11.46 Release Notes

For cPanel & WHM 11.46

This page was last updated on: ⊞ Nov 29, 2017 15:06

Upgrade blockers

Microsoft® FrontPage® extensions

> **Warning:**
> - **Before you upgrade, make certain that you no longer wish to use FrontPage on your server**. After you upgrade to cPanel & WHM version 11.46, you **cannot** restore the cPanel-provided FrontPage functionality on your server.
> - We **strongly** recommend that you rebuild EasyApache without FrontPage **before you attempt to upgrade**.

You **must** remove the Microsoft FrontPage RPM from your server before you upgrade to cPanel & WHM version 11.46.

- On servers that run cPanel & WHM version 11.44, remove the FrontPage RPM from your server in WHM's *Uninstall FrontPage Extensions* interface (*Home* >> *FrontPage* >> *Uninstall FrontPage Extensions*).
- On servers that run cPanel & WHM version 11.44.2.3 and higher, the system automatically removed unused FrontPage installations during the upgrade to version 11.44.2.3.

> **Note:**
> The FrontPage RPM and the FrontPage opt mod (`mod_frontpage`) in EasyApache are separate entities. The presence of `mod_frontpage` will **not** block upgrades to cPanel & WHM version 11.46.

Additional swap space requirements

In cPanel & WHM version 11.46 and later, fresh installations and upgrades require **at least** 3 GB of available disk space for staging purposes.

PHP version 5.3 RPM installed

If the `cpanel-php53` RPM target is set to `installed` on your server, you **cannot** upgrade to cPanel & WHM version 11.46.

To uninstall the `cpanel-php53` RPM target, run the following commands:

```
/scripts/update_local_rpm_versions --del target_settings.cpanel-php53
/scripts/check_cpanel_rpms --fix
```

Staging Directory

Version 11.46.3.3 introduces the Staging Directory. The system notifies you if there is insufficient space available to complete the upgrade and allows you to select a new location for the Staging Directory.

New features

Single Sign On for default email account

In cPanel & WHM version 11.46, if you use the cPanel interface to log in to Webmail, you will automatically log in to the email account. However, if you go directly to the URL of the Webmail interface, you must use the email account's username and password.

ModSecurity™ Tools and Configuration

In cPanel & WHM version 11.46, we have added interfaces that allow users to manage ModSecurity rules and configurations.

WHM now includes the following interfaces:

- The *ModSecurity™ Tools* interface (*Home >> Security Center >> ModSecurity™ Tools*) allows you to install and manage ModSecurity rules.
- The *ModSecurity™ Configuration* interface (*Home >> Security Center >> ModSecurity™ Configuration*) allows you to configure ModSecurity settings.

cPanel now includes the *ModSecurity Domain Manager* interface (*Home >> Security >> ModSecurity™ Domain Manager*), which allows you to disable ModSecurity for one or more domains.

MySQL backups include triggers and events

In cPanel & WHM version 11.46, MySQL backups now include triggers and events.

New Tweak Settings options

> **Warning:**
> **We strongly recommend that you do not disable the *Maintenance cPanel RPM Check* and *Maintenance cPanel RPM Digest Check* settings**. If you disable these settings, the system will **not** check existing RPMs for problems during updates **or** maintenance. This could leave your system vulnerable to unnoticed tampering or other risks.

WHM's *Tweak Settings* interface (*Home >> Server Configuration >> Tweak Settings*) now includes two new settings in its *Software* section.

- *Maintenance cPanel RPM Check* — This option allows you to enable or disable the cPanel RPM check, which runs the `/scripts/check_cpanel_rpms` script, during your system's nightly maintenance.
- *Maintenance cPanel RPM Digest Check*— This option allows you to enable or disable digest authentication for the cPanel RPM check during your system's nightly maintenance. If you disable this setting, nightly maintenance runs the `/scripts/check_cpanel_rpms` script with the `--no-digest` option.

> **Note:**
> Both of these options default to *On.* You can also modify these settings via the `maintenance_rpm_version_check` and `maintenance_rpm_version_digest_check` values in the `/var/cpanel/cpanel.config` file.
>
> - For more information about the `/scripts/check_cpanel_rpms` script, read our The /scripts/check_cpanel_rpms Script documentation.
> - For more information about the `/var/cpanel/cpanel.config` file, read our The cpanel.config File documentation.

