Tweak Settings - Security

For cPanel & WHM version 68

(*WHM >> 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 legacy `cgi-sys` scripts interpret files in a user's `public_html` directory as potential input templates if they contain square bracket (`[ ]`) characters.

> **Warning:**
> The *CGI Center* interface *(cPanel >> Home >> Software and Services >> CGI Center)* **only** exists in cPanel's **deprecated** x3 theme. You **cannot** create new CGI scripts with cPanel's current theme (Paper Lantern), and we **strongly** discourage the use of the x3 theme.

This setting defaults to *On*.

Hide login password from cgi scripts

This setting hides the `REMOTE_PASSWORD` variable from scripts that the `cpsrvd` daemon's CGI handler executes.

> **Warning:**
> The *CGI Center* interface *(cPanel >> Home >> Software and Services >> CGI Center)* **only** exists in cPanel's **deprecated** x3 theme. You **cannot** create new CGI scripts with cPanel's current theme (Paper Lantern), and we **strongly** discourage the use of the x3 theme.

This setting defaults to *Off*.

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

Cookie IP validation

> **Important:**
> We **strongly** recommend that you do **not** rely on cookie-based IP validation.

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

You can select one of the following options:

- *disabled* — The system does not validate IP addresses.
- *loose* — The system requires that the access IP address and the cookie IP address must be in the same class C subnet.
- *strict* — The system requires that the access IP address and the cookie IP address match exactly.

This setting defaults to *strict.*

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

Generate core dumps

This setting specifies whether cPanel & WHM's services create core dumps. You can 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 to avoid a security risk.

Enable File Protect

This setting enables EasyApache 4's FileProtect module, which improves the security of each user's `public_html` directory.

This setting defaults to *On.*

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 the system to prevent cross-site request forgery (XSRF) attacks.

This setting defaults to *Off*.

> **Warning:**
> Exercise caution when you **enable** this setting. This setting can 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 function.

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 to prevent cross-site request forgery (XSRF) attacks.

This setting defaults to *Off*.

> **Warning:**
> Exercise caution when you **enable** this setting. This setting can 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 function.

Require SSL for cPanel Services

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 enables resellers to run PHP code in WHM. WHM's PHP code runs as the `root` user.

This setting defaults to *Off*.

> **Warning:**
> Exercise caution when you **enable** this setting.

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

This setting allows unregistered AppConfig applications to run when you log in to WHM as a reseller. When 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 unregistered AppConfig applications to run when you log in as a `root` user. When you disable this setting, a `root` user 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 registered AppConfig applications and addons to run without a defined ACL list. When you disable this setting, cPanel & WHM forces registered AppConfig applications and addons to set an ACL list.

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 registered AppConfig cPanel and Webmail apps to run without a defined required features list. When you disable this setting, cPanel & WHM forces registered AppConfig cPanel and Webmail apps to set a *Required Features* list.

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. Because Apache `.htpasswd` files can contain a mix of crypt- and MD5-encoded passwords, this setting does not change the encoding of any existing passwords.

This setting defaults to *On*.

Notes:

- When you disable this setting, Apache uses crypt hashing.
- MD5-encoded passwords provide more security 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.

Warning:
This feature is unstable and can result in unintended consequences. Exercise **extreme caution** if you enable an *EXPERIMENTAL* feat ure or setting.

- These features may **not** function with other features or settings.
- These features do **not** provide current and effective security controls.
- *EXPERIMENTAL* features do **not** qualify for our security bounty.

For information about an *EXPERIMENTAL* feature's compatibility, read our Change Logs documentation.

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

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

This setting defaults to *Off*.

Notes:

- You can use this setting when you compile Apache through EasyApache and you have installed `mod_ruid2` version 0.9.4a or later.
- You can use this setting with CentOS, RHEL 6 or 7, or Amazon® Linux.
- CloudLinux™ does not support the `mod_ruid2` module.

When you enable this option, each user with a configured `jailshell` or `noshell` 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. For example:

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

- The system limits the user's filesystem view to their `/home/virtfs/username` filesystem. Various jail shell-related options in the *Twea k Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings)* control the `/home/virtfs/username` 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 `httpupdate` mirrors.

For more information about these GPG keys, read our cPanel & WHM Download Security documentation.

You can select one of the following options:

- *Off* — The system does not validate any digital signatures.
- *Release Keyring Only* — The system uses the Release GPG keyring to validate official release downloads from cPanel & WHM `httpupdate` mirrors.
- *Release and Development Keyrings* — The system uses the Release and Development GPG keyrings to validate test and development release downloads from cPanel & WHM `httpupdate` mirrors.

This setting defaults to *Release Keyring Only*.

> **Warning:**
> This setting does **not** provide effective security control.

Generate a self signed SSL certificate if a CA signed certificate is not available when setting up new domains.

When you create a new domain, cPanel will automatically enable SSL for that domain if an SSL certificate exists. If no SSL certificate exists, this functionality will generate a self-signed certificate.

> **Note:**
> If you have **not** enabled a CA signed certificate or AutoSSL, Google search results may point to the SSL site version with a self-signed certificate. Self-signed certificates generate browser warnings.

This setting defaults to *On*.

> **Warning:**
> - We **strongly** recommend that you enable AutoSSL.
> - If you **disable** this option, and a CA signed certificate is **not** available, when a user attempts to visit the newly created domain over https, the user will see the first SSL certificate installed on that IP address.

Verify Signatures of 3rdparty cPAddons.

This setting verifies all 3rdparty cPAddons' GPG keys. You can enable this setting with the *Signature validation on assets downloaded from cPanel & WHM mirrors* setting.

This setting defaults to *Off*.

> **Warning:**
> This experimental setting does **not** provide effective security control.

Allow weak checksum schemes.

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

This setting defaults to *Off*.

> **Warning:**
> - You **must** enable this setting when you configure your system to download custom RPMs, cPADDONs, or EasyApache updates from non-cPanel sources.
> - The overall security of your system decreases when you **enable** this setting.

Allow deprecated WHM accesshash authentication

This setting allows users to authenticate with WHM via an access hash that they can create in WHM's *Remote Access Key* interface (*WHM >> Home >> Clusters >> Remote Access Key*).

> **Warning:**
> We deprecated WHM's *Remote Access Key* feature in cPanel & WHM version 64. We **strongly** recommend that you use API tokens in stead.

This setting defaults to *Off*.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

Content by label

There is no content with the specified labels

Content by label

There is no content with the specified labels

- Basic Security Concepts
- How to Determine Password Strength
- cPanelID
- Problems When You Log Out Of An Account
- Additional Security Software

Content by label

There is no content with the specified labels