
cPanel™ 11.26 Release Notes

Copyright © 2010 cPanel, Inc.

Published September 10, 2010

Abstract

Please refer to the cPanel™ 11.26 release notes [<http://docs.cpanel.net/twiki/bin/view/AllDocumentation/ReleaseNotes>] for the most recent version.

Table of Contents

1. Notice of Version Number Change	2
2. Feature Updates	2
2.1. Account Transfers	2
2.2. Account Backup and Restoration	2
2.3. Apache Configuration	2
2.4. APIs	3
2.5. Bandwidth Statistics Generation	5
2.6. Customer Contact	5
2.7. Database Soft Quotas	5
2.8. DNS Clustering	6
2.9. Email Addresses	6
2.10. Email Accounts X3 Interface	7
2.11. Fetch CSV	7
2.12. Integration	7
2.13. Localization	7
2.14. Log Processing	8
2.15. MX Editor	8
2.16. Password Strength Validation	9
2.17. PostgreSQL	9
2.18. Pure-FTPd	9
2.19. Reseller Nameservers	10
2.20. Roundcube	10
2.21. VirtFS and Jailshell	11
3. Added Features	12
3.1. cPanel™ DNS Editors	12
3.2. Custom MIME Types for cpsrvd	13
3.3. File and Directory Access Optimization	13
3.4. JSON API	14
3.5. MySQL Upgrade	15
3.6. Security Improvements	15
3.7. Task Queue	17
3.8. Web Template Editor	18
4. Application Updates	18
A. Issues Resolved in cPanel™ 11.26	19

1. Notice of Version Number Change

cPanel has changed its version number scheme as outlined at cPanel Product Versions [<http://etwiki.cpanel.net/twiki/bin/view/AllDocumentation/InstallationGuide/CpanelProductVersions>]. To bring the current product in line with this change cPanel 11.25.0 was reverted to 11.26. As part of this change the update tier is no longer displayed in WHM or cPanel.

Product Documentation and Release notes have been updated to reflect this change.

2. Feature Updates

2.1. Account Transfers

For cPanel™ to cPanel™ transfers, the single and multiple account transfer interfaces in WHM now provide the ability to skip the home directory when packaging an account. This allows you to reduce the amount of time a transfer takes and choose a more efficient method to transfer the user's home directory.

The cPanel™ version of the remote server is auto-detected for cPanel™-to-cPanel™ account transfers. The *Remote Server Type* menu in the transfer interface is updated to reflect this change.

When transferring a mixture of reseller and non-reseller accounts using the **Multiple Account Transfer** interface, the resellers will transfer first. Prior cPanel™ versions would iterate through the users alphabetically.

Streaming support, introduced in cPanel™ 11.24, received various performance improvements. When the *Express Transfer* method is used with streaming, zone activation is deferred until the end of the account restoration process. This resolves an issue that occurs when transferring accounts among servers within a DNS cluster.

A **Select All** button was added to the **Express Transfer** column in the **Multiple Account Transfer** interface.

The transfer system now detects when the remote or local servers run out of disk space. The errors are captured and the administrator is notified.

2.2. Account Backup and Restoration

Bug #4090: [http://bugzilla.cpanel.net/show_bug.cgi?id=4090] Added the ability for the `/scripts/pkgacct` utility to only **tar** accounts, rather than **taring** and compressing, via **gzip**. This option reduces the CPU load and overall time required to generate a full backup, with the trade-off of consuming more disk space.

When restoring backups from read-only media a working directory is created in a suitable, writable location. The location is determined by the same function used during account creation, based upon the **HOMEDIR** and **HOMEMATCH** values in `/etc/wwwacct.conf`. The backup is extracted into the working directory, then the restoration occurs. Afterwards, the working directory is cleared.

The `cpmove` file location is now output at the end of the packaging process. Prior versions displayed it earlier in the process, risking losing the location due to terminal scroll buffer constraints.

2.3. Apache Configuration

Directives used by the *Prefork MPM* are available in the configuration interface found at **WHM >> Service Configuration >> Apache Configuration >> Global Configuration**. These directives include:

- MinSpareServers
- MaxSpareServers

- MaxClients
- MaxRequestsPerChild

2.4. APIs

2.4.1. Custom Event Handlers

cPanel™ 11.26 marks the beginning of transitioning the cPanel™ interface to using API2 for interaction with the product. To accomplish this some of the existing methods for triggering events were converted into API2 calls.

When an existing function is converted into an API2 call the function interface changes. In turn this changes the data passed to Custom Event handlers. Example 1, “Email :: addpop comparison between 11.24 and 11.26” illustrates the changes.