WHM's *Tweak Settings* interface (*Home >> Server Configuration >> Tweak Settings*) now includes one new setting in its *Stats and Logs* section.

- *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.

UI Includes system

cPanel & WHM version 11.46 introduces the use of UI Includes in Paper Lantern. Resellers and administrators can use Template Toolkit to insert custom content in the cPanel interface.

- The `root` user can insert global header and footer content across all of the interfaces in cPanel.
- Resellers can insert content across targeted interfaces to display custom headers and footers.

For more information, read our Customize Content in Paper Lantern documentation.

Mass edit for TTL added

You can now edit the TTL for all of the zones that your account owns. To do this, use WHM's *Set Zone Time to Live (TTL)* interface *(Home >> DNS Functions >> Set Zone Time to Live (TTL))* and the `/scripts/set_zone_ttl` script.

System improvements

Paper Lantern

In cPanel & WHM version 11.46, users can now customize their cPanel dashboards. Resellers and `root` users can choose to either develop a style or use WHM's *Customize Paper Lantern* interface (*Home >> cPanel >> Customize Paper Lantern*) to create new styles and share them with their customers.

For more information, read our Paper Lantern 11.46 Release Notes.

Improved upgrade logic

We have improved the upgrade process to ensure that upgrades finish on the latest version of cPanel & WHM possible, even if the upgrade encounters blockers for the next major version of cPanel & WHM.

For example, if you begin an upgrade from cPanel & WHM version 11.40 to version 11.46, but Microsoft® Frontpage® is installed on the server, the server will upgrade to the latest release of version 11.44.

For more information about the upgrade process, read our Upgrade Blockers documentation.

Binary improvements

`cpsrvd` now supports SSL. For this reason, we no longer ship `cpsrvd-ssl` as a separate entity.

Changes to the x3 theme's dynamicui.conf file

We have updated cPanel's `dynamicui.conf` file. If you use a custom x3 style, you may need to refork the x3 theme after you upgrade. If you do not refork the x3 theme for your custom branding, you may see nonfunctional features in the cPanel *Home* interface.

Apache SpamAssassin upgrade

We upgraded the cPanel-provided installation of Apache SpamAssassin™ to Apache SpamAssassin version 3.4.

> **Note:**
> For more information, read the Apache SpamAssassin 3.4 release notes.

Updated re2c RPM

We have updated the re2c RPM to version 0.13.7.4. cPanel & WHM uses re2c to compile the Apache SpamAssassin™ ruleset. For more information, visit the re2c website.

Unprivileged and unmanaged database and database username renames

In cPanel & WHM version 11.46, if you create an account that matches an unprivileged and unmanaged database user name, the system will rename the database user name so that the system can create the account.

> **Notes:**
> * An unmanaged database object is one that is not owned by a cPanel user account.
> * An unprivileged database user is one that does not have privileges on any databases, no database object depends on it, and does not have any triggers for events.

Updated Perl environments and modules

We now compile cPanel binaries against Perl 5.14.4, instead of Perl 5.6.2. We have also updated all cPanel-included CPAN modules to the newest available version as of July 2014.

> **Important:**
> If you use custom Perl modules or Perl scripts on your server, or if you are a third-party developer, it is **critical** that you test your plugins and hook code against Perl 5.14.4 to be certain that it functions correctly. **Modules that were built and used against Perl**

> **5.6.2 will not work with the new cPanel & WHM version 11.46 binaries.**

Custom modules that you previously compiled with the `buildperl` system will **not** function properly in cPanel & WHM version 11.46 and later, because the module was built against an older version of Perl.

Before you recompile all of your modules, check whether cPanel & WHM already includes your modules. We have added many modules to the list of modules that cPanel ships, and expect that cPanel & WHM will now ship with the majority of the modules that developers built with this tool.

- **cPanel wants to make certain that we ship the modules that you need**. If you discover that cPanel & WHM does **not** ship with a CPAN module that you need, send an email to integration@cpanel.net to request it. While it is possible to install custom modules to the `/opt/cpanel/perl5/514/site_lib` library with the `/usr/local/cpanel/3rdparty/perl/514/bin/cpan` command, this will cause further problems when cPanel switches to even newer versions of Perl.

