11.38 Release Notes

Upgrade Blockers

An upgrade to 11.38 will be blocked if Interchange is enabled. As of cPanel & WHM 11.38, Interchange will no longer be included in an installation.

cPanel & WHM version 11.38.1

Tweak Settings for AppConfig

The *Security* section of *Tweak Settings* includes four new features:

- *Allow WHM apps registered with AppConfig to be executed even if a Required ACL list has not been defined*
  - This setting allows applications and addons that are registered with AppConfig to execute even if a Required ACL has not been defined.
    If you disable this setting, applications and addons that are registered with AppConfig will be forced to set an ACL list before they can be executed.

- *Allow cPanel and Webmail apps registered with AppConfig to be executed even if a Required Features list has not been defined*
  - This setting allows cPanel and Webmail apps that are registered with AppConfig to execute even if a required features list has not been defined.
    If you disable this setting, cPanel and Webmail apps that are registered with AppConfig will be forced to set a Required Features list before they can be executed.

- *Allow apps that have not registered with AppConfig to be run when logged in as a reseller in WHM*
  - This setting allows applications that are not registered with AppConfig to be run when logged in as a reseller in WHM.
    If you disable this setting, resellers will be unable to run applications that are not registered with AppConfig.

- *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 applications that are not registered with AppConfig to be run when logged in as `root` or a reseller in WHM with the **all** ACL enabled.
    If you disable this setting, `root` and reseller accounts with root privileges can only run applications that are registered with AppConfig.

More information about these settings is available.

Advanced Settings for the Backup Configuration

The *Backup Configuration* feature in WHM has a new section. Under the *Advanced Settings* section, you can control how long a backup will attempt to run before it times out.

Reusable Active Security Tokens

You may now reuse an active security token for additional `Cpanel::LogMeIn` requests. This ensures that the new login URL shares the same security token.

New Features

Improved Backup System

In 11.38, WHM offers a new interface to create backups. This new interface has several features that give system administrators the opportunity to customize the backup configuration.

Legacy Backup

In 11.38, WHM features an updated interface for the *Backup Configuration* screen in WHM's *Backup* section. System administrators who may not feel comfortable with this update can still use the 11.36 version of *Backup Configuration*, formerly called *Configure Backups* now called *Legacy Backup Configuration*.

User Backup Selection

We added a new feature called 11.38 Release Notes under the *Backup* section in WHM. This feature allows system administrators to backup each account with the *Legacy Backup Configuration*, the new *Backup Configuration*, or both. For example, a system administrator can configure `user1` to use the *Legacy Backup Configuration* while `user2` is configured to use the new *Backup Configuration*.

> The new *Backup Restoration* feature will not restore backups saved with the *Legacy Backup Configuration*.

For more information, read our documentation about the user backup selection.

Timing Settings

The *Backup Configuration* feature allows system administrators to choose when to run a backup. A system administrator may choose one or more days of the week, or once or twice a month. After a system administrator decides when to run backups, he can choose how many backups to keep.

For more information, read our documentation about the timing settings.

Files, and Databases

The new *Backup Configuration* feature allows a system administrator to choose to backup access logs, bandwidth data, system files, and databases. A system administrator may also choose whether or not to assign the accounts a local DNS during the backup.

For more information, read our documentation about the account settings.

Configure Backup Directory

After a system administrator chooses when to run backups and what content to back up, he can decide where to save the backups. The *Configure Backup Directory* feature allows the system administrator to choose the path for backups.

For more information, read our documentation about backup directory configuration.

Additional Destinations

A key aspect of the *Backup Configuration* feature is the ability to save backups to one or more additional destinations such as FTP, Additional Local Directory, SFTP, or WebDAV. In addition to these pre-configured destinations, a system administrator may also choose to create a custom destination.

For more information, read our documentation about additional destinations.

Backup Restoration

WHM 11.38 has a new *Backup Restoration* feature that allows system administrators to choose to restore backups by account or by date.

Restore by Account

The *Backup Restoration* feature allows a system administrator to choose individual accounts to restore. After the system administrator selects an account, he may choose which backup date to restore, and then which *Additional Options* to restore.

For more information, read our documentation about how to restore by account.

Restore by Date

The *Backup Restoration* feature allows a system administrator to choose a date to restore, and then which accounts with backups on that date to restore. After you select an account, you may choose which *Additional Options* to restore.

For more information, read our documentation about how to restore by date.

Restoration Queue

The *Restoration Queue* feature allows a system administrator to see which accounts are queued to be restored. From this queue, a system administrator can also see the status of each restoration, or remove any queued accounts.

