10	11.32.0
phpPgAdmin	5.0.3	11.32.0
phpMyAdmin	3.4.9	11.32.0

[1] Users who run MySQL versions earlier than 5.1 will likely encounter sub-optimal performance for bandwidth calculations and mail delivery reports.
[2] An upgrade to MySQL version 5.5 will block your system from downgrading from cPanel & WHM version 11.32 to version 11.30 in the future.

Removed third-party applications

As of cPanel & WHM version 11.32, Melange Chat System software is no longer available.

Appendix B: New and modified API calls

New XML API calls:

- get_available_tiers — Returns a list of available cPanel & WHM tiers.
- `remove_in_progress_exim_config_edit` — Allows you to remove dry run files after a failed Exim update attempt.
- `exim_configuration_check` — Checks and attempts to repair the Exim configuration.
- `validate_current_installed_exim_config` – Validates the system's current Exim configuration.
- `accesshash` — Retrieves an access hash for the root user. Authenticated resellers who have the *all* ACL may also retrieve an access hash. In addition, you can use this API call to generate or regenerate an access hash.
- `get_password_strength` — Checks the strength of a specified password.
- `get_tweaksetting` — Allows you to retrieve the value of an option in WHM >> *Tweak Settings*.
- `set_tweaksetting` — Allows you to change the value of an option in WHM >> *Tweak Settings*.

New API2 calls:

- `PasswdStrength::get_password_strength` — Checks the strength of a specified password.

Modified XML API calls

- Create Account (`createacct`) — Create a new cPanel account.
- Modify Account (`modifyacct`) — Modify an existing cPanel account.
- List Accounts (`listaccts`) — List cPanel accounts hosted on your system.
- Add Package (`addpkg`) — Add a new cPanel package.
- Edit Package (`editpkg`) — Edit an existing cPanel package.

- List packages (`listpkgs`) — List existing cPanel packages on your system.

Appendix C: New configuration directives

We have added the following configuration directives to cPanel & WHM version 11.32.

Each directive corresponds to an option in WHM >> *Tweak Settings*. The server administrator may also create the `/root/cpanel_profile/cpanel.config` file and set the directive's value within the `cpanel.config` file with the following format:

- `ionice_optimizerefs=5`

Directive in cpanel.config	*Tweak Settings* label	*Tweak Settings* description	Input type (acceptable values)	Default value
`email_send_limits_count_mailman`	Count mailman deliveries towards a domain's Max hourly emails.	If enabled messages sent from a mailing list owned by a user's domain with be counted towards the maximum number of emails the domain is permitted to send per hour.	Boolean (1, 0)	`0`
`email_send_limits_defer_cutoff`	The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery.	When an account exceeds the maximum number of emails it is allowed to send per hour, by default, any additional messages are queued for delivery and sent in the next hour. This setting allows you to limit the number of messages that will be queued by the system. For example, if you set this value to 125%, once the account reaches its hourly limit, Exim will queue any additional messages, up to 125% of the *Max hourly emails per domain* value. Once the account reaches 125% of the *Max hourly emails per domain* value, any additional outgoing messages are discarded.	Integer (100-10,000)	`125`
`email_send_limits_max_defer_fail_percentage`	Maximum percentage of failed or deferred messages a domain may send per hour	The maximum percentage of a domain's outgoing mail that can consist of failed or deferred messages. Once the domain exceeds this percentage, it is temporarily blocked from sending mail	Integer (1-100; 0 is unlimited)	`unlimited`
`exim_retention_days`	The interval, in days, to retain Exim stats in the database	*N/A*	Integer (1-365,000)	`90`
`ionice_optimizefs`	I/O priority level at which optimizefs is run	**optimizefs is a file system optimization utility used by cPanel & WHM**. You must compile ionice with your kernel to use this option. ionice manages I/O scheduling for processes on your system. Specifying a lower value for this option gives the process a higher priority. This option can accept integer values between *0* and *7*.	Integer (0-7)	`6`

`ionice_userproc`	I/O priority level for user-initiated processes	This option applies to a few especially I/O-intensive user functions, such as actions initiated through the cPanel *File Manager*. You must compile ionice with your kernel to use this option. ionice manages I/O scheduling for processes on your system. Specifying a lower value for this option gives the process a higher priority. This option can accept integer values between *0* and *7*.	Integer (0-7)	5
`send_update_log_for_analysis`	Send update analyses to cPanel	This option allows you to select whether to send an analysis file to cPanel when you update your server.	Boolean (1,0)	1
`skiplogaholic`	Enable Logaholic stats	*N/A*	Boolean (1,0)	0
`transfers_timeout`	Number of seconds an SSH connection related to an account transfer may be inactive before timing out	*N/A*	Integer (300-3,600)	300
`update_log_analysis_retention_length`	Update analysis retention interval	This option allows you to specify how long you wish to keep the update analysis files you send cPanel.	Positive integer; 0 disables retention; `undef` retains data indefinitely	90 (days)

Appendix D: New and modified user interfaces

New user interfaces

- *Logaholic* — We added the Logaholic stats program to the *Logs* section of the cPanel interface. This feature also adds an *Enable Logaholic stats* option to the WHM *Tweak Settings* screen. This option is disabled by default.