For more information about the available Perl environments, read our Guide to Perl in cPanel & WHM documentation.

Check for custom modules

To test whether the module that you need already ships with cPanel & WHM, run the following command, where `My::Module` represents your module's name:

```
/usr/local/cpanel/3rdparty/bin/perl -MMy::Module -E'say
$My::Module::VERSION'
```

For example, `LWP` is a common module that was previously compiled against the `buildperl` system. cPanel & WHM ships with `LWP` version 6.05 with Perl 5.14, as shown by the following command and its output:

```
/usr/local/cpanel/3rdparty/bin/perl -MLWP -E'say $LWP::VERSION'
6.05
```

Removed buildperl binary

Due to the updates to cPanel & WHM's Perl binary, we have removed the `/usr/local/cpanel/build-tools/buildperl` binary.

> **Notes:**
> - To install a Perl module to cPanel & WHM's internal Perl binary, use the `/usr/local/cpanel/3rdparty/perl/514/bin/cpan` tool.
> - For more information, read our Guide to Perl in cPanel & WHM documentation.

Updated Security Advisor warnings

WHM's *Security Advisor* interface (*Home >> Security Center >> Security Advisor*) now reports an issue if the following custom modules exist on your server:

- `mod_frontpage`
- `mod_auth_passthrough`

> **Important:**
> If these modules are present on your server, we **strongly** recommend that you rebuild EasyApache **without** FrontPage to remove the modules. cPanel & WHM version 11.46 and later do **not** support Microsoft® FrontPage®.

Streaming transfers use rsync

In cPanel & WHM version 11.46, streaming account transfers now use `rsync` if both the source and target servers have `rsync` installed.

New styling for WHM News

The WHM *News* section now uses bootstrap styling, and we have improved it to behave more consistently.

- We have introduced a primary news area that displays the three most recent news items.
- The *Continue Reading* link now displays consistently, regardless of the news item's origin.

Notifications for the cpanel.config file

In cPanel & WHM version 11.46 and later, we have reduced the number of `cpanel.config` file validation notifications:

- System administrators will only receive email notifications about the `/var/cpanel/cpanel.config` file if the system could not find the `/var/cpanel/cpanel.config` file.
- If individual `cpanel.config` values are missing or invalid, the system will update the file and log the changes to the `/usr/local/cpanel/logs/error_log` file.

For more information about `cpanel.config` file validation, read our The cpanel.config File documentation.

Deprecated `killacct` script, new `removeacct` CLI script

When you delete an account through the command line interface, we no longer recommend that you use the `killacct` script. The default behavior of this script did not remove DNS entries for an account. Instead, we recommend that you use the `/scripts/removeacct` script, which, by default, removes an account and its DNS entries.

Added record types for the Advanced DNS Zone Editor

cPanel's *Advanced DNS Zone Editor* interface (*Home* >> *Domains* >> *Advanced DNS Zone Editor*) now supports AAAA and SRV record types.

Localization of x3 for 29 languages

You can now use the cPanel interface's x3 theme in 29 different locales. You can choose from the following locales:

- Arabic
- Chinese
- Czech
- Danish
- Dutch
- English
- Filipino
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Iberian Spanish
- Indonesian
- Italian
- Japanese
- Korean
- Latin American Spanish
- Malay
- Norwegian
- Polish
- Portuguese
- Romanian
- Spanish
- Swedish
- Thai
- Traditional Chinese
- Turkish
- Ukrainian
- Vietnamese

To change your interface to these locales, select them from the login interface or the *Change Language* page (*Home* >> *Preferences* >> *Change Language)* of x3. x3 will automatically default to your browser language setting.

Dovecot and Courier IPv6 capabilities

Dovecot and Courier can now listen to IPv6 requests for POP3 and IMAP. This includes POP3SSL and IMAPSSL.

This is configurable in the *Mailserver Configuration* .

Package name display behavior

cPanel & WHM considers the underscore character (_) to be a separator between the reseller that owns the package and the package's name. The system considers characters to the left of the underscore to be the reseller's name, and characters to the right of the underscore to be the package's name.