Example 1. Email :: addpop comparison between 11.24 and 11.26

In cPanel™ 11.24 and older the data passed to the Email :: addpop function hook was:

```
<cpanelevent>
  <errors></errors>
  <event>addpop</event>
  <module>email</module>
  <params>
    <param0>username</param0>
    <param1>password</param1>
    <param2>100</param2>
    <param3>domain.com</param3>
  </params>
</cpanelevent>
```

In cPanel™ 11.26 the data passed to the Email :: addpop function hook is:

```
<cpanelevent>
  <errors></errors>
  <event>addpop</event>
  <module>email</module>
  <params>
    <domain>domain.com</domain>
    <email>username</email>
    <password>password</password>
    <quota>100</quota>
  </params>
  <result>
    <reason>username+domain.com</reason>
    <result>1</result>
  </result>
</cpanelevent>
```

The following interfaces were changed to use API2 functions:

- Change MX Record
- Cron
- Email Accounts

2.4.2. XML-API

2.4.2.1.

The XML-API no longer prompts for HTTP authentication. Most of the time this is not an issue. Some HTTP libraries may wait for HTTP authentication requests before sending headers. Users of such libraries need to adjust usage to send headers with the initial request.

The following functions were added to the XML-API in cPanel™ 11.26:

2.4.2.2. Account Functions

`domainuserdata` This function displays information about a given domain, including addon and subdomains, whether CGI aliasing is enabled, log locations, and other details.

`setsiteip` This function allows you to change the IP address associated with a website, or a user's account, hosted on your server.

2.4.2.3. DNS Functions

`addzonerecord` This API function allows you to add a zone record.

`editzonerecord` This function allows you to edit an existing zone record.

`getzonerecord` This function allows you to view DNS zone records associated with a given domain

`removezonerecord` This function allows you to remove a zone record from the server

`resetzone` This API function will reset a DNS zone to its default values

2.4.2.4. Reseller Functions

`setresellerips` This function lets you add IP addresses to a reseller's account.

`setresellerlimits` This function lets you set limits on the amount of bandwidth and disk space a reseller can use.

`setresellermainip` This function lets you assign a main, shared IP address to a reseller's account.

`setresellerpackagelimit` This function allows you to control which packages resellers are able to use. It also lets you define the number of times a package can be used by a reseller.

`suspendreseller` This function lets you suspend a reseller, thereby preventing the reseller from accessing his or her account.

`unsuspendreseller` This function lets you unsuspend a reseller, thereby allowing the reseller to access his or her account.

acctcounts	This function lists the number of accounts owned by each reseller on the server.
setresellernameservers	This function allows you to define a reseller's nameservers.
configureservice	This function allows you to enable or disable a service, and enable or disable monitoring of that service, as in the WHM Service Manager

Further information is available in the XML-API Documentation [<http://docs.cpanel.net/twiki/bin/view/AllDocumentation/AutomationIntegration/XmlApi>]

2.5. Bandwidth Statistics Generation

The system for compiling, and displaying, bandwidth statistics received many updates in cPanel 11.25/11.26. For the most up to date information consult cPanel Log Processing and Configuration [<http://docs.cpanel.net/twiki/pub/AllDocumentation/ReleaseNotes/cPanellogd.pdf>]

2.6. Customer Contact

The **Customer Contact** feature replaces the **Support Request** system that exists in prior versions. Resellers may configure this feature to display contact details for support, billing and sales departments.

The feature retains the ability to allow contact submissions via email or external applications. A simplified branding editor in this interface allows the reseller to modify the cPanel™ interfaces used by this feature.

This feature is available to all resellers. Configuration and template data for each reseller is stored in the `cpanelbranding` directory in the reseller's home directory. For the **root** user this is `/var/cpanel/cpanelbranding`. Configuration data is stored in the `contactinfo.yaml` file while branding related changes are stored in one of the following:

Table 1. Customer Contact Branding Files

File Name	Purpose
<code>contactinfo_include.html</code>	Displays contact information in the Contact and Help cPanel™ interfaces.
<code>supportinfo_include.html</code>	Displays a support request form in the Contact and Help cPanel™ interfaces.

2.7. Database Soft Quotas

The file used to cache the number of databases owned by an account moved from `/home/user/.cpanel/datastore/mysql-db-count` to `/var/cpanel/datastore/user/mysql-db-count`. Likewise the PostgreSQL cache file is now `/var/cpanel/datastore/user/postgres-db-count`.

To keep the cache file current, a cron job executes the following command periodically: `/scripts/update_db_cache`.

cPanel™ 11.26 provides support for including the disk space consumed by an account's MySQL and PostgreSQL database in the disk usage for the account. To enable this feature toggle the following Tweak Setting:

When displaying disk usage in cPanel/WHM include Postgresql and MySQL® disk usage.