- *Delivery Reports* — New interfaces appear in the cPanel *Mail* section, the WHM *Email* section, and *Webmail*. These interfaces include:
  - **WHM** — *Mail Delivery Reports*, *View Sent Summary*
  - **cPanel** — *Email Trace*
  - **Webmail** — *Delivery Reports*

Modified user interfaces

The following interfaces changed:

- The login screen for cPanel, WHM, and Webmail

WHM:

- *Mail Queue Manager* — This interface changed with the implementation of the new mail delivery reporting system.
- *View Relayers* — This interface changed with the implementation of the new mail delivery reporting system.
- *Tweak Settings* — New options:
  - *Enable Logaholic stats*
  - *The interval, in days, to retain Exim stats in the database* — Formerly, this interval was set at 16 days, with no option to modify it. The new default interval is 90 days.
  - *I/O priority for user-initiated processes. (ionice must be available and supported by the kernel for this functionality.)* — This option applies to I/O usage by the cPanel *File Manager* interface only. 0 is the highest priority, 7 is the lowest priority.
  - *I/O Priority at which the optimizefs is run. (ionice must be available and supported by the kernel for this functionality.)* — 0 is the highest priority, 7 is the lowest priority
  - *Enable DKIM on domains for newly created accounts*
  - *Enable SPF on domains for newly created accounts*
  - *Prevent cPanel users from creating certain domains* — This option was formerly called *Block Common Domain Usage*.
  - *The percentage of email messages (above the account's hourly maximum) to queue and retry for delivery.*

- *Maximum percentage of failed or deferred messages a domain may send per hour*
- *Count mailman deliveries towards a domain's Max hourly emails*
- *System disk space usage warnings*
- *Account system disk usage "warn" percentage*
- *Account system disk usage "critical" percentage*
- *Tweak Settings* — Existing options that have changed:
  - *Account disk quota "warn" percentage* — Formerly, *Account disk usage "warn" percentage*. This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
    - *Notify admin or reseller when disk quota reaches "warn" state* — Formerly, *Notify admin/reseller at disk usage "warn" state*.
    - *Account disk quota "critical" percentage* — Formerly, *Account disk usage "critical" percentage*. This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
    - *Notify admin or reseller when disk quota reaches "critical" state* — Formerly, *Notify admin/reseller at disk usage "critical" state*.
    - *Account disk quota "full" percentage* — *Account disk usage "full" percentage*. This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
    - *Notify admin or reseller when disk quota reaches "full" state* — Formerly, *Notify admin/reseller at disk usage "full" state*.
    - *Mailbox disk quota "warn" percentage* — This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
    - *Mailbox disk quota "critical" percentage* — This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
    - *Mailbox disk quota "full" percentage* — This option now accepts floating-point numbers with up to 4 significant digits after the decimal as input.
- *Initial Setup Wizard* — We've added options to the *Subscribe to cPanel News* mailing list and *Subscribe to cPanel Releases* mailing list.
  Create a New Account — This interface now allows resellers and root users to add add DKIM and SPF records when creating cPanel accounts. These settings override the server-wide *Tweak Settings* options for DKIM and SPF.
- *Modify an Account* — This interface now allows resellers and root users to add DKIM and SPF records when modifying cPanel accounts. These settings override the server-wide *Tweak Settings* options for DKIM and SPF. This interface also offers a way to enable or disable DKIM and SPF entries for all zones owned by the account.
- *Exim Configuration Manager* — We've converted this to a tab-based interface. We've also added the ability to download backups, restore backups, reset the Exim configuration, as well as enable and disable DKIM checking and signature verification in incoming email.
- *Feature Manager* — *Email Delivery Route* is now deprecated. *Email Trace* is the replacement feature.
- *Scan for Trojan Horses* — This interface has been removed.

cPanel:

- *Email Delivery Route* — We redesigned this interface. It also now allows users to search for a specific email message.
- *Email Authentication* — We've replaced the DomainKeys functionality with DKIM.
- *BoxTrapper* — We've added the following settings to the *BoxTrapper Configuration* interface:
  - *Minimum SpamAssassin Spam Score required to bypass BoxTrapper*
  - *Auto Whitelist To and From lines from whitelisted senders (whitelist by association)*