As of cPanel & WHM version 11.46, the cPanel interface only displays the package's name. For example, the interface will display the `reseller_package` package as `package`.

For more information, read our *Add a Package.*

Removed items

Interchange

We deprecated Interchange in cPanel & WHM version 11.38. In cPanel & WHM version 11.46, we have removed all references to it from the cPanel & WHM codebase.

This includes the removal of the following items:

- The `/usr/local/cpanel/3rdparty/interchange/interchange.cfg` file.
- The `/scripts/restartsrv_interchange` script.
- The *Reset Shopping Cart* (`res-cart`) feature limit.
- The `interchangever` setting in the `/etc/cpanel.config` file.

Removed ModSecurity Plugin interface

We have removed the *ModSecurity Plugin* interface.

The *ModSecurity Tools* interface (*Home >> Security Center >> ModSecurity™ Tools*) and *ModSecurity Configuration* interface (*Home >> Security Center >> ModSecurity™ Configuration*) replace this plugin.

Deprecation of LANG system

cPanel & WHM version 11.46 deprecates the old style LANG system.

Examine your systems for use of the deprecated lookup keys. Sometimes these keys are called short tags. The following are examples of these deprecated keys:

- `ChangePassword`
- `email_page_description_singular`

A full list of deprecated lookup keys can be found in `/usr/local/cpanel/lang` and `/usr/local/cpanel/base/frontend/x3/lang`.

If you used the LANG system to provide your own custom translations, the x3 and Paper Lantern themes will no longer use them. Your users will only see English text. To allow them to function, you will need to convert your translations to the Locale Maketext format. To translate phrases, use WHM's *Edit a Locale* interface *(Home >> Locales >> Edit a Locale)* .

If you have implemented deprecated lookup keys in one of the following ways, the correct text will continue to display:

- Customizations of x3 or Paper Lantern
- Custom applications that use deprecated lookup keys
- Third-party themes that use deprecated lookup keys

Removed variables

We have removed the following variables from the `/var/cpanel/cpanel.config` file:

- `interchangever`
- `maildir`

- `popchecktimes`
- `popcheckflood`

> **Note:**
> - Maildir is the **only** mail storage format that cPanel & WHM supports.
> - API calls that previously returned the `maildir` parameter will continue to do so.

> **Important:**
> Be **certain** that you update any third-party code that may use these variables.

Deprecated scripts

The following scripts are now deprecated:

- `/usr/local/cpanel/bin/force_maildir`
- `/usr/local/cpanel/bin/hasmaildir`

> **Important:**
> Be **certain** that you have updated any cron jobs or other dependencies that may have used these scripts.

Removed scripts

We have removed the following scripts:

- `/usr/local/cpanel/bin/installimap`
- `/usr/local/cpanel/etc/cppop/authresettime`
- `/usr/local/cpanel/etc/init/scripts/centos/cppop`
- `/usr/local/cpanel/etc/init/scripts/rhel/cppop`
- `/usr/local/cpanel/etc/init/startcppop`
- `/usr/local/cpanel/etc/init/stopcppop`
- `/usr/local/cpanel/scripts/restartsrv_cppop`
- `/usr/local/cpanel/scripts/restartsrv_interchange`
- `/usr/local/cpanel/scripts/chownpublichtmls`

> **Note:**
> Prior to cPanel & WHM version 11.42.1.16, the `/scripts/chownpublichtmls` script could change file and directory ownership within the target user's `public_html` directory if it was run with `root` permissions. In cPanel & WHM version 11.42.1.16 and later, we modified the script to perform ownership changes with the effective UID and GID of the target user. This change addresses a security vulnerability in the script, but also limits the script's usefulness.

> **Important:**
> Be **certain** to update any cron jobs or other dependencies that may have used these scripts.