As with the database counts, the disk usage calculation is handled by `/scripts/update_db_cache` which executes every 4 hours. This script is executed upon enabling the Tweak Setting. Administrators may also execute this script to recalculate the figures. The disk usage figures are stored in `/var/cpanel/datastore/mysql-disk-usage` and `/var/`

cpanel/datastore/postgres-disk-usage. The file contents are a colon (:) separated list of user names and figures in bytes. See Example 2, “mysql-disk-usage contents”

Example 2. mysql-disk-usage contents

```
root@c5vm [~]# cat /var/cpanel/datastore/mysql-disk-usage
user1: 0
user2: 3190942
user3: 42519945
```

Support for `/scripts/updatesmysqlquota` ends as of cPanel™ 11.25.0. Per this change `/scripts/updatesmysqlquota` is no longer distributed with the product.

2.8. DNS Clustering

Certain **dnsadmin** operations are now performed in batches. This reduces both the memory needed during large operations, and the amount of time needed to perform the operation.

Each cPanel™ 11.26 cluster member may now configure a peer failure threshold. This option is found in the **Configure Cluster** interface in WHM. The threshold specifies how many **dnsadmin** commands a peer may fail to respond to before that peer is automatically disabled. The threshold is local to the server where it is stipulated.

By default, each cPanel™ 11.26 cluster member will notify the system administrator when peers are disabled due to reaching the failure threshold. The notifications are sent to the *High* priority destinations as set in the **Contact Manager** in WHM.

The amount of time between BIND restarts issued by **dnsadmin** is configurable via a new option in the WHM *Tweak Settings* interface. This option is labeled:

Number of seconds dnsadmin will wait before restarting BIND. Additional restart requests during this time period will be silently discarded. On systems that process very frequent DNS updates a setting of 300 or 600 seconds is recommended. On systems with few DNS changes, the default setting of 0 is recommended. Note that DNS changes will not take effect until the restart is complete.

Prior versions would use two separate **dnsadmin** calls to add a zone and reconfigure BIND. In cPanel™ 11.26, this common activity is reduced to a single **dnsadmin** call.

2.9. Email Addresses

cPanel™ 11.26 expands the range of acceptable characters in the local part of email addresses to be closer in line with RFC 5322. Addresses created and managed by cPanel™ have the following limitations:

- Disallowed characters that have special meaning to the shell: `&\'*/`
- Disallowed characters due to use as data value separators: `@:%`

Prior versions of cPanel™ only accepted the dash (-), underscore (_), and period (.) in the local part of an email address.

Interfaces that accept an email address for contact purposes should accept all RFC 5322 characters in the local part.

When upgrading to cPanel™ 11.26, email accounts with quotas larger than 2 GB will be upgraded to *unlimited*. This is due to limitations with Exim and Courier in handling larger quota values.

2.10. Email Accounts X3 Interface

This interface is replaced with a new JSON-based AJAX interface. A limited Javascript version exists for users who disable or block Javascript. The new JSON interface consumes less memory in the browser and is more responsive.

The pagination and display of this interface now handles thousands of accounts quickly and efficiently.

2.11. Fetch CSV

The Fetch CSV feature within the List Accounts interface received the following improvements in cPanel™ 11.25.0:

- Column headers are now provided.
- The generated file now contains every column that is in the List Accounts interface.

2.12. Integration

The `Digest::MD5` Perl module is no longer bundled with the cPanel and WHM application suite. Existing applications and cPAddons that rely upon this Perl module being provided by cPanel will not function properly after upgrading to cPanel™ 11.25.0.

Developers can address this change in one of two ways:

1. Use the `md5_fallback.pm` functionality provided in the OSCommerce cPAddon.
2. Bundle the `Digest::Perl::MD5` Perl module with their application.

2.13. Localization

cPanel™ 11.26 comes with a new localization system: `Cpanel::Locale`. This new system simplifies the translation and localization of cPanel, WHM, themes and command line applications. `Cpanel::Locale` is backwards-compatible with existing translation methods and language files.

`Cpanel::Locale` uses an XML format for interoperability. Two new interfaces in WHM make provision for importing and exporting a locale using XML.

Languages are now identified in the system by the two-letter ISO 639 [http://en.wikipedia.org/wiki/ISO_639] code. Territory-specific languages are indicated by the two-letter ISO 639 [http://en.wikipedia.org/wiki/ISO_639] code, followed by an underscore, then the two-letter ISO 3166 [http://en.wikipedia.org/wiki/ISO_3166] code. See Example 3, “ISO 639 + 3166 Example”

Example 3. ISO 639 + 3166 Example

The regional language for English as spoken in the United Kingdom is represented in the system as `en_gb`.