For more information, read our documentation about the restoration queue.

Improved SSL Management System

In 11.38, the SSL Management System has been updated.

These updates include:

- SNI support: You can now host multiple SSL Certificates, for different domains, on the same IP address.
- Server owners and users can now determine the primary virtualhost for an IP address
- Improved Wildcard and UCC/SAN certificate support, which allows users to use the same certificate for multiple subdomains.
- UCC/SAN certificates allow for simplified certificate sharing across multiple domains.
- Updated interfaces that provide more guidance through the various workflows of managing certificates and their assets.
- Certificate data is UTF8 safe, which allows for native language support in certificates and their assets.
- OSCP stapling support is available on systems using Apache 2.4.

Determine the primary virtual host

In 11.38, system administrators can explicitly set an IP address's primary SSL and non-SSL virtual hosts through the following calls:

- `set_primary_servername`
    - System administrators can call `set_primary_servername` through Remote API version 1 in the HTTPD module.
    - This call allows WHM users to set the primary domain on an IP address and port type for their accounts' sites.
- `set_primary_ssl`
    - System administrators can call `set_primary_ssl` through UAPI in the SSL module.
    - This function sets a new primary SSL website for a dedicated IP address.

The primary virtual host serves 2 purposes:

- If an HTTP request comes to an IP address that hosts several virtual hosts, Apache will serve the primary virtual host, either SSL or non-SSL, based on the request.
- If the server supports SNI, receives an SSL request on an IP address that hosts multiple SSL virtual hosts, and the client does not support SNI, Apache will serve the primary virtual host's SSL certificate.

> The `/var/cpanel/conf/apache/primary_virtual_hosts.conf` file stores the server name of the primary SSL and non-SSL virtual host on each IP address found in Apache's configuration file. When cPanel rebuilds Apache's configuration file, cPanel uses the data from the `primary_virtual_hosts.conf` file to arrange an IP address's virtual host with the indicated host first.
>
> > This file's internal format is subject to change. We highly recommend that third-party integrators use the API calls to configure data rather than alter the file directly.

Broken SSL Pages in cPanel

In 11.38, we changed the SSL support system in the cPanel and WHM interfaces. It is important to note that any *x3*-cloned themes from 11.34 or 11.36 will **not** work in the updated SSL sections in the 11.38 version of cPanel.

To resolve this issue, system administrators should follow the steps below. System administrators should replace the `$your_theme_backup` text with the name of their *x3* theme.

1. Create a backup of your custom theme:
    - `cp -afv /usr/local/cpanel/base/frontend/$your_theme /usr/local/cpanel/base/frontend/$your_theme_backup`
2. Synchronize the new 11.38 SSL-related files into the theme's directory:
    - `rsync -av /usr/local/cpanel/base/frontend/x3/ssl/ /usr/local/cpanel/base/frontend/$your_theme/ssl/`
    - `rsync -av /usr/local/cpanel/base/frontend/x3/js2/ssl/ /usr/local/cpanel/base/frontend/$your_theme/js2/ssl/`
    - `rsync -av /usr/local/cpanel/base/frontend/x3/css2/ssl/ /usr/local/cpanel/base/frontend/$your_theme/css2/ssl/`
    - `rsync -av /usr/local/cpanel/base/frontend/x3/js2-min/ssl/ /usr/local/cpanel/base/frontend/$your_theme/js2-min/ssl/`
    - `rsync -av /usr/local/cpanel/base/frontend/x3/css2-min/ssl/ /usr/local/cpanel/base/frontend/$your_theme/css2-min/ssl/`

System Improvements

General Improvements

- `Chkservd` now monitors `crond`.
- The *IP Migration Wizard* is now faster on systems with a large number of users or domains.
- The performance of `pkgacct` has been improved by changing how the home directory is stored within the archive.

Autodiscovery

- An alternate host can be configured for use with Autodiscovery.
- You can now configure POP3 as the default mail delivery protocol.

Improved transfer speeds

Backups and account transfer speeds can be improved by using the newly supported, pigz utility.

Update to Mail settings in Exim Configuration Manager

The *EXPERIMENTAL: Rewrite From: header to match actual sender* option is located in the *Mail* section of the *Exim Configuration Manager* (*Home >> Service Configuration >> Exim Configuration Manager >> Basic Editor >> Mail*).

This option rewrites the *From* header in emails to show the original identity of the actual sender for messages sent from your server. Email recipients can see the original *From* header as *X-From-Rewrite* along with the rewritten *From* header. This option is useful to determine the actual mail sender.

New cPanel & WHM installs will feature MySQL 5.5

Beginning with version 11.38, MySQL 5.5 is installed during a fresh install of cPanel & WHM.

