Tweak Settings - Security

For cPanel & WHM version 11.50

(*Home* >> *Server Configuration* >> *Tweak Settings*)

Allow autocomplete in login screens.

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

This setting defaults to *On*.

CGIEmail and CGIEcho

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

This setting defaults to *On* for backward compatibility.

Hide login password from cgi scripts

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

This setting defaults to *Off*.

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

Cookie IP validation

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

Select one of the following options:

- *disabled* — Does **not** validate IP addresses.

- *loose* — The access IP address and the cookie IP address **must** be in the same class C subnet.
- *strict* — The access IP address and the cookie IP address **must** match exactly.

This setting defaults to *strict.*

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

Generate core dumps

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

This setting defaults to *Off*.

> **Warning:**
> Core dumps contain sensitive information. Make certain that you keep them secure.

Send passwords when creating a new account

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

This setting defaults to *Off*.

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

Blank referrer safety check

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

This setting defaults to *Off*.

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

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

Referrer safety check

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

This setting defaults to *Off*.

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

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

Require SSL

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

This setting defaults to *On*.

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

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

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

This setting defaults to *Off*.

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

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

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

This setting defaults to *Off*.

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

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

This setting defaults to *Off*.

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

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

This setting defaults to *Off*.

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

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

This setting defaults to *Off*.

Use MD5 passwords with Apache

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

This setting defaults to *On* .

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

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

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

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

This setting defaults to *Off*.

> **Warning:**
> We **strongly** recommend that you do **not** use the setting with CentOS 5 or Red Hat Enterprise Linux 5, because these operating systems distribute older kernels with limitations. The Linux kernel versions for these operating systems and the number of bind mounts that VirtFS requires make it difficult to ensure system stability.

> **Notes:**
> - This option is **only** available if you compile Apache through EasyApache and installed `mod_ruid2` version 0.9.4a or later.
> - You can use this option with CentOS 5, 6, or 7, or Red Hat Enterprise Linux® 5 or 6.
> - This option is unavailable on systems that run CentOS or Red Hat Enterprise Linux version 5 with 256 or more users.

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

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

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

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

Signature validation on assets downloaded from cPanel & WHM mirrors

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

Select one of the following options:

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

This setting defaults to *Off*.

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

Verify Signatures of 3rdparty cPAddons

This setting verifies all 3rdparty cPAddons' GPG keys.

This setting is **only** available if you enable the *EXPERIMENTAL: S ignature validation on assets downloaded from cPanel & WM mirrors* setting.

This setting defaults to *Off.*

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

Allow weak checksum schemes

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

This setting defaults to *Off.*

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