Prior cPanel™ 11 versions presented languages in two, or sometimes more, encodings: UTF-8 and Latin1 (ISO 8859-1). This caused unnecessary confusion and made translation more difficult. Languages used by `Cpanel::Locale` use UTF-8 unless there is a very specific reason not to.

`Cpanel::Locale` is more memory-efficient than the prior system, since phrases are only loaded when requested by the user interface.

Complete phrases are available for translation, a format more flexible than the prior method of translating phrase fragments.

The list of phrases in a language, known as a lexicon, is stored locally in YAML [<http://www.yaml.org/>] format and is subsequently compiled into GDBM [<http://www.gnu.org/software/gdbm/>] databases. This introduces a new dependency into the system, the `GDBM_File` [http://search.cpan.org/perldoc?GDBM_File] Perl module.

Although `GDBM_File` is a core Perl module, it will only exist if `libgdbm` was present when compiling Perl, when Perl is installed from source. On systems where Perl is installed via a binary package, this module may still not exist unless `libgdbm` was also installed. For example, on Red Hat Enterprise and CentOS systems, if the Development Tools package group is installed, then the `GDBM_File` [http://search.cpan.org/perldoc?GDBM_File] module will exist.

To account for systems that do not have the `GDBM_File` [http://search.cpan.org/perldoc?GDBM_File] module installed, `/scripts/checkperlmodules` is updated to install `GDBM_File` [http://search.cpan.org/perldoc?GDBM_File]. If necessary, `libgdbm` will be built from source and installed to `/opt`.

If the error message "Can't locate GDBM_File.pm in @INC ..." appears on a system, executing `/scripts/checkperlmodules` will resolve it.



Developer Warning

Application and theme developers should no longer use `Cpanel::Lang::LANG` in their products, as it is no longer supported.

Further information about `Cpanel::Locale` is available at docs.cpanel.net/locale [<http://docs.cpanel.net/locale>].

2.14. Log Processing

The way Apache and Bandwidth logs are processed changed in cPanel™ 11.25.0. The basic pattern for log processing is:

1. Construct a list of all logs that need processed.
2. Move each log in the list to a backup version (denoted by the `bkup` extension).
3. Restart Apache if at least one file was moved to a backup version.
4. Process the backup version of the logs.
5. Remove the backup version of the logs.



Note

A backup of the bandwidth bytes logs is always created and processed as above. A backup of the access log(s) is only created if the log processing configuration instructs the log processing to delete rather than preserve the log. In this case, the file is processed in place.

2.15. MX Editor

The cPanel™ and WHM **MX Editor** interfaces and subsystems received an update in cPanel™ 11.26.

The cPanel™ interface is JSON powered, requiring Javascript to function.

The method of configuring how the local server routes mail is improved in cPanel™ 11.26. With cPanel™ 11.24 and prior versions a single check box, labeled *Always accept mail locally even if the primary MX does not point to this server* was the only control exposed in the **MX Entry** interface. This option could still be over-ridden by various circumstances.

This changed for cPanel™ 11.26. There are now the following options to configure how mail is to be handled by the local server:

- Automatically Detect MX Configuration
- Local Mail Exchanger
- Backup Mail Exchanger
- Remote Mail Exchanger

These options are presented in the **Email Routing** section of the **MX Entry** cPanel™ interface. A brief description of each option appears in the cPanel™ interface. The description includes how the option will change the way the local system handles email for the domain being modified. This setting may be changed independently from the action of modifying a MX record.

Modifying the Email Routing for domain changes, or adds, an entry to the cPanel™ user file, normally in `/var/cpanel/users`. See Table 2, “Email Routing Configuration Directives”.

Table 2. Email Routing Configuration Directives

Option	Directive
Automatically Detect	Removes MXCHECK
Local MX	<code>MXCHECK-example.com=0</code>
Backup MX	<code>MXCHECK-example.com=secondary</code>
Remote MX	<code>MXCHECK-example.com=remote</code>

Both **MX Editor** interfaces properly support multiple MX entries of the same priority.

2.16. Password Strength Validation

The algorithm used to rate the strength of a password is improved in cPanel™ 11.26. This may cause passwords that had high ratings with the prior algorithm to be rated as less strong.

The password validation used on various forms is now in sync with the server side algorithm. This eliminates inconsistencies that exist in cPanel™ 11.24 and prior versions.

Spaces are no longer accepted in passwords.