Updates to Jailed Shells and Tweak Settings

In 11.38, in a jailshell, all filesystems are mounted with the `nosuid` option by default. The `nosuid` option blocks the operation of `setuid` and `setgid` commands, such as `crontab` and `ping`. This does not apply to the `/usr/sbin/`directory for Exim.

- By default, jailed shell users cannot run the `setuid` and `setgid` commands. Again, this does not apply to the `/usr/sbin` directory for Exim. Additional settings allow jailed shell users to run the `setuid` and `setgid` commands in `/bin` and =/usr/bin=

    > All of an account's background processes are terminated when a jailshell exists for that user.

In the *System* tabs in the *Tweak Settings* feature, system administrators can enable or disable new options for their jailed shells.

These new options are:

- *Jailed /proc mount method*

- *Jailed /bin mounted suid*

- *Jailed /usr/bin mounted suid*

More information about these options is available in our documentation.

Remove bind mounts for a particular user

In 11.38, system administrators can remove all bind mounts for a particular user with the command below. In the following command, replace USER with the desired user:

```
/usr/local/cpanel/3rdparty/bin/perl -MCpanel::Filesys::Virtfs -e
'Cpanel::Filesys::Virtfs::clean_user_virtfs("USER");'
```

Jail Apache Virtual Hosts Via mod_ruid2 and cPanel Jailshell

In 11.38, the *Tweak Settings* section in WHM includes a new option. Under the *Security* tab, users can enable the ***EXPERIMENTAL: Jail Apache Virtual Hosts using mod_ruid2 and cPanel(®) jailshell* option.

When you enable this setting, the `mod_ruid2` module chroots Apache virtual hosts. (This action will run Apache virtual hosts in a jailed environment.)

This item defaults to *Off*.

More information regarding this option is available.

Processes created by mail filters or forward files

When a user's shell is configured to `jailshell` or `noshell`, Exim will now run any process created from alias or filter files inside of VirtFS.

More information regarding VirtFS in 11.38 is available.

TailWatch Updates

In 11.38, the *Service Manager* section in WHM includes the new TailWatch driver called *JailManager*. This TailWatch driver manages jails used for the EXPERIMENTAL: Jail Apache Virtual Hosts using mod_ruid2 and cPanel® jailshell? option. This TailWatch driver keeps each user's jail updated with the `root` filesystem.

Additionally, *Chkservd* now monitors the `crond` daemon and knows about non-standard SSH and FTP ports.

More information regarding these additions is available on our SDK website and in our Service Manager documentation.

Integration Focused Improvements

- Serialization within the AdminBin system is now encapsulated within the Cpanel::AdminBin::Serializer.
- Cpanel::JSON now uses JSON::XS. This improves system performance anywhere that JSON is used (e.g. the remote json-api).
- The AdminBin system now allows for third party namespaces.
- The AdminBin system now has a pluggable architecture, simplifying its use by third parties.
- The UAPI is now accessible through the LiveAPI system.

Apache Improvements

- Apache Include entries are now added to VirtualHosts at the time of domain creation and `httpd.conf` does not have to be regenerated for the entries to appear.
- Proxy Subdomain records are now kept in sync with IP address changes as they happen.
- The speed in which the Apache Configuration file is generated, has been improved significantly.

Apache Template Update

In 11.38, addon domains, subdomains, and newly created accounts now use the same template system. The Apache template system allows your customizations to remain in place after you rebuild the Apache configuration file. As a result, we have removed the legacy `/httptemplates/` system. An Apache configuration file rebuild will override the `/httptemplates/` system.

More information regarding custom templates is available in the EasyApache: Changes Contained Within a VirtualHost Directive document.

Updates to Tweak Settings

The *Domain* section of *Tweak Settings* includes two new features:

- ** *Preferred mail service to configure to use for Thunderbird and Outlook autodiscover and autoconfig support*
  - System administrators can choose the email transfer method to use with Thunderbird and Outlook with AutoDiscover and AutoConfig support. System administrators can choose *imap* or *pop3*.

- ** *Host to publish in the SRV records for Outlook autodiscover support.*
  - System administrators can choose the host that is published in the SRV records. System administrators can change the default host if they have an SSL-enabled host with an SSL certificate signed by a Certificate Authority.

More information about these options is available.

Removed Items

Optional Security Tokens

Security tokens are always on and are no longer allowed to be disabled, as of version 11.38.

Legacy Apache Template System

The Apache template system that was used prior to cPanel & WHM 11, has been removed. This was located in `/usr/local/cpanel/etc/htt pdtempates`. More information on the updated Apache Template System can be found in our EasyApache Documentation.