Appendix A: Provided third-party applications

cPanel & WHM version 11.46 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	4.84.1	11.45.0
MySQL 5.5	5.5.39-1	11.45.0
NSD	3.2.17-1	11.45.0
MyDNS	1.2.8.31-7	11.45.0
Pure-FTPd	1.0.36-10	11.45.0

Pro-FTPd	1.3.5-1	11.45.0
Courier	4.15-1	11.45.0
Dovecot	2.2.13-1	11.45.0
Horde Groupware	5.1.4-1	11.45.0
Roundcube	0.9.5	11.45.0
SquirrelMail	r14346	11.45.0
phpPgAdmin	5.1	11.45.0
phpMyAdmin	4.1.8	11.45.0

Appendix B: New and modified API calls

New UAPI Calls

- `Brand::read` — This function returns the information configured in WHM's *Customize Paper Lantern* interface (*Home >> cPanel >> Customize Paper Lantern*).
- `Styles::list` — This function lists information about all of the styles that are available to the reseller account.
- `Styles::set_default` — This function allows you to set a default style for your customers.
- `Styles::update` — This function applies a new style to the cPanel interface.

New WHM API Calls

- `abort_transfer_session` — This function allows you to abort an active transfer session.
- `load_style` — This function retrieves information about your custom style.
- `modsec_add_rule` — This function adds a new ModSecurity rule to the specified ModSecurity configuration-staging file.
- `modsec_batch_settings` — This function processes a set of global ModSecurity configuration directives.
- `modsec_deploy_rule_changes` — This function takes the staged changes for the ModSecurity configuration file, deploys them to the live configuration file, and restarts Apache.
- `modsec_deploy_settings_changes` — This function deploys the staged changes to the /usr/local/apache/conf/modsec2.conf file and attempts to restart Apache.
- `modsec_disable_rule` — This function disables a single ModSecurity rule for a specified rule ID in a specified ModSecurity configuration file.
- `modsec_discard_rule_changes` — This function discards the staged rule changes, if present, for the specified configuration file.
- `modsec_edit_rule` — This function allows you to edit an existing rule in a ModSecurity configuration file.
- `modsec_get_config_text` — This function retrieves the contents of a ModSecurity configuration file.
- `modsec_get_configs` — This function retrieves the list of known ModSecurity configuration files which are eligible for this API to manage.
- `modsec_get_configs_with_changes_pending` — This function searches for ModSecurity configuration files that contain staged pending changes and returns a list of those files.
- `modsec_get_log` — This function retrieves ModSecurity log events from the modsec MySQL database.
- `modsec_get_rules` — This function retrieves the ModSecurity rules from a single ModSecurity configuration file.
- `modsec_get_settings` — This function retrieves the ModSecurity settings stored in the /usr/local/apache/conf/modsec2.conf file.
- `modsec_is_installed` — This function verifies whether the ModSecurity Apache module is installed.
- `modsec_make_config_active` — This function adds an include for a ModSecurity configuration file in the modsec2.cpanel.conf file.
- `modsec_make_config_inactive` — This function removes an include for a ModSecurity configuration file in the modsec2.cpanel.conf file.
- `modsec_remove_rule` — This function removes a ModSecurity rule from the specified ModSecurity configuration file.
- `modsec_remove_setting` — This function allows you to remove a single global ModSecurity configuration directive.
- `modsec_set_config_text` — This function allows you to set the contents of a specified ModSecurity configuration file.
- `modsec_set_setting` — This function sets the value of a single global ModSecurity configuration directive.
- `modsec_undisable_rule` — This function enables a single ModSecurity rule with a specified rule ID in a specified ModSecurity configuration file.
- `save_style` — This function allows you to save an uploaded style and retrieve it later.

Modified WHM API Calls

- `create_user_session` — This function now accepts the `webmaild` value for the `session` parameter.
- `listacls` — This function no longer returns the `res-cart` parameter.
- `myprivs` — This function no longer accepts the `acl-res-cart` parameter.
- `saveacllist` — This function no longer accepts the `acl-res-cart` parameter.

- `setacls` — This function no longer accepts the `acl-res-cart` parameter.

Modified cPanel API Calls

- `Frontpage::fpstatus` — This function will now only return the `'not installed'` value.
- `Frontpage::delfp` — This function will now only return a `Microsoft® FrontPage® is not available on servers that run cPanel & WHM version 11.46 and later.` message.
- `Frontpage::addfp` — This function will now only return a `Microsoft® FrontPage® is not available on servers that run cPanel & WHM version 11.46 and later.` message.