2.17. PostgreSQL

Clicking the **PHPPgAdmin** link in cPanel™ now logs the user into **PHPPgAdmin** automatically.

The configuration of PostgreSQL within WHM is also more reliable.

2.18. Pure-FTPd

Version 1.0.22 and higher of this popular FTP daemon allows the administrator to enforce TLS encryption on both the command and data channels of an FTP session. The **FTP Server Configuration** interface in WHM is updated to provide access to this feature.

The **Broken Clients Compatibility** directive is added to the WHM **FTP Server Configuration** interface. When enabled, this directive causes Pure-FTPd to ignore parts of the FTP protocol standards, to improve compatibility with some buggy FTP clients and firewalls.

2.19. Reseller Nameservers

Resellers may modify their nameservers using a new, simplified **Basic cPanel/WHM Setup** interface. This was available only for the root user in the **Edit Privileges/Nameservers** interface in the **Reseller Center** for cPanel™ 11.24.4 and prior versions. This feature is automatically available for all Resellers and is not governed by ACLs.

2.20. Roundcube

cPanel™ 11.26 adds support for using SQLite [http://www.sqlite.org/] as the RoundCube data store. When this option is enabled, each email account receives its own SQLite database file, which resides in `/home/user/etc/example.com/user.rcube.db`. The database file for the cPanel™ account is `/home/user/etc/example.rcube.db`.

This feature also changes the process ID of webmail logins for RoundCube sessions. Rather than being owned by the `cpanelroundcube` user, the process is owned by the cPanel™ system account that owns the email account. See Example 4, “User owned roundcube session”.

Example 4. User owned roundcube session

The RoundCube session for the `<user@example.com>` account, owned by the *example* cPanel™ account appears as:

```
example 27245 0.3 1.8 20764 9340 ? Ss 22:10 0:00 webmaild - serving 10.250.0.10
```

2.20.1. Pre-conversion Considerations

Before performing the conversion, the following matters need considered:

- The upgrade affects the entire server. It is not possible to mix use of the MySQL database and the SQLite database method.
- RoundCube only supports SQLite version 2, which is the default version provided by PHP 5.
- SQLite version 2 databases are incompatible with SQLite version 3 utilities.
- No system utilities are provided for managing the SQLite databases. This means no **sqlite** binary is installed by which a system administrator may view or manage a SQLite version 2 database.
- Conversion is an elective process, with *no* support for returning to using MySQL for the database.
- As with any volatile system change, please ensure current, tested system and account backups exist.
- Each email account has its own SQLite database. This database is stored in the *etc* directory of the cPanel™ account home directory that owns the email account.
- Since the SQLite database is placed in `/home/user`, it is included in the disk usage calculations and file system quota.



Disk Usage Warning

RoundCube stores information about each email message in the database. Tests show that, on average, 1 MB of disk space is consumed by the SQLite database per 10-15,000 messages in an email account.

If an account consumes its remaining disk quota during the conversion process, the remainder of the email addresses for the account are skipped. The conversion process will proceed with the remaining cPanel™ accounts. Once conversion is complete, the account(s) whose quota was consumed by the process will need disk space freed, or the quota increased. Then, conversion for the account may be completed using the `/scripts/convert_roundcube_mysql2sqlite` method described in Section 2.20.3, “SQLite Maintenance and Utilities”.

2.20.2. Converting to SQLite

The conversion to SQLite is accomplished by executing the command:

```
/scripts/convert_roundcube_mysql2sqlite
```

The `convert_roundcube_mysql2sqlite` script will first convert the MySQL RoundCube database to corresponding SQLite databases. Since the MySQL database contains all data for every email account that uses RoundCube, this part of the conversion can be a lengthy process. After database conversion, RoundCube is reconfigured to use SQLite, and the process completes. Any errors encountered are reported on the console. Problems converting individual accounts do not halt the conversion process.

After performing the conversion, the MySQL RoundCube database is no longer needed and may be dropped.

2.20.3. SQLite Maintenance and Utilities

Once the server is converted, individual cPanel™ accounts may be converted using `/scripts/convert_roundcube_mysql2sqlite`. This script accepts a single parameter: *user*.

```
/scripts/convert_roundcube_mysql2sqlite user
```

An SQLite configured RoundCube is updated using `/usr/local/cpanel/bin/update-roundcube-sqlite`. Calling `/usr/local/cpanel/bin/update-roundcube` on an SQLite configured system results in a warning message being displayed and the proper script being **execed**.

SQLite versions prior to 3.1 do not automatically **VACUUM** a database. As documented in the SQLite FAQ [<http://sqlite.org/faq.html#q12>] the **VACUUM** returns unused disk space to the operating system. To work around this a **VACUUM** routine is added to the logout sequence in RoundCube. Users that click the **logout** link in RoundCube will have their database automatically **VACUUM**ed.