Interchange

Interchange has been removed from cPanel & WHM 11.38. Upgrades from cPanel & WHM 11.36 will be blocked if Interchange is enabled.

Appendix A: Provided third-party applications

cPanel & WHM 11.38 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	4.80.1-1	11.37.0
MySQL 5.5	5.5.30-4	11.37.0
NSD	3.2.14-1	11.37.0
MyDNS	1.2.8.31-4	11.37.0
Pure-FTPd	1.0.36-6	11.37.0
Pro-FTPd	1.3.5rc1-3	11.37.0
Courier	4.12.0-1	11.37.0
Dovecot	1.2.17-2	11.37.0
Horde Groupware	1.2.11	11.37.0
Roundcube	0.8.5	11.37.0
SquirrelMail	1.4.22	11.37.0
phpPgAdmin	5.0.4	11.37.0
phpMyAdmin	3.5.8	11.37.0

Appendix B: New and modified API calls

New UAPI Calls

- Unified API - SSL Module — This module and its functions will allow users to manage SSL certificates.

New Remote API Functions

- Set the Primary Domain (`set_primary_servername`) — This function allows WHM users to set the primary domain on an IP address and port type for their accounts' sites.
- Restore Queue Add Task (`restore_queue_add_task`) — This function allows you to restore a user's account from a backup file.
- Restore Queue Activate (`restore_queue_activate`) — This function allows you to activate the restore queue and trigger a process to restore all queued accounts.
- Restore Queue Is Active (`restore_queue_is_active`) — This function allows you to see if the queue is actively processing restore jobs.
- Restore Queue List Pending (`restore_queue_list_pending`) — This function allows you to list all queued accounts to be restored.
- Restore Queue List Active (`restore_queue_list_active`) — This function allows you to list all accounts currently being restored.
- Restore Queue List Completed (`restore_queue_list_completed`) — This function allows you to list all completed restorations along with the success or failure of the restore and the restore log.
- Restore Queue Clear Pending Task (`restore_queue_clear_pending_task`) — This function allows you to clear a single pending account from the *Restoration Queue*.
- Restore Queue Clear All Pending Tasks (`restore_queue_clear_all_pending_tasks`) — This function allows you to clear all pending accounts from the *Restore Queue*.
- Restore Queue Clear Completed Task (`restore_queue_clear_completed_task`) — This function allows you to clear a single, completed account from the *Restoration Queue*.
- Restore Queue Clear All Completed Tasks (`restore_queue_clear_all_completed_tasks`) — This function allows you to clear all successfully completed tasks from the *Restoration Queue*.
- Restore Queue Clear All Failed Tasks (`restore_queue_clear_all_failed_tasks`) — This function allows you to clear all failed tasks from the *Restoration Queue*.
- Restore Queue Clear All Tasks (`restore_queue_clear_all_tasks`) — This function allows you to clear the *Restoration Queue* of all jobs, no matter the status.
- Backup Config Get (`backup_config_get`) — This function allows you to receive detailed data from your backup destination config file.
- Backup Config Set (`backup_config_set`) — This function allows you to save the data from the backup config page and put the data in `/var/cpanel/backups/config`
- Backup Skip Users All (`backup_skip_users_all`) — This function allows you to save the configuration for a given backup type. You can enable or disable backups all users.
- Backup Skip Users All Status (`backup_skip_users_all_status`) — This function allows you to retrieve the value from the status log file in the `backup_skip_users_all` api call.
- Backup Set List (`backup_set_list`) — This function allows you to find all backup files available on the server. This function also returns a list of users and dates so that the Restore Account(s) feature in WHM can show them.
- Backup Date List (`backup_date_list`) — This function allows you to retrieve a list of all dates that have backups.
- Backup User List (`backup_user_list`) — This function allows you to list all users with a backup file on a specific date.
- Backup Destination Validate (`backup_destination_validate`) — This function allows you to run a validation routine on a specified backup destination.
- Backup Destination Add (`backup_destination_add`) — This function allows you to create a backup destination and save it to a config file.
- Backup Destination Set (`backup_destination_set`) — This function allows you to modify the setup and data for a backup destination. The information is saved to the config file of the backup destination.
- Backup Destination Delete (`backup_destination_delete`) — This function allows you to remove the backup destination config file.
- Backup Destination Get (`backup_destination_get`) — This function allows you to retrieve detailed data for a specific backup destination from the backup destination config file.
- Backup Destination List (`backup_destination_list`) — This function allows you to list all backup destinations, including their configuration information.