Appendix E: Script updates

In the `/usr/local/cpanel/scripts` directory

New scripts —

- `nameserverup` — This is the primary script that keeps the nameservers NSD and MyDNS-NG up to date.
- `restartsrv_cphulkd` — This script restarts `cphulkd`.
- `restartsrv_dnsadmin` — This script restarts `dnsadmin`.
- `import_exim_data` — When cPanel & WHM upgrades from version 11.30 to 11.32, it invokes this script, which imports data from the Exim mainlog and archives into the eximstats database.
- `try-later` — Executes a user-defined `check` command at a specified interval. If the `check` command returns an error, it will be retried later. When the check succeeds, a user-defined `action` command runs. For detailed information on this script's options, visit our Scripts ? document.
- `upcp-running` — Specifies whether a `upcp` command is running. This information displays in text output and the script's exit value.
- `chkmydns` — Performs a simple configuration check of MyDNS.
- `exportmydnsdb` — Exports zones from MyDNS for use with BIND and NSD.
- `fixmailinglistperms` — Repairs permissions for all mailing list files and directories.
- `gather-update-logs` — Sends update logs to cPanel for analysis.
- `hook` — Executes any hooks that would be called normally in the specified context.
- `importmydnsdb` — Imports zone information from BIND and NSD into MyDNS.
- `mydnsup` — Installs and updates MyDNS packages.
- `restartsrv_mydns` — Restarts script from MyDNS.
- `slurp_exim_mainlog` — Imports exim mainlog data into the eximstats database.
- `update_php_timezonedb` — Updates the timezone DB used by PHP.
- `xfer_horde_sid_resolver.pl` — Resolves key collision errors before importing Horde data during an account transfer.
- The following new scripts are not intended for command line use:
  - `check_xml_libxml_error`

- `patch_xml_libxml_error`
- `xfer_rcube_uid_resolver`
- `xfer_rcube_schema_migrate`

Deprecated scripts —

- `nsdup` — This script is replaced by `nameserverup`.
- `update_email_limits` — While this script still functions, it only serves as a wrapper for `updateuserdomains`. It will be removed in the future.

Nonexistent scripts —

- `downgrade_cpanel` — Instead of using this script, system administrators can downgrade using the WHM *Update Preferences* interface.

Modified scripts —

- We made the following changes to the `phpextensionmgr` script:
    - This script allows you to upload a custom tarball that contains your custom PHP extensions.
        - Upload the custom tarball using the following command: `/usr/local/cpanel/scripts/phpextensionmgr --local-tarball $pathtotarball`
    - You can enable the `xcache` PHP extension using the `phpextensionmgr` script, as well as the WHM *EasyApache* interface.

In the /usr/local/cpanel/bin directory

New scripts —

- `build_mydns_conf` — Creates a database, database user, configuration file, and the necessary tables for a fresh installation of MyDNS-NG.
- `cpconftool` — Backs up and restores the Exim configuration file and `cpanel.config`.
- `eximstats_server_test` — Provides a simple summary of email stats for each cPanel account. Useful for testing.
- `fetch_cpconf_value` — Retrieves values from `cpanel.config`. Primarily useful in scripts and applications.
- `force_maildir` — Sets `maildir=1` in `cpanel.conf`. This script is called by `upcp`.
- `mailman-tool` — Enables or disables Mailman at the system level.
- `manage-hooks` — Adds, removes, and lists hooks on your system.
- `migrate_all_feature_lists_to_current` — Updates existing feature lists for compatibility with the installed version of cPanel & WHM.
- `update-logaholic` — Updates the Logaholic installation.
- The following new scripts are not intended for command line use:
    - `emailtrack`
    - `eximstats_server`
    - `eximstatsadmin`
    - `featureadmin`
    - `hooks2admin`
    - `logaholicadmin`

Appendix F: Translatable user interface text strings

The attached files below are designed to interact with an outside translation service. As such, user interface text strings will remain in those files until fully translated. The included strings derive from cPanel & WHM version 11.32 and earlier.

- new.yaml
- pending.yaml

Appendix G: Translatable user interface text strings

`atd` used for upcp log analysis

cPanel & WHM version 11.32 now installs the at daemon (`atd`) as part of the update process. We use `atd` for launching the update-analysis process to validate the health of the system after updates.

Update-analysis information is stored in the directory `/usr/local/cpanel/logs/update_analysis/`. There are two new Tweak Settings that will let you choose to send update analyses to cPanel and set the retention interval of the logs.

Finally, because `atd` is necessary to run the analysis of the upcp log, the Quick Security Scan no longer disables `atd`.