Disk Usage Warning

The **VACUUM** command will temporarily consume twice the disk space consumed by the database file. As this happens in `/home/user/etc` it is possible for the process to consume the remaining disk quota of the cPanel™ account.

2.21. VirtFS and Jailshell

When terminating an account, the VirtFS mounts for the account are removed.

The VirtFS mounts for an account are cleared when changing the shell of the account. This only happens automatically when using the **Manage Shell Access** interface in WHM.



Session Disruption

If a user has an active jailshell session when the Administrator changes the user's shell, the user's connection is terminated. This is necessary to allow successful removal of the bind mounts used in the jailshell environment.

Administrators may use the following script for clearing VirtFS mounts: `/scripts/clear_orphaned_virtfs_mounts`. This script only removes the mounts for users who no longer use jailshell or no longer exist. This script accepts the following parameters:

`--help` Outputs brief description of the command and accepted parameters.

`--erroronly` Limit output to error messages.

Jailshell sessions now include the name of the logged-in account in the process table as demonstrated in Example 5, “Jailshell Login Name”.

Example 5. Jailshell Login Name

```
root@pxe [~]# ps ax | grep jail
20847 pts/2    Ss      0:00 jailshell (case899) [20953]
```

3. Added Features

3.1. cPanel™ DNS Editors

In cPanel™ 11.26, the X3 interface includes both a **Simple DNS Editor** and an **Advanced DNS Editor** feature. The Simple editor is enabled by the default. The Advanced editor is disabled by default. Access to either editor is handled via the **Feature Manager** in **WHM**.

3.1.1. Simple DNS Editor

The cPanel™ **Simple DNS Editor** permits users to add and remove A and CNAME resource records for existing zones. No editing of records is permitted via this interface. To edit a record, the existing one must first be deleted. Duplicate A records are permitted.

A Record: The user is permitted to supply the name of the record and an IP address. The TTL specified in the **WHM Basic cPanel/WHM Setup** interface is used.

CNAME Record: the user is permitted to supply the name and CNAME of the record. The TTL specified in the **WHM Basic cPanel/WHM Setup** interface is used.

3.1.2. Advanced DNS Editor

The **Advanced DNS Editor** lets users add, edit and delete A, CNAME and TXT resource records. The user may specify the TTL when creating or modifying the record.

Both editors automatically append the name of the domain being modified to new records. To provide a fully-qualified name, terminate the name with a period. Refer to Figure 1, “Using A Fully Qualified Name in the DNS Editor”.

Figure 1. Using A Fully Qualified Name in the DNS Editor**Add a Record**

Name: ✓

TTL: ✓

Type: ▼

TXT Data: ✓

3.2. Custom MIME Types for cpsrvd

Administrator defined MIME-types may be added to cpsrvd. This is accomplished by adding entries to `/var/cpanel/config/cpsrvd/custom_mime_types`. As shown in Example 6, “Custom MIME Types” the file format is:

- Entries are new-line separated.
- Entry is a **key=value**

The **key** portion of the entry represents the file extension. The **value** represents the MIME type.

Example 6. Custom MIME Types

```
xls=application/vnd.ms-excel
txt=text/plain
```

3.3. File and Directory Access Optimization

A common tactic used to improve file system performance is to use the `noatime` **mount** option for a mount point. The `ext` family, beginning with `ext2`, supports disabling `atime` for individual files and directories. This can be accomplished with the following command:

```
root@pxe# chattr +A /path/to/file/or/directory
```

cPanel™ 11.26 uses `/usr/local/cpanel/bin/optimizefs` to disable the `atime` attribute for a specific list of files and directories. A cronjob is created to perform this optimization periodically. As of cPanel™ 11.25.0, the list of files and directories modified by this cron job are:

Files and Directories Modified by optimizefs

- Files
- /etc/relayhosts
 - /etc/wwwacct.conf
 - /etc/wwwacct.conf.shadow
 - /etc/wwwacct.conf.shadow.cache
 - /etc/wwwacct.conf.cache
 - /etc/relayhostsusers
 - /etc/cpbackup.conf
 - /etc/cpbackup.conf.cache
 - /etc/exim.pl
 - /etc/exim.pl.local
 - /etc/passwd
 - /etc/shadow
 - /etc/group
 - /etc/termcap
 - /etc/fstab
 - /etc/localtime
 - /usr/local/cpanel/cpanel.lisc
 - /usr/local/cpanel/cpsanitycheck.so
- Directories
- /usr/local/cpanel/base/frontend
 - /etc/valiases
 - /etc/vfilters
 - /etc/vdomainaliases
 - /var/cpanel/adminsessions
 - /usr/local/apache/domlogs

3.4. JSON API

cPanel™ 11.26 adds support for JSON output from an API call. As discussed in the JSON [<http://docs.cpanel.net/twiki/bin/view/AllDocumentation/AutomationIntegration/XmlApi>] documentation, developers can activate this by using **/json-api/** in the API call, rather than **/xml-api/**.

Long running JSON initiated processes appear in the process table as (example truncated for display purposes):

```
22410 ?          D          0:03 /usr/local/cpanel/cpanel --json-fast-connect --stdin
```

3.5. MySQL Upgrade

A new interface for managing the process of upgrading MySQL is available as of cPanel™ 11.25.0 build 41902. The new interface is found in the **Software** section in WHM. The MySQL version selection is removed from Tweak Settings.

The new MySQL Upgrade interface walks you through the upgrade process. This process typically includes rebuilding PHP for Apache and sometimes for cPanel. The majority of the process may be accomplished unattended.

The interface only supports upgrading versions, for example from MySQL 4.1 to MySQL 5.1. It does not support downgrading. Downgrades are not recommended.

As part of the MySQL upgrade, the version of PHPMyAdmin installed may change. This happens when upgrading from MySQL 4.0 or 4.1 to MySQL 5.0 and higher.



PHP Version Incompatibility

PHPMyAdmin 3 is not compatible with PHP 4. cPanel™ provides PHP 5.2.6 for the internal PHP binary. This binary, at `/usr/local/cpanel/3rdparty/bin`, is used to serve the internal PHP applications that ship with the product, such as PHPMyAdmin. If this binary has been modified, or overwritten to be PHP 4, then complications will arise with PHPMyAdmin upon upgrading MySQL 5.0.

3.6. Security Improvements

Cross-site request forgery (CSRF or XSRF) attack prevention is improved with the addition of several options in the WHM *Tweak Settings* interface.

3.6.1. Referer Checks against Destination URL

Along with the blank referer check that existed in prior versions, server owners may now require the domain and port (or IP address and port) combination in the referer to match the destination URL. To enforce this, enable the following **Tweak Settings** option:

Only permit cpanel/whm/webmail to execute functions when the browser provided referrer (Domain/IP and Port) exactly matches the destination URL. This will help prevent XSRF attacks, but may break integration with other systems, login applications, and billing software. Cookies are required with this option enabled.

3.6.2. Security Tokens

The new security token feature prevents XSRF attacks by injecting a token unique to the session into the URL. Use of this feature is strongly recommended. Enable this feature with the following option in **Tweak Settings**:

Require security tokens for all interfaces. This will greatly improve the security of cPanel™ and WHM against XSRF attacks, but may break integration with other systems, login applications, billing software and third party themes.



Product Incompatibility Warning

The Security Tokens feature will break third party applications, scripts and themes that are not updated to work with Security Tokens. Information regarding the Security Token feature was sent to Third Party developers in advance. Please ensure any third party products integrated with cPanel™ are fully updated before enabling this feature.



Backwards Incompatibility Warning

Active cPanel, Webmail and WHM sessions will generate 404 errors if the security token feature is enabled and the system is subsequently downgraded to cPanel™ 11.24.4. Active sessions will need to log out manually, then re-log in. Manual logouts are accomplished by changing the URL to /logout/

3.6.3. IP Address Validation

To improve security of cookie based logins server owners can opt to record the client IP Address in the server and client side cookies. The IP address is subsequently validated for each request during the session. This option is enabled via the following **Tweak Setting**:

Validate the IP addresses used in all cookie based logins. This will limit the ability of attackers who capture cPanel™ session cookies to use them in an exploit of the cPanel™ or WebHost Manager interfaces. For this setting to have maximum effectiveness, proxydomains should also be disabled.

3.6.4. Other Security Improvements

3.6.4.1. Disabling Root Login to cPanel

Server administrators can prevent root login to the cPanel™ interface. This is a refinement of the existing reseller override feature, wherein both the reseller and root user may access a cPanel™ account by using the account name and the root or reseller password.

To restrict root access, enable the following option in **Tweak Settings**:

Only allow reseller to log in to users' cPanel™ interface with reseller password

3.6.4.2. Require SSL Authentication for Remote Logins

It is now possible to disable all authentication and access on the non-SSL ports used by `cpsrvd`. These ports are:

- 2082
- 2086
- 2095

This is accomplished by setting the following configuration item in **Tweak Settings**:

Require SSL for all remote logins to cPanel, WHM and Webmail. This setting is recommended.

When enabled, accessing the non-SSL ports produces a page containing a link redirecting the user to the SSL port. Logins that originate from localhost are still allowed with this setting enabled.



Incompatibility Warning

Since this **Tweak Settings** option disables access on the non-SSL ports, custom scripts and third-party applications that access the server remotely must use the SSL ports.

Bookmarked URLs that use the non-SSL ports will need to be updated to use the SSL port. When a user clicks a bookmark that uses the non-SSL port, the link is not carried through the manual redirect to the SSL port.

3.6.4.3. Session Handling

Sessions that are inactive for 8 hours or more are now invalidated. Subsequent use of such session will force re-authentication. Invalidated, or inactive, session files are purged from the system every 20 minutes.

In determining which of the new settings to activate cPanel™ recommends the following:

- Require SSL for all remote logins to cPanel, WHM and Webmail.
- Require security tokens for all interfaces.
- Validate the IP addresses used in all cookie based logins.

The referrer settings are only recommended if the security tokens are not enabled.

3.7. Task Queue

Events in cPanel™ often cause one or more services to be restarted. For example, a user adding a subdomain causes a restart of Apache and the nameserver daemon. On busy servers, such restart requests can cause quality of service issues.

To handle these requests, cPanel™ 11.26 comes with a task queueing and processing system. cPanel™ subsystems that are aware of the task queue submit their requests to it, rather than issuing the restart (or other request) directly.

A primary benefit of the task queueing system is that multiple requests for an outstanding request are handled as a single action. At this time, only the Apache restarts issued by the WHM *Tweak Settings* interface are task queue-aware.

There are two aspects of the task queueing system: the queueing mechanism and the queue processor. Queueing of tasks is handled via `/usr/local/cpanel/bin/servers_queue` which has the following usage:

```
/usr/local/cpanel/bin/servers_queue [queue command] [unqueue task id]
```

`queue command` The queue parameter requires a command string as an argument. The command string should be quoted. See Example 7, “Queueing Tasks”. Only commands known to the task queueing system are accepted. Providing an unknown command returns an error. See Example 8, “Queueing an Unknown Task”.

`unqueue id` Requires a task ID number. This is output when queueing a task. It may also be obtained by examining the `/var/cpanel/taskqueue/servers_queue.yaml` file. See Example 9, “Unqueueing A Task”.

Queued tasks are stored in YAML files in `/var/cpanel/taskqueue`.

The task queue is processed periodically by a new daemon `queueprocd`. This daemon resides in `/usr/local/cpanel/libexec` and is started by the cPanel™ start up process. It may be managed using `/scripts/restartsrv_queueprocd`. The daemon is monitored by `chkservd`.

Example 7. Queueing Tasks

```
root@example [~]# /usr/local/cpanel/bin/servers_queue queue 'apache_restart'
Id: TQ:TaskQueue:4
```

Example 8. Queueing an Unknown Task

```
root@example [~]# /usr/local/cpanel/bin/servers_queue queue 'buildapacheconf'  
ERROR: No known processor for 'buildapacheconf'. at /usr/local/lib/perl5/site_perl/5.8.8/
```

Example 9. Unqueueing A Task

```
root@pxe [~]# /usr/local/cpanel/bin/servers_queue queue 'apache_restart'  
Id: TQ:TaskQueue:8  
root@pxe [~]# /usr/local/cpanel/bin/servers_queue unqueue TQ:TaskQueue:8  
1 tasks unqueued
```

3.8. Web Template Editor

This new WHM interface presents a unified method of modifying various templates used by Apache. Some of these templates were available for editing in prior versions of cPanel. This interface is automatically available to all resellers.

The templates available are:

- Default Web Page
- Suspended Account Page
- Account Moving Page
- Connection Detection Page

Template Toolkit provides the template processing engine.

The following CGI binaries in `/usr/local/cpanel/cgi-sys` handle displaying of the templates:

- defaultwebpage.cgi
- movingpage.cgi
- suspendedpage.cgi
- templatepreview.cgi

This initial implementation only supports creation and serving of templates in English. Future versions of this interface will support more languages.

4. Application Updates

The following applications are upgraded as part of cPanel™ 11.26:

- glib to 2.20.0

- Mailman to 2.1.13
- phpMyAdmin 2 to 2.11.10
- phpMyAdmin 3 to 3.2.4
- Pure-FTPd to 1.0.22
- RoundCube to 0.3.1
- SquirrelMail to 1.4.21

A. Issues Resolved in cPanel™ 11.26

Please see the change log at changelog.cpanel.net [<http://changelog.cpanel.net>] for a list of issues addressed in cPanel